

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

PRIVACY IMPACT ASSESSMENT (PIA) ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NOAA0201 Web Operations Center (WOC)

FISMA Name/ID (if different): _____

Name of IT System/ Program Owner: Cameron Shelton

Name of Information System Security Officer: David J. Skiffington

Name of Authorizing Official(s): Douglas A. Perry

Date of Last PIA Compliance Review Board (CRB): 1/9/2017
(This date must be within three (3) years.)

Date of PIA Review: 12/4/2017

Name of Reviewer: David Skiffington

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: SKIFFINGTON.DAVID.1374262730
Digitally signed by SKIFFINGTON DAVID 1374262730
DN c US, o U S Government, ou DoD, ou PKI, ou CONTRACTOR,
cn SKIFFINGTON DAVID 1374262730
Date 2017.12.04 08:28:08 -0500

Date of BCPO Review: 12.5.17

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: 7892
GRAFF.MARK.HYRUM.151444
Digitally signed by GRAFF MARK HYRUM 1514447892
DN c US, o U S Government, ou DoD, ou PKI,
ou OTHER, cn GRAFF MARK HYRUM 1514447892
Date 2017.12.05 09:24:06 -0500

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Thursday, January 11, 2018 2:08 PM
To: Gioffre, Kathy (Federal); CPO
Cc: Mark Graff NOAA Federal
Subject: NOAA0201 re signed PIA and new PTA
Attachments: NOAA0201 Web Operations Center WOC_011118.pdf; NOAA0201 PTA_122717 v2 mhg.pdf

Kathy, please put these in your folder with the certification I had already sent you.

Per our discussion, I put a note in the PIA under the "yes, new privacy risks" answer, to explain:

Note: there were such changes in 2017 but none in 2018 (dated 1 11 18)

ALSO note that other than the above addition and the updated ATO date NO changes were made to the PIA!

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751

Ce (b)(6)

**U.S. Department of Commerce
National Oceanic and Atmospheric Administration
(NOAA)**



**Privacy Threshold Analysis
for the
Web Operations Center (NOAA0201)**

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/Web Operations Center

Unique Project Identifier: 006-000351100 00-48-03-17-01-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

The Web Operations Center (WOC) is a diverse information technology services provider to Line and Staff Offices within NOAA. The WOC provide a wide range of information technology services and functions which include high availability, scalability, redundancy, clustering, and high performance computing to replicate and distributed general information as well as critical time sensitive life and property information to the general public and meteorology community.

The services and functions of the information system technology have been broken down into five (5) core services and functions: WOC Domain Name System Services (WOCDNSS), WOC Information Sharing Services (WOCISS), WOC Adoptive System Framework (WOCASF), WOC NOAA Enterprise Message System (WOCNEMS) and WOC Collaboration Services (WOCCS). These services and functions make up the subsystems within NOAA0201. Each subsystem has a different FIPS 199 security categorization as described in the NOAA0201 FIPS 199 Security Categorization document. NIST SP 300-37 rev1 describes how various independent subsystems could be grouped together for purpose of risk management into more comprehensive system (system of systems).

The WOC systems are physically located at 8 NOAA datacenters (W1: Silver Spring, Maryland W2: Largo, Maryland W3: Norman, Oklahoma W4: Boulder, Colorado W5: Fort Worth, Texas and W6: Seattle, Washington, W7: Ashville, NC and W8: Fairmont, WVA).

Note: NOAA0201 has been assessed on 1/12/2017 using NIST 800-53 Rev 4.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

- This is a new information system. *Continue to answer questions and complete certification.*
- This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

This is an existing information system in which changes do not create new privacy risks. *Continue to answer questions, and complete certification.*

Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *Please describe the activities which may raise privacy concerns.*

No

2. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the submitter has a commercial interest” and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.).”

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities

No, this IT system does not collect any BII.

3. Personally Identifiable Information

3a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 3a, please respond to the following questions.

3b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

3c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 3b, and/or 3c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

 x I certify the criteria implied by one or more of the questions above **apply** to NOAA0201 and as a consequence of this applicability, I will perform and document a PIA for this IT system.

 I certify the criteria implied by the questions above **do not apply** to NOAA0201 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

David J. Skiffington

Signature of ISSO or SO: SKIFFINGTON.DAVID.JEROME.1374262730 Digitally signed by SKIFFINGTON.DAVID.JEROME.1374262730
DN: c US, o U.S. Government, ou DoD, ou PKI,
ou CONTRACTOR,
cn SKIFFINGTON.DAVID.JEROME.1374262730
Date: 2018.01.10 13:45:29 -05'00' Date: _____

Name of Information Technology Security Officer (ITSO): Jean Apedo

Signature of ITSO: APEDO.JEAN.1188076064 Digitally signed by APEDO.JEAN.1188076064
DN: c=US, o=U.S. Government, ou=DoD,
ou=PKI, ou=OTHER,
cn=APEDO.JEAN.1188076064
Date: 2018.01.11 08:22:08 -05'00' Date: _____

Name of Authorizing Official (AO): Douglas Perry

Signature of AO: PERRY.DOUGLAS.A.1365847270 Digitally signed by
PERRY.DOUGLAS.A.1365847270
Date: 2018.01.10 17:13:05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): MARK GRAFF

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892
DN: c US, o U.S. Government, ou DoD, ou PKI,
ou OTHER, cn GRAFF.MARK.HYRUM.1514447892
Date: 2018.01.11 08:47:32 -05'00' Date: _____

U.S. Department of Commerce NOAA



Privacy Impact Assessment for NOAA0201 Web Operations Center (WOC)

Reviewed by: _____, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment NOAA0201 Web Operations Center (WOC)

Unique Project Identifier: 006-000351100 00-48-03-17-01-00

Introduction: System Description

The Web Operations Center (WOC) is a diverse information technology services provider to Line and Staff Offices within NOAA. The WOC provide a wide range of information technology services and functions which include high availability, scalability, redundancy, clustering, and high performance computing to replicate and distributed general information as well as critical time sensitive life and property information to the general public and meteorology community.

The services and functions of the information system technology have been broken down into five (5) core services and functions: WOC Domain Name System Services (WOCDNSS), WOC Information Sharing Services (WOCISS), WOC Adoptive System Framework (WOCASF), WOC NOAA Enterprise Message System (WOCNEMS) and WOC Collaboration Services (WOCCS). These services and functions make up the subsystems within NOAA0201.

NOAA WOC NOAA Enterprise Message System (WOCNEMS): The WOC NOAA Enterprise Message System (former MOC) provides top-level Directory Service, as part of NOAA's distributed Unified Messaging System. This includes maintaining the Master Directory, and replication of directory information to approximately 11 second to tier II level Consumers Directory Servers. WOCNEMS was recently merged into the WOC.

The WOCNEMS systems are physically located at 3 NOAA datacenters (W1: Silver Spring, Maryland W2: Largo, Maryland and W4: Boulder, Colorado).

As part of the distributed NEMS system, a redundant Master Directory Service is hosted at NOAA3400 (outside of NOAA0201 boundary) in Boulder, Colorado. This provides fault-tolerance. Directory services continue to operate despite failure of either location. All master directory replication traffic is encrypted using Secure Sockets Layer (SSL).

In addition to the top-level Directory services described above, there are consumers Directory Servers that provide local directory service to the departmental users. All directory synchronization traffic between Master and Consumer directory servers is encrypted using SSL.

WOCNEMS has also retained a limited portion of its Message Transfer Agent (MTA) server for mailing capability. There are a limited number of LDAP group accounts, ship's user accounts and trusted NOAA wide application servers that rely on the MTA for SMTP mail transfers. These accounts are allowed access if the sender is an authenticated LDAP user or the sending host machine is "Trusted hosts" on the MTA servers.

A typical transaction is LDAP verification and SMTP forwarding.

The WOC has now absorbed NOAA0300, Messaging Operations Center(MOC). The MOC services included servicing LDAP directories for all of NOAA. The information collected includes:

- Name
- Work address
- Work phone numbers
- Work e-mail addresses
- Organization name

5 U.S.C. 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Information sharing The information is shared only within the bureau.

The WOCNEMS is one of five subsystems which comprise NOAA0201 Web Operations Center (WOC). Taken together, NOAA0201 has a FIPS 199 security input category of “High”.

Individually the five subsystems are evaluated as follows:

SC (NOAA0201 Domain Name System Service) = (Low, High, High)

SC (NOAA0201 Information Sharing Services) = (Low, High, High)

SC (NOAA0201 Adoptive System Framework) = (Low, Low, Moderate)

SC (NOAA0201 Collaboration Services) = (Low, Low, Low)

SC (NOAA0201 NOAA Enterprise Message System) = (Low, Medium, Low)

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

This is a new information system.

This is an existing information system with changes that create new privacy risks.

(Check all that apply.)

***Note: there were such changes in 2017 but none in 2018 (dated 1-11-18)**

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging	X	g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

Section 2: Information in the System

- 2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: N/A					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	
e. Age		k. Email Address		q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	
b. Job Title		e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): X Organization Name					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify): None					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	<input checked="" type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input checked="" type="checkbox"/>		
Other (specify):					

Government Sources					
Within the Bureau	<input type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		
Other (specify)					

Non-government Sources					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
-------------------------------------	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	There are not any IT system supported activities which raise privacy risks/concerns.
-------------------------------------	--------------------------------------------------------------------------------------

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.
(Check all that apply.)

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The information which is subject to this PIA is not private and is not sensitive. The information is used for IT administration and for LDAP verification (federal employees and contractors)

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	-----------------------------------------------

- 6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input type="checkbox"/>	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

- 6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

- 7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.		
<input type="checkbox"/>	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at:		
X	Yes, notice is provided by other means.	Specify how: Notice is provided as part of employee enrollment,	

		and on the staff directory warning banner.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: An individual may decline but would not have access to the NOAA IT network.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: There is only one use, which is explained during employee orientation.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals may view their info online and make a request for a change.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 1/12/2018 <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.

X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Only NOAA personnel with authenticated access would be able to change or delete information.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C.

§ 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i> : DEPT-18 SORN
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. "Destroy immediately after copying to a recordkeeping system or otherwise preserving, but longer retention is authorized if required for business use." from http://www.corporateservices.noaa.gov/audit/records_management/schedules/index.html , Chapter 200-12.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Minimal admin information for IT work identity
X	Quantity of PII	Provide explanation: Minimal work contact information
X	Data Field Sensitivity	Provide explanation: There are no sensitive data fields.
X	Context of Use	Provide explanation: Minimal data for IT user identification
	Obligation to Protect Confidentiality	Provide explanation:

	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

<p>Information System Security Officer or System Owner Name: David J. Skiffington Office: OCIO Web Operations Center Phone: 301-628-5662 or 703-405-7900 (mobile) Email: david.j.skiffington@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: right;">SKIFFINGTON.DAVID.137426 <small>Digitally signed by SKIFFINGTON DAVID 1374262730 DN: c US, o U.S. Government, ou DoD, ou PKI, ou CONTRACTOR, cn SKIFFINGTON DAVID 1374262730 Date: 2017.12.27 08:01:23 -05'00'</small></p> <p>Signature: 2730</p> <p>Date signed:</p>	<p>Information Technology Security Officer Name: Jean Apedo Office: OCIO Cyber Security Division Phone: 301-638-5730 Email: jean.apedo@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: right;">APEDO.JEAN <small>Digitally signed by APEDOJEAN.1188076064 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn APEDOJEAN.1188076064 Date: 2018.01.10 10:09:49 -05'00'</small></p> <p>Signature: .1188076064</p> <p>Date signed:</p>
<p>Authorizing Official Name: Douglas Perry Office: OCIO Deputy Chief Information Officer Phone: 301-713-9600 Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: right;">PERRY.DOU <small>Digitally signed by PERRY.DOUGLAS.A.1 365847270 Date: 2018.01.10 12:19:56 -05'00'</small></p> <p>Signature: GLAS.A.136</p> <p>Date signed: 5847270</p>	<p>Bureau Chief Privacy Officer Name: Mark Graff Office: OCIO Privacy Office Phone: 301-638-5658 Email: mark.graff@noaa.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p style="text-align: right;">GRAFF.MARK.HY <small>Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.11 08:55:50 -05'00'</small></p> <p>Signature: RUM.151444789</p> <p>Date signed: 2</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Friday, January 12, 2018 12:02 PM
To: Toland, Michael; Gitelman, Steve (Contractor); PrivacyAct
Cc: Mark Graff NOAA Federal; Ed Kearns NOAA Federal
Subject: NOAA 20 SORN in new template
Attachments: NOAA 20 SORN in new template_011218.docx

No updates made by the SARSAT system personnel. The only change is the latest breach routine use; the last amended SORN published 1 12 17 and it already had the volunteer routine use in it.

Let me know if you need me to send a list of SORNs submitted to you so far. I still have five to go, but at least two of those have no changes by the system personnel.

Thanks, Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Mark Graff - NOAA Federal

From: Mark Graff NOAA Federal
Sent: Tuesday, January 16, 2018 2:25 PM
To: Pua Kamaka NOAA Federal
Subject: Re: Discussion on Overview and Breach Response Notification Plan
Attachments: Summary Legal Experts Call 3.23.16.docx

Hi Pua

No, we don't have a slide deck on PA Processing exclusively. We rely almost entirely on DOJ's guidance here:

https://www.justice.gov/oip/blog/foia_update_foia_counselor_privacy_actfoia_conflict_or_harmony. The Legal Experts call we had on point (summary attached) is the closest we had to direct training on point. Do we need me to create a more specific training outline or would this overview suffice? I could easily break up this summary into a slide deck if that format works better

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
[\(301\) 628 5658](tel:3016285658) (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Tue, Jan 16, 2018 at 12:45 PM, Pua Kamaka NOAA Federal <pua.kamaka@noaa.gov> wrote:

Hi Mark,

Just following up on this. I don't recall whether or not you said you had training/slide deck specifically for the Privacy Act. My RA wanted me to follow up with you on this.

Thanks
Pua

On Mon, Aug 28, 2017 at 7:33 AM, Pua Kamaka NOAA Federal <pua.kamaka@noaa.gov> wrote:

Hi Mark,

Thanks for the slides. These are all FOIA based training, correct, or did I miss something? I was wondering if you had something more along the lines of FOIA vs. Privacy Act.

Pua

On Mon, Aug 28, 2017 at 3:18 AM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:

Hi Pua

No problem. Here are the slides from the NMFS training. We also used these as the basis for a subsequent training at NOS, which included a few quick reference guides specific to their office that may be helpful for you. All of these will soon be on the NOAA FOIA Webpage as well if they're not already there. (here: <https://sites.google.com/a/noaa.gov/foia/home>).

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
[\(301\) 628 5658](tel:(301)6285658) (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Fri, Aug 25, 2017 at 9:45 PM, Pua Kamaka NOAA Federal <pua.kamaka@noaa.gov> wrote:

Hi Mark,

Just following up on this, I was just pinged on this again by management. Would you be able to share the slides with me?

Thanks,
Pua

On Wed, Aug 9, 2017 at 12:39 PM, Pua Kamaka NOAA Federal <pua.kamaka@noaa.gov> wrote:

Hi Mark,

Could I please get the slide deck to look over? This keeps falling off my radar. I think if I have the slides to look over, I'll be able to get a better idea of what to propose to management.

thanks
Pua

On Wed, Jun 28, 2017 at 10:39 AM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:

Hi Pua,

Not a problem I'd love to schedule the best time for the training that works on your end. We recently had a training for NMFS that I'll send you the slide deck for. I'm going out of town for all of next week, so maybe we could touch base when I get back to try to firm up a schedule. I'll talk to you soon,

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
[\(301\) 628 5658](tel:(301)6285658) (O)

(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Wed, Jun 28, 2017 at 3:48 PM, Pua Kamaka NOAA Federal <pua.kamaka@noaa.gov> wrote:
Hi Mark,

Sorry I missed the boat on this one. I've been swamped with FOIAs and have been trying to keep my head above water. Are you still open to doing this training? Most folks in our region telework on Wednesdays and Fridays, so Tuesdays or Thursdays work best. Do you have the slide deck for me to look at, that way I can see who I need to loop in. Once I look over, can we set up some time to discuss via phone? I think that will be easier than going back and forth in emails.

Thanks
Pua

On Tue, May 9, 2017 at 4:44 AM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:
You bet, Pua

My best time would likely be in mid June, and if you want to just send me a Webinar Link, I'll send you a slide deck in the couple weeks or so. You would likely be the owner of the Webinar, and then you'd just transfer screen control to me once my portion starts. That way, we also could loop in GC or Lola if we wanted to split up the presentation. Does that sound good? Wednesdays seem to catch the most folks around here, so maybe tentatively June 14?

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
[\(301\) 628 5658](tel:3016285658) (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Fri, May 5, 2017 at 6:32 PM, Pua Kamaka NOAA Federal <pua.kamaka@noaa.gov> wrote:
Hi Mark,

Sorry it took me a while to get back to you, I was waiting on management. Our RA, Mike Tosatto, would like to take you up on your offer for training. Something along the lines of FOIA vs. Privacy Act. Webinar works for us as well. When you have time, we can discuss potential dates and times.

Thanks again for all your help

Pua

On Wed, Apr 26, 2017 at 11:34 AM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:
Hi Pua,

As you and I discussed, I've gone over the Privacy obligations with Mike Toland at DOC, as well as with Bogo in DOC/GC. No privacy incident was reported to N CIRT, and none would be necessary in this case. The PII submitted by the requester, and ultimately released, was in the public domain, and any subsequent disclosure would not then constitute a Privacy Incident under the DOC Breach Response and Notification Plan.

There are some best practices that may be helpful in three areas that you'd asked about. Specifically (1) first party access requests under the Privacy Act following the assertion of a Privacy Act Exemption after the requester's identity has been verified (2) the threshold of a Privacy Incident if there is a disclosure of Sensitive PII and (3) disclosure options at the time of the closure of a case, including publication codes, avoidance of inadvertent disclosures, and business interests sufficient under NAO 205 14 to preclude publication of records in FOIAOnline.

Let us know if this type of presentation would be helpful on your end, and if so, the best venue for us to provide it. Best,

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
[\(301\) 628 5658](tel:3016285658) (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

Multi-Track System Complex FOIA's versus "Unusual Circumstances"—

1. A complex request is one track for processing in a "multi-track" processing methodology. It is not required, but places the request in a slower track based on the volume and/or complexity of the records for first-in/first-out processing. 552(a)(6)(D). <https://www.justice.gov/oip/blog/foia-update-oip-guidance-guidelines-agency-preparation-and-submission-annual-foia-reports>. This is usually helpful in determining the realistic estimated completion time which is required to be communicated to the requester. <https://www.justice.gov/oip/blog/foia-post-2010-oip-guidance-importance-good-communication-foia-requesters>. These are best practices that allow quicker cases and expedited processing case to respectively be closed out first so they are not log-jammed behind complex cases in the First-in First-out queue.
2. Unusual circumstances, pursuant to 15 CFR 4.6(d)(2) exist with one of the following three situations and warrant the 10 day extension (552(a)(6)(B)) although different language, the basic criteria for "unusual circumstances" is very close to "exceptional circumstances" way round limit on fee after 20 day limit 552(a)(6)(C)(ii):
 - a. the component needs to search for and collect responsive records from a field office or other entity separate from the office processing the request;
 - b. the request involves a "voluminous" amount of records that must be located, compiled, and reviewed; or
 - c. the component needs to consult with another federal agency or two or more Department of Justice components that have a substantial interest in the responsive information.
 - i. "Exceptional Circumstances" is also able to consider refusal of requester to narrow scope.
3. As a general rule, many complex cases will also qualify for Unusual Circumstances, but these two are not mutually exclusive. For Example, Consultations are not always complex, but may take a long time due to inter-agency delays warranting unusual circumstances. Voluminous records may qualify for the complex track, but not require unusual circumstances extension due to simplicity of processing (Glomar Response, or clearly withheld in full).

The Glomar Response:

1. The Glomar Response is not, in and of itself, an exemption. Rather, it is a special type of response that is necessary in order to avoid disclosing exempt information when confirming or denying the existence of records itself would be exempt from disclosure. <https://www.justice.gov/oip/blog/foia-update-oip-guidance-privacy-glomarization>. The first judicially recognized use was when the CIA used this response in refusing to confirm or deny its ties to Howard Hughes' submarine retrieval ship, the Glomar Explorer. Thus, the first use of the response was in the national security context, *see Phillippi v. CIA*, 546 F.2d 1009, 1013 (D.C. Cir. 1976).

- a. As such, Glomar is a response premised on an underlying exemption. In most instances at NOAA, Glomar will be premised upon (b)(7)(C). Possible other exemptions (consider hypothetical 4 trying to find unit pricing, or hypothetical 7D to protect confidential sources like MLAT).
- b. The application of "Glomarization" in the privacy context is appropriate because disclosure of the mere fact that an individual is mentioned in an agency's law enforcement files carries a stigmatizing connotation, one certainly cognizable under FOIA Exemption 7(C), 5 U.S.C. § 552(b)(7)(C). *See, e.g., Fund for Constitutional Government v. National Archives & Records Service*, 656 F.2d 856, 865 (D.C. Cir. 1981). This is usually when a third party is asking for enforcement records regarding a named individual, and providing records even withheld in full acknowledges that a law enforcement action involved that individual.
- c. "Glomarization" approach under Exemption 7(C) is justified only when it is determined that there is a cognizable privacy interest at stake and that there is insufficient public interest in disclosure to outweigh it. *See, e.g., Common Cause v. National Archives & Records Service*, 628 F.2d 179, 184-86 (D.C. Cir. 1980)
- d. Exceptions:
 - i. The named individual in the law enforcement record is deceased. *See, e.g., Tigar & Buffone v. United States Department of Justice*, Civil No. 80-2382, slip op. at 9-10 (D.D.C. Sept. 30, 1983).
 - ii. The named individual has provided a privacy waiver. *See Perry v. FBI*, 759 F.2d 1271, 1276 (7th Cir. 1985)
 - iii. If the federal government has officially confirmed the involvement of the individual in the investigation. *See, e.g., Heimerle v. United States Department of Justice*, Civil No. 83-1944-(MEL), slip op. at 5 (S.D.N.Y. Mar. 4, 1985).
- e. Even in these circumstances, the privacy balancing inquiry must be conducted, and sometimes misconduct by high-ranking officials qualifies for 7(C) to not apply and thus not the Glomar response that exemption would require.
- f. The search for records must still be conducted, and the balancing inquiry determined, and then the decision on whether or not to apply the Glomar response. *See Gilday v. United States Department of Justice*, Civil No. 85-292, slip op. at 5-10 (D.D.C. July 23, 1985).

Privacy and FOIA Exemption Handoff:

- g. The Privacy Act generally allows individuals to have access to records regarding themselves pursuant to 5 USC 552a(d)(1). This is called an "Access" request, and is usually an individual requesting records contained in a System of Records searchable by a unique identifier that allows retrieval of records pertaining to them. It is a separate analysis, and must dovetail into a FOIA Exemption review, if applicable in a 1st party access request. *See, <https://www.justice.gov/opcl/individuals-right-access>.*

- i. An individual's access request for his own record maintained in a system of records should be processed under both the Privacy Act and the FOIA, regardless of the statute(s) cited. See 5 U.S.C. § 552a(t)(1) and (2) (prohibiting reliance on FOIA exemptions to withhold under Privacy Act, and vice versa). More specifically, pursuant to Shapiro v. DEA, 762 F.2d 611, 612 (7th Cir. 1985) "Congress intends that the courts construe the Privacy Act and the Freedom of Information Act separately and independently so that exemption from disclosure under the Privacy Act does not exempt disclosure under the Freedom of Information Act, and vice versa."
- ii. What this means is that "Even though information may be withheld under the [Privacy Act], the inquiry does not end. The agency must also process requests under the FOIA, since the agency may not rely upon an exemption under the [Privacy Act] to justify nondisclosure of records that would otherwise be accessible under the FOIA. (Harvey v. DOJ, No. 92-176-BLG slip op. at 8 (D. Mont. Jan. 1996).
- iii. I was the lead in the litigation team handling the following case: Gonzales & Gonzales Bonds & Ins. Agency, Inc. v. DHS, 913 F.Supp.2d 865, 868 n.3 (N.D. Cal. 2012) (noting DHS' error in responding to plaintiff's FOIA requests under the Privacy Act, and stating that "the FOIA and the Privacy Act are distinct mechanisms for obtaining government information, and it is legal error to conflate them".
 1. If no Privacy Act Exemption applies: FOIA cannot be invoked to exempt the records, and they are disclosed pursuant to (d)(1) of the Privacy Act. This is why SORNs with PA Exemptions exist so that an exemption to the PA can be asserted, and then ordinary FOIA responses continue. Otherwise, Viotti v. Air Force, 902 F. Supp. 1331, 1336-37 (D. Colo. 1995) ("If the records are accessible under the Privacy Act, the exemptions from disclosure in the FOIA are inapplicable." Please let me know if you are maintaining records on an individual outside of an approved PIA/SORN covered system of records.
 2. Even if a Privacy Act Exemption applies, then the FOIA must be used for segregation of the record for releasability. Martin, 819 F.2d at 1184 ("[I]f a Privacy Act exemption but not a FOIA exemption applies, the documents must be released under FOIA.").
- iv. PA Exemptions cover global record access. They are not used for reasonable segregation. That is the role of the FOIA, but only after the PA Exemption is determined to apply.
- h. However, the carte blanche access to records regarding an individual has its own exemptions. The most common are (k)(2), (j)(2), (k)(5),(k)(6), and (d)(5). (k)(2) and (j)(2) are sister exemptions, one for administrative (non-criminal) law enforcement proceedings (including adverse employment actions see, Menchu v. HHS, 965 F. Supp. 2d 1238, 1248 (D. Or. 2013)),

and the other exclusively for criminal proceedings. (k)(5) is primarily for hiring purposes (requires express promise of confidentiality Viotti v. Air Force, 902 F. Supp. 1331, 1336 (D. Colo. 1995)), (k)(6) is for testing and examination material for appointment or promotion to Federal Employment, and (d)(5) is primarily for civil litigation-related records with a clear congressional intent to exclude civil litigation files from access under subsection (d)(1). See 120 Cong. Rec. 36,959-60 (1974).

- i. This means you must be extraordinarily careful what you place into a system of record regarding an individual, especially if you do not know the SORN Exemption listing, and whether or not that person could gain access to the records due to a lack of Exemptions to be asserted (see, e.g., Voelker v. IRS, holding that all information pertaining to the individual, including some confidential informant material, was disclosable, as no Privacy Exemption applied to that system of records. 646 F.2d 332, 333-35 (8th Cir. 1981).

FOIA Tasker Memo (Kim)

1. GC NLO (No Legal Objection) as opposed to GC Review.

Rohit Munjal - NOAA Affiliate

From: Rohit Munjal NOAA Affiliate
Sent: Friday, January 19, 2018 8:58 AM
To: Sarah Brabson NOAA Federal; Mark Graff NOAA Federal
Cc: Mark Mohs NOAA Federal; John D. Parker NOAA Federal
Subject: Re: NOAA6301 PTA/PIA for Signatures
Attachments: NOAA6301_PIA_Annual_Review_Certification_2018.pdf; NOAA6301_PTA_2018.pdf; NOAA6301_PIA_2018.pdf

Hi Sarah & Mark (Graff),

Please find attached the AO-signed PTA, PIA and also the Annual PIA Review Certification form. Let me know for any questions or concerns.

Thank you,

Rohit Munjal

ISSO (Cont.) - IT Branch, Business Mgmt. Division
NCCOS | NOAA National Ocean Service
240-533-0289 | rohit.munjal@noaa.gov

On Wed, Jan 17, 2018 at 2:48 PM, John D. Parker NOAA Federal <john.d.parker@noaa.gov> wrote:

Hi Rohit,

I have attached the signed PDF files. Please provide, if you haven't already, the MS Word files used to create these specific PDF versions.

My apologies for the delay in getting this back to you.

Thanks,

John

--

John D. Parker, CISSP, CISA <John.D.Parker@noaa.gov>
NOS IT Security Officer
DOC/NOAA/NOS IMO [240-533-0832](tel:240-533-0832) (office) (b)(6) (mobile)
Email NOS IT security inquires: NOS.ITSP@noaa.gov

On 1/16/2018 8:17 AM, Rohit Munjal NOAA Affiliate wrote:

Morning John,

Just chasing on my last few mails.
If you could please review and sign this today.

Thank you,

Rohit Munjal
ISSO (Cont.) - IT Branch, Business Mgmt. Division
NCCOS | NOAA National Ocean Service
[240-533-0289](tel:240-533-0289) | rohit.munjal@noaa.gov

Forwarded message

From: **Rohit Munjal - NOAA Affiliate** <rohit.munjal@noaa.gov>
Date: Wed, Jan 10, 2018 at 4:15 PM
Subject: NOAA6301 PTA/PIA for Signatures
To: "John D. Parker NOAA Federal" <john.d.parker@noaa.gov>
Cc: Mark Mohs NOAA Federal <mark.mohs@noaa.gov>

Hi John,

Can you please review and sign these documents which will then help me route it to Steve and Mark Graff for signatures.

Sarah is following up on these too.

Thank you,

Rohit Munjal
ISSO (Cont.) - IT Branch, Business Mgmt. Division
NCCOS | NOAA National Ocean Service
[240-533-0289](tel:240-533-0289) | rohit.munjal@noaa.gov

Forwarded message

From: **Rohit Munjal - NOAA Affiliate** <rohit.munjal@noaa.gov>
Date: Mon, Jan 8, 2018 at 2:19 PM
Subject: NOAA6301 Re certification of PTA/PIA
To: "John D. Parker NOAA Federal" <john.d.parker@noaa.gov>
Cc: Mark Mohs NOAA Federal <mark.mohs@noaa.gov>

Hi John,

I updated the *PIA Annual Review Certification* based on the template Sarah sent out this morning, so re-sending this mail with the updated document.

Thank you,

Rohit Munjal
ISSO (Cont.) - IT Branch, Business Mgmt. Division
NCCOS | NOAA National Ocean Service
[240-533-0289](tel:240-533-0289) | rohit.munjal@noaa.gov

Forwarded message

From: **Rohit Munjal - NOAA Affiliate** <rohit.munjal@noaa.gov>
Date: Fri, Jan 5, 2018 at 9:57 AM
Subject: NOAA6301 Re certification of PTA/PIA

To: "John D. Parker NOAA Federal" <john.d.parker@noaa.gov>

Cc: Mark Mohs NOAA Federal <mark.mohs@noaa.gov>

Hi John,

Happy New Year!

Please find attached the PTA and PIA for your signatures. As soon as you sign it, I will route it for signatures from Steve and Mark Graff.

I'm also attaching herewith the PIA Annual Review Certification 2018, in case you want to review it.

Please let me know for any questions/comments.

Thank you,

Rohit Munjal
ISSO (Cont.) - IT Branch, Business Mgmt. Division
NCCOS | NOAA National Ocean Service
[240-533-0289](tel:240-533-0289) | rohit.munjal@noaa.gov

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NCCOS Research Support System

FISMA Name/ID (if different): NOAA6301

Name of IT System/ Program Owner: National Centers for Coastal Ocean Science

Name of Information System Security Officer: Rohit Munjal

Name of Authorizing Official(s): Steven Thur / Cheryl Marlin

Date of Last PIA Compliance Review Board (CRB): 3/16/2017

(This date must be within three (3) years.)

Date of PIA Review: 1/8/2018

Name of Reviewer: Rohit Munjal

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: MUNJAL.ROHIT.1500946381 Digitally signed by MUNJAL.ROHIT.1500946381
Date: 2018.01.08 12:19:26 05'00'

Date of Privacy Act (PA) Review: _____

Name of Reviewer: _____

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: _____

Date of BCPO Review: _____

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): _____

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: _____

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Friday, January 19, 2018 12:24 PM
To: Toland, Michael; Gitelman, Steve (Contractor); PrivacyAct
Cc: Mark Graff NOAA Federal; Ed Kearns NOAA Federal
Subject: NOAA 22 SORN in new template
Attachments: NOAA 22 SORN in new template_011618.docx

The only changes are contact information and the two latest routine uses.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Tuesday, January 23, 2018 8:36 AM
To: Mark Graff NOAA Federal
Cc: Rohit Munjal NOAA Affiliate
Subject: NOAA6301 certification docs for signature; SAR is in PIA file
Attachments: NOAA6301_PIA_2018 v2.pdf; NOAA6301_PIA_Annual_Review_Certification_2018.pdf; NOAA6301_PTA_2018 v2.pdf

Mark, attached are the certification docs for your signature and the SAR zipfile is in the PIA folder. I asked Rohit about the SC, SI and AC weaknesses, if most have been addressed, since this SAR was from last March. He had thought he might be able to send a draft, but this is what we have. Overall risk is/was Moderate.

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751

Ce (b)(6)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NCCOS Research Support System

FISMA Name/ID (if different): NOAA6301

Name of IT System/ Program Owner: National Centers for Coastal Ocean Science

Name of Information System Security Officer: Rohit Munjal

Name of Authorizing Official(s): Steven Thur / Cheryl Marlin

Date of Last PIA Compliance Review Board (CRB): 3/16/2017

(This date must be within three (3) years.)

Date of PIA Review: 1/8/2018

Name of Reviewer: Rohit Munjal

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: MUNJAL.ROHIT.1500946381 Digitally signed by MUNJAL.ROHIT.1500946381
Date: 2018.01.08 12:19:26 05'00'

Date of Privacy Act (PA) Review: _____

Name of Reviewer: _____

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: _____

Date of BCPO Review: _____

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): _____

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: _____

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Zachary Goldstein - NOAA Federal

From: Zachary Goldstein NOAA Federal
Sent: Tuesday, January 23, 2018 9:38 AM
To: Jean Apedo NOAA Federal
Cc: Ann Madden NOAA Federal; Justin May NOAA Affiliate; Mark Graff NOAA Federal
Subject: Re: FW: NOAA0500 PIA and PTA
Attachments: NOAA0500 PIA_17Jan18 ISSO_Signed.pdf; NOAA0500_PTA_Updated_14Dec17 LBH (2).pdf

Jean,

The NOAA0500 PTA and PIA with my digital signature are attached.

(b)(5)

[Mark, feel free to weigh in on the questions]

Regards,
Zach

On Thu, Jan 18, 2018 at 6:29 AM, Jean Apedo NOAA Federal <jean.apedo@noaa.gov> wrote:

Good morning Zach,

Please find attached NOAA0500 PTA and PIA for your review. The system owner, the ISSO, the privacy office and I have reviewed the documents and are ready for your approval.

Thank you.

From: Justin May - NOAA Federal [mailto:justin.may@noaa.gov]
Sent: Wednesday, January 17, 2018 8:11 PM
To: Jean Apedo - NOAA Federal
Cc: Hadona Diep - NOAA Affiliate; Sarah Brabson - NOAA Federal
Subject: NOAA0500 PIA - Updated

Zachary G. Goldstein

Chief Information Officer and Director, High Performance Computing and Communications
National Oceanic and Atmospheric Administration

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Mark Graff - NOAA Federal

From: Mark Graff NOAA Federal
Sent: Tuesday, January 23, 2018 10:19 AM
To: Sarah Brabson NOAA Federal
Subject: Re: NOAA6301 certification docs for signature; SAR is in PIA file
Attachments: NOAA6301_PIA_Annual_Review_Certification_2018 mhg.pdf; NOAA6301_PTA_2018 v2 mhg.pdf; NOAA6301_PIA_2018 v3 mhg.pdf

Sure

Attached are all three, signed.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Tue, Jan 23, 2018 at 10:10 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
Mark, can you please sign? thx

On Tue, Jan 23, 2018 at 8:57 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
Here's the corrected PIA. The changes that were in there were from the 2017 12b response, for planned changes.

Also Rohit says the weaknesses for those three families have been addressed.

On Tue, Jan 23, 2018 at 8:45 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
It was my error in not deleting the "other changes" text. As you can see, the "no changes creating privacy risks" was checked. I will send you another copy.

On Tue, Jan 23, 2018 at 8:42 AM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:
Is the change listed in Sec. 1.1 from last year, or is that a new change for this year? If it is a change from this year, how are we not required to conduct a CRB?

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Tue, Jan 23, 2018 at 8:35 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
Mark, attached are the certification docs for your signature and the SAR zipfile is in the PIA folder. I asked Rohit about the SC, SI and AC weaknesses, if most have been addressed, since this SAR was from last March. He had thought he might be able to send a draft, but this is what we have. Overall risk is/was Moderate.

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division

Office [301 628 5751](tel:3016285751)

Ce (b)(6)

**U.S. Department of Commerce
NOAA**



**Privacy Impact Assessment
for the
National Centers for Coastal Ocean Science (NCCOS) Research
Support System (NOAA6301)**

Reviewed by: _____, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301)

Unique Project Identifier: 006-00-02-00-01-0511-00

Introduction: System Description

The NOAA6301 NCCOS Research Support System provides the network infrastructure, hardware and software necessary to enable the mission of NCCOS, the organization. NCCOS's mission is to provide coastal managers with scientific information and tools needed to balance society's environmental, social, and economic goals.

NCCOS is passionate about supporting NOAA's environmental and economic missions by providing valuable scientific information to its constituents. NCCOS's fundamental principles are:

- To deliver high quality science in a timely and consistent manner using productive and strong partnerships.
- To develop and maintain relevant research, long term data collection and analyses, and forecasting capabilities in support of its customers, stakeholders, and partners.
- To build capacity in the private, local, state, and tribal sectors by transferring technology and providing technical assistance and knowledge to its customers and partners.
- To conduct the anticipatory science necessary to manage potential impacts of multiple stressors on coastal ecosystems.

The NOAA6301 system:

- provides support to the program areas which are responsible for conducting research in the areas of marine bio-toxins; eco-toxicology; forensics; biotechnology; marine mammal stranding and necropsies; risk analysis; DNA sequencing; and marine related viruses and pathogens;
- provides an operational environment supporting the mission and staff of the program offices located on the Silver Spring Metro Center Campus - NCCOS Head Quarters (HQ), Center for Sponsored Coastal Ocean Research (CSCOR), and Center for Coastal Monitoring and Assessment (CCMA); Beaufort, NC - Center for Coastal Fisheries and Habitat Research (CCFHR); Charleston, SC - Center for Coastal Environmental Health and Biomolecular Research (CCEHBR) and Hollings Marine Laboratory (HML); and Oxford, MD - Cooperative Oxford Laboratory (COL);
- provides all resources related to data management, electronic file, COTS, printing, computer and software, field data acquisition, backup and restoration, LAN, helpdesk, specialty applications for GIS and statistical analysis, moderate programming, Web design and Web product delivery, video conferencing, and other media support services; and
- Provides continued service to the local area network (LAN) connections for non-SSMC locations.

In addition to the general purposes office automation support (file/printer sharing, application

hosting, collaboration, etc.) provided by NOAA6301, the system provides help desk services and supports a number of web sites and internal minor applications, one of which stores PII for the purpose of conducting the external grant review process as defined within the NOAA Grants Online System, (FISMA system ID, NOAA1101, PIA signed 7/6/2017). Grant applications are downloaded from Grants Online on a case by case basis, for review. They are stored by opportunity or grant number.

As detailed in the information sharing section below, NCCOS gathers and stores PII related to employees and contractors for Human Resource-related issues such as the hiring process as well as workforce planning, COOP Operations, and documentation. The NCCOS collects BII during the pre and post activities associated with the acquisition and management of contracts.

Information Sharing

NOAA6301 NCCOS Research Support System General Support System (GSS) collects and collects and stores limited PII, specifically, names, telephone numbers and email addresses (voluntarily submitted by staff, partners, volunteers, and government and non-government collaborators) to facilitate internal and external communications to facilitate business and collaborative functions. This is not a central collection, but rather separated by function or individual project or person.

NOAA6301 is a general support system for NCCOS and stores information about individuals during the application and hiring of (electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase), including standard HR information (such as Travel authorization and vouchers, passports and international travel forms (completed by the employee through the travel portal), information for security badging process (contact information only the employee completed the badge application on paper forms, which are taken to the NOAA Office of Security), and performance appraisal ranking).

NCCOS' employee data is collected, stored and maintained for internal COOP, Human Resources, and workforce planning purposes (federal employee/contractor).

NCCOS collects BII during the pre and post activities associated with the acquisition and management of contracts. The storage is in the form of PDF forms or MS Word documents. There is no major application or database used to collect or store BII or employee PII information. NCCOS does not have a separate HR division since NCCOS utilizes the NOAA Workforce Management Office.

With exception of the CSCOR Review Application, all information is stored on supervisors' and acquisition managers' restricted access file storage available only to the specific employee(s). Access is restricted to those on a need to know basis, by permissions settings and/or passwords. The data is access controlled when on a supervisor's desktop machine or file share; if stored on a supervisor's laptop, the data is encrypted since all mobile devices have full encryption. The CSCOR Review Application although managed by NCCOS, is hosted by an NOAA6001 NOS Enterprise Services server and is restricted by username and password.

CSCOR Review Application Information in identifying form is made available by NOAA Grants Online (FISMA system ID, NOAA1101, PIA signed 7/6/2017) to NCCOS to accomplish Independent Individual Merit Reviews supporting the NOAA Grants Online system and process.

Information about the NOAA Grants Program may be found at: <http://www.corporateservices.noaa.gov/~grantsonline/index.html>. This is a non-public system. Information extracted from NOAA Grants Online to support the Independent Individual Merit Reviews is temporarily stored to facilitate the review process lifecycle. This information can include any general personal information and work related information. Although it is not the intent to extract PII information from the NOAA Grants Online system, it is possible the information could contain the Employer Identification Number (EIN). The EIN is a non-mandatory field which may be populated on the grants information made available by federal forms not managed by NCCOS. The NCCOS information system does not collect this identifying information directly.

A citation of the legal authority to collect PII and/or BII

The general legislation supporting the system is 5 U.S.C.301, one of the statutes concerning government organization and employees.

Additional authorities from DEPT-2, Accounts Receivable: H.R. 4613 (97th): Debt Collection Act of 1982, a bill to increase the efficiency of Government-wide efforts to collect debts owed the United States and to provide additional procedures for the collection of debts owed the United States and 5 U.S.C. 5701-09; 31 U.S.C. 951-953, 4 CFR 102.4, FPMR 101-7; Treasury Fiscal Requirements Manual.

Additional authorities from GSA/GOVT-9, System for Award Management: Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204, and 40 U.S.C. 121(c), Regulations by Administrator. For the Entity Management functional area of Systems Award Management, the authorities for collecting the information and maintaining the system are the Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204 and 2 CFR, Subtitle A, Chapter I, and Part 25, as well as 40 U.S.C. 121(c). For the exclusions portion of the Performance Information functional area, the authorities for collecting the information and maintaining the system are FAR Subparts 9.4 and 28.2, Executive Order 12549 (February 18, 1986), Executive Order 12689 (August 16, 1989).

The Federal Information Processing Standard (FIPS) 199 security impact category for NOAA6301 is moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- This is a new information system.
- This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	

b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

X This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID	X**	f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport	x	k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					
** Same data element checked for Grants Online, as in the NOAA1101 PIA.					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	x	o. Medical Information	
d. Gender		j. Telephone Number	x	p. Military Service	
e. Age		k. Email Address	x	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	x	d. Telephone Number	x	g. Salary	x
b. Job Title	x	e. Email Address	x	h. Work History	x
c. Work Address	x	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify): NCCOS does not capture photographs for badging since it is performed and stored by the NOAA badging office of security.					

System Administration/Audit Data (SAAD)					
a. User ID	x	c. Date/Time of Access	x	e. ID Files Accessed	
b. IP Address	x	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)
Pre and Post Acquisition. This BII information would be obtained and utilized during the pre acquisition obtained through deliverable BIDS package and contain specific company information. BII information would be maintained on specific secure network folders during the execution of awarded contract and other information from companies not receiving awards would be deleted, when appropriate. This information is protected under 41 USC 253, the FOIA Exemption 3 statute for contract proposals and collections associated with them.

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	x	Hard Copy: Mail/Fax	x	Online	
Telephone		Email	x		
Other (specify):					

Government Sources					
Within the Bureau	x	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify): NOAA Grants Online http://www.corporateservices.noaa.gov/~grantsonline/index.html .					

Non-government Sources					
Public Organizations	x	Private Sector	x	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): NCCOS does not acquire PII from other non-government sources other than associated through formal partnership agreements and for the purpose of facilities safety, security, and COOP. Other non-government sources would be only for BII associated with Pre/Post Acquisition Sensitive Information obtained through delivered bids on NCCOS Acquisitions.					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)					
Smart Cards		Biometrics			
Caller-ID		Personal Identity Verification (PIV) Cards			
Other (specify):					

x	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
---	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

x	There are not any IT system supported activities which raise privacy risks/concerns.		
---	--------------------------------------------------------------------------------------	--	--

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	x
For administrative matters	x	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Collected BII would be associated with determine qualification/eligibility for open acquisitions. PII would be collected for administrative actions, for HR and Workforce management. PII/BII: NOAA Grants Online - Grant Merit Reviews			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

In general, the laws that created the various NOS programs, specifically NCCOS, include provisions for the program to accomplish a mission. The mission may involve partnerships and educating the public. The collection and storage of information is part of accomplishing the legislated mission of the NCCOS, the NOS, and NOAA (members of the public and federal employees).

NOAA6301 stores PII on an ad hoc basis as part of the application and hiring of employees, including electronic copies of resumes and the processing of HR data about employees including hiring ranking. This information is stored temporarily during the hiring phase, as well as standard HR information such as travel authorization and vouchers, passports and international travel forms, information for the security badging process (name, work email address and work telephone number, and performance appraisal ranking).

NCCOS stores limited PII and potentially an EIN (BII), for grant review only, on an ad hoc basis about individuals or entities that are providing information in support of a grant application submitted through NOAA Grants Online which is retained for the review process lifecycle only.

BII Pre and Post Acquisition. This BII information would be obtained and utilized during the pre-acquisition obtained through deliverable BIDS package and contain specific company information. BII information would be maintained on specific secure network folders during the execution of awarded contract and other information from companies not receiving awards would be deleted, when appropriate.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	x		
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	-----------------------------------------------

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NOAA6301 connects to the NOS Line Office information system NOAA6001 and other NOAA information systems for VPN, Security and Network Operations. NCCOS established security permissions based on NOS Active Directory Network account (enforced 2FA when possible), restrictions in firewall ACL and security permissions on specific network folders where documentation is stored.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. (*Check all that apply.*)

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. (*Check all that apply.*)

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
x	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://coastalscience.noaa.gov/contact/privacy . A PAS for Grants Online has been finalized and has been posted at: https://grantsonline.rdc.noaa.gov/	
x	Yes, notice is provided by other means.	Specify how: (Specific to PII) Verbally by administrative appointed staff or supervisor OR this address is referenced: https://coastalscience.noaa.gov/contact/privacy . This is an NOS standard privacy policy and not specific to NCCOS. BII is provided for the purpose of acquisition consideration only through government managed acquisition processes and forms only. NCCOS does not generate or maintain additional forms or processes to support acquisition activities. BII provided within NOAA Grants Online utilized within the CSCOR Review Application is managed through the NOAA Grants Online application only.

	No, notice is not provided.	Specify why not:
--	-----------------------------	------------------

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

x	Yes, individuals have an opportunity to decline to provide PII/BII.	<p>Specify how: PII: No information collected is mandatory. Individuals are verbally told by administrative appointed staff or supervisor that they can decline or individuals are directed to review the privacy policy at this address: https://coastalscience.noaa.gov/contact/privacy, where it is stated all information collected is voluntary. This is an NOS standard privacy policy and not specific to NCCOS.</p> <p>BII provided for acquisition consideration is not mandatory. However, declining to provide the information necessary to evaluate them for an acquisition could result in non-award.</p> <p>PII provided within NOAA Grants Online, utilized within the CSCOR Review Application, is managed through the NOAA Grants Online application only. Completion of the Grants Online application would be needed for award consideration.</p>
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	<p>Specify how: Applicants for positions are providing their personal information on a voluntary basis through their resumes. There is only one use for this information. The employment application contains the Privacy Act notice. Applicants have the opportunity to consent to only particular uses of their PII, in writing, to the HR representative or their supervisor, but it may affect the overall processing of their employment.</p> <p>For ongoing employee business, such as travel, there is only one specific use for each PII collection.</p> <p>BII is submitted for a specific purpose which consent is implied with the submittal of the package. BII provided within NOAA Grants Online utilized within the CSCOR Review Application is managed through the NOAA Grants Online application only.</p>
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

x	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: (Specific to PII) NCCOS employees can contact HR staff or the federal employee personnel page to update their information, as they are informed as part of new employee
---	-----------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>orientation.</p> <p>BII is provided for the purpose of acquisition consideration through government managed acquisition processes and forms only. NCCOS does not generate or maintain additional forms or processes to support acquisition activities. BII provided within NOAA Grants Online utilized within the CSCOR Review Application is managed through the NOAA Grants Online application only.</p> <p>Regarding contracts and grants that are in process or awarded, the applicants or awardees would send updates to the stated NOAA contact.</p>
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to the PII/BII is restricted to authorized personnel only.
x	<p>Access to the PII/BII is being monitored, tracked, or recorded.</p> <p>Explanation: With exception to the CSCOR Review Application, access to storage folders are restricted by ACL and since PII/BII is not centralized in a database it cannot be easily monitored for access. The CSCOR Review Application has a database which is monitored, tracked and recorded.</p>
x	<p>The information is secured in accordance with FISMA requirements.</p> <p>Provide date of most recent Assessment and Authorization (A&A): 3/23/2017. Next one is no later than 3/22/2018.</p> <p><input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.</p>
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
x	Other (specify): All appropriate contractors and contract clauses include non-disclosure, but not all federal employees sign a confidentiality agreement or non-disclosure agreement.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

All information is stored within the accredited boundaries of NOAA6301 in network data shares controlled by established permission based on the organizational, project, or employee access rights. Any access to specific restricted files or folders must be requested through an access change request which is reviewed and documented by the NOAA6301 Information System Security Officer for authorization and mission ‘need-to-know’ requirement prior to implementation. Least privilege is implemented through file share permissions to ensure privacy and open only to those demonstrating a “need to know.”

Any PII information which is transmitted electronically must follow the federal government and NOAA standard procedure of secure packaging such as utilization of Department of Commerce (DOC) Accellion for encryption in transit.

NCCOS implements security controls listed in NIST Special Publication 800-53 R4 required for a moderate system. In compliance with NIST Special Publication 800-53 rev 4, NCCOS has a security program, with performance measures and goals, in order to complete continuous monitoring activities, which include annual security control reviews, quarterly vulnerability scanning, monthly review of security access control list, weekly review of audit logs, handling of access change requests and change control board activities. The risk assessment includes the possible threats and vulnerability to the confidentiality, integrity, and availability of mission and sensitive PII data along with the countermeasures.

The controls supporting the use of Microsoft Azure FedRamp approved system as a customer are in place in NOAA6301. There are currently Web applications, with no PII, hosted on Microsoft Azure. As noted in Section 12.2, we are transitioning CSCOR to Azure prior to December 2018. The same sharing controls that are in place currently for CSCOR will apply when it is moved to Azure.

Every year the IT system undergoes a thorough continuous monitoring for the assessment and authorization (A&A) process that is performed by an independent. The A&A process ensures that the security plan and operational, management, and technical controls meet Department of Commerce (DOC) and NOAA guidelines for continued operation.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C.

§ 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

x	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i> : COMMERCE/DEPT-18 - Employees Personnel Files Not Covered By Notices of Other Agencies; DEPT-2 , Accounts Receivable; GSA/GOVT-9 , System for Award Management.
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created:

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

x	<p>There is an approved record control schedule. Provide the name of the record control schedule: Chapters 1601 and 1607 of NOAA’s Records Schedules, http://www.corporateservices.noaa.gov/audit/records_management/schedules/, provide supplemental record retention guidance for the NCCOS Research Support System. Chapter 1601 pertains to general administration for the National Ocean Service and Chapter 1607 pertains to specific records managed by the NCCOS Research Support System. Specifically, 1601-02 Grants Working Files (N1-370-02-5), 1601-04 Electronic Copies (N1-370-02-5), 1601-05 NOS Annual Operating Plan (AOP) Information Tracking Systems (N1-370-04-4), 1609-06 in the NOAA Disposition Handbook and 1607-04 Program Funding Database.</p> <p>The retention period for these records is guided by the General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the federal government. In accordance with GRS 20, item 3, electronic versions of records scheduled for disposal may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. In accordance with GRS 20, item 3, the data is presently being retained indefinitely.</p> <p>For NCCOS administrative PII data, the records would be covered under the following NARA general records schedules: GRS 2 – payroll and pay administrative records GRS 20 – electronic records GRS 23 – records common to most offices within agencies</p> <p>NCCOS’ contact information (contractor and partner) is collected to provide a means for the Office of Coast Survey to communicate and respond to needs and requests. This data would be retained as long as the individual continued to request contact and information. It is technologically possible to delete information at the request of the individual. There is no scheduled records retention for this information.</p>
	<p>No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:</p>
x	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	x	Overwriting	x
Degaussing	x	Deleting	x
Other (specify): Compliant sanitization methods.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. (Check all that apply.)

X	Identifiability	Provide explanation: Evaluated how easily PII could be used to identify a specific individual. Based on contact information, individuals can be identified.
X	Quantity of PII	Provide explanation: Considered how many individuals can be identified from the PII. The PII is only temporarily stored for a limited amount of individuals, therefore reducing the breach impact.
X	Data Field Sensitivity	Provide explanation: Data fields are limited and only used when absolutely required. SSN is not one of these data fields. EIN is a field which can be populated within NOAA Grants Online, however, is not required and is not utilized. This field will not be extracted from NOAA Grants Online in the future revision of the CSCOR Review Application.
X	Context of Use	Provide explanation: Evaluated the context of use—the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated. The use of the PII is restricted to specific individuals, stored for a limited amount of time and is not utilized in more than one way reducing the impact.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: The PII is only temporarily stored in a protected location for a limited amount of individuals, therefore reducing the breach impact.
X	Other:	Provide explanation: The loss of a single individual's PII would have an impact on that individual through possible identify theft and NCCOS as a government identity BUT it would not have an impact on the NCCOS mission or have a serious impact on reputation.

Section 12: Analysis


12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
x	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

x	Yes, the conduct of this PIA results in required technology changes. Explanation: NOAA6301 is utilizing Azure SQL in the Microsoft Azure PaaS environment to store web application data. Although there is currently no PII/BII associated with the web/apps and transitioning to the new environment is not expected prior to December 2018, controls are already in place to encrypt at rest data through the Azure SQL TDE capability: https://msdn.microsoft.com/en-us/library/dn948096.aspx . All SQL databases will have this feature turned on at inception and it will remain on. This storage is currently planned only for CSCOR and will further secure the CSCOR Review Application Database.
	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

<p>Information System Security Officer or System Owner Name: Rohit Munjal Office: NOS/NCCOS Phone: 240-533-0289 Email: Rohit.Munjal@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: right;">MUNJAL.ROHIT.1500 Digitally signed by MUNJAL.ROHIT.1500946381 Date: 2018.01.05 09:46:15 -05'00'</p> <p>Signature: 946381</p> <p>Date signed:</p>	<p>Information Technology Security Officer Name: John D. Parker Office: NOS Phone: 240-533-0832 Email: John.D.parker@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: right;">PARKERJOHN.D.13658359 Digitally signed by PARKERJOHN.D.1365835914 Date: 2018.01.17 14:46:55 -05'00'</p> <p>Signature: 14</p> <p>Date signed:</p>
<p>Authorizing Official Name: Steven Thur Office: NOS/NCCOS Phone: 240-533-0146 Email: Steven.Thur@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: right;"> Digitally signed by THUR.STEVEN.M.1365841299 Date: 2018.01.19 07:50:30 -05'00'</p> <p>Signature:</p> <p>Date signed:</p>	<p>Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p style="text-align: right;">GRAFF.MARK. Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c U.S., o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447 892 Date: 2018.01.23 10:12:39 -05'00'</p> <p>Signature: HYRUM.15144</p> <p>Date signed: 47892</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NCCOS Research Support System

FISMA Name/ID (if different): NOAA6301

Name of IT System/ Program Owner: National Centers for Coastal Ocean Science

Name of Information System Security Officer: Rohit Munjal

Name of Authorizing Official(s): Steven Thur / Cheryl Marlin

Date of Last PIA Compliance Review Board (CRB): 3/16/2017

(This date must be within three (3) years.)

Date of PIA Review: 1/8/2018

Name of Reviewer: Rohit Munjal

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: MUNJAL.ROHIT.1500946381 Digitally signed by MUNJAL.ROHIT.1500946381
Date: 2018.01.08 12:19:26 05'00'

Date of Privacy Act (PA) Review: _____

Name of Reviewer: _____

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: _____

Date of BCPO Review: 1/23/18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF MARK HYRUM 1514447892
DN c US, o U S Government, ou DoD, ou PKI,
ou OTHER, cn GRAFF MARK HYRUM 1514447892
Date 2018 01 23 10 17 27 -05'00'

**U.S. Department of Commerce
NOAA**



**Privacy Threshold Analysis
for the
National Centers for Coastal Ocean Science (NCCOS) Research
Support System (NOAA6301)**

U.S. Department of Commerce Privacy Threshold Analysis
NOAA/National Centers for Coastal Ocean Science (NCCOS) Research
Support System (NOAA6301)

Unique Project Identifier: 006-00-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: The NOAA6301 National Centers for Coastal Ocean Science (NCCOS) Research Support System provides the network infrastructure, hardware and software necessary to enable the mission of NCCOS, the organization. NCCOS's mission is to provide coastal managers with scientific information and tools needed to balance society's environmental, social, and economic goals.

NCCOS is passionate about supporting NOAA's environmental and economic missions by providing valuable scientific information to its constituents. NCCOS's fundamental principles are:

- To deliver high quality science in a timely and consistent manner using productive and strong partnerships.
- To develop and maintain relevant research, long term data collection and analyses, and forecasting capabilities in support of its customers, stakeholders, and partners.
- To build capacity in the private, local, state, and tribal sectors by transferring technology and providing technical assistance and knowledge to its customers and partners.
- To conduct the anticipatory science necessary to manage potential impacts of multiple stressors on coastal ecosystems.

The NOAA6301 system:

- provides support to the program areas which are responsible for conducting research in the areas of marine bio-toxins; eco-toxicology; forensics; biotechnology; marine mammal stranding and necropsies; risk analysis; DNA sequencing; and marine related viruses and pathogens;
- provides an operational environment supporting the mission and staff of the program offices located on the Silver Spring Metro Center Campus - NCCOS Head Quarters (HQ), Center for

Sponsored Coastal Ocean Research (CSCOR), and Center for Coastal Monitoring and Assessment (CCMA); Beaufort, NC - Center for Coastal Fisheries and Habitat Research (CCFHR); Charleston, SC - Center for Coastal Environmental Health and Biomolecular Research (CCEHBR) and Hollings Marine Laboratory (HML); and Oxford, MD - Cooperative Oxford Laboratory (COL); Beaufort, NC (CCFHR); Charleston, SC (CCEHBRC and CHHR/HML); and Oxford, MD (CCEHBRO);

- provides all resources related to data management, electronic file, COTS, printing, computer and software, field data acquisition, backup and restoration, LAN and WAN, helpdesk, specialty applications for GIS and statistical analysis, moderate programming, Web design and Web product delivery, video conferencing, and other media support services; and

- Provides continued service to the local area network (LAN) and the wide area network (WAN) connections for non-SSMC locations.

Questionnaire:

1. What is the status of this information system?

This is a new information system. *Continue to answer questions and complete certification.*

This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

This is an existing information system in which changes do not create new privacy risks.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *Please describe the activities which may raise privacy concerns.*

No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

 X I certify the criteria implied by one or more of the questions above **apply** to the National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

 I certify the criteria implied by the questions above **do not apply** to the National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO): Rohit Munjal

Signature of ISSO: MUNJAL.ROHIT.1500946 Digitally signed by MUNJAL.ROHIT.1500946381 Date: 2018.01.05 09:43:16 -05'00' 381 Date: _____

Name of Information Technology Security Officer (ITSO): John D. Parker

Signature of ITSO: PARKER.JOHN.D.136583591 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.01.17 14:18:00 -05'00' 4 Date: _____

Name of Authorizing Official (AO): Steven Thur

Signature of AO:  Digitally signed by THUR.STEVEN.M.1365841299 Date: 2018.01.19 07:49:11 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRU Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.23 10:18:48 -05'00' M.1514447892 Date: _____

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Tuesday, January 23, 2018 10:23 AM
To: Mark Graff NOAA Federal
Cc: Gary Petroski NOAA Federal
Subject: NOAA8884 PIA and PTA for your signature
Attachments: NOAA8884 PIA 011618 Final_SO ITSO Signature.pdf; NOAA8884 PTA 01162018 Final_SO ITSO Signed.pdf

Revised per your comments, and okay'd for signatures by you. Despite the file names, the AO did sign as well.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751

Ce (b)(6)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Tuesday, January 23, 2018 10:26 AM
To: Gioffre, Kathy (Federal); CPO
Cc: Mark Graff NOAA Federal; Rohit Munjal NOAA Affiliate
Subject: NOAA6301 CERTIFICATION, PIA and PTA for your review
Attachments: NOAA6301_PIA_Annual_Review_Certification_2018 mhg.pdf; NOAA6301_PTA_2018 v2 mhg.pdf; NOAA6301_PIA_2018 v3 mhg.pdf

Kathy, here are the certification, PIA and PTA. No changes except the ATO date and the checking of 'no new privacy risks".

thanks, Sarah

**U.S. Department of Commerce
NOAA**



**Privacy Impact Assessment
for the
National Centers for Coastal Ocean Science (NCCOS) Research
Support System (NOAA6301)**

Reviewed by: _____, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301)

Unique Project Identifier: 006-00-02-00-01-0511-00

Introduction: System Description

The NOAA6301 NCCOS Research Support System provides the network infrastructure, hardware and software necessary to enable the mission of NCCOS, the organization. NCCOS's mission is to provide coastal managers with scientific information and tools needed to balance society's environmental, social, and economic goals.

NCCOS is passionate about supporting NOAA's environmental and economic missions by providing valuable scientific information to its constituents. NCCOS's fundamental principles are:

- To deliver high quality science in a timely and consistent manner using productive and strong partnerships.
- To develop and maintain relevant research, long term data collection and analyses, and forecasting capabilities in support of its customers, stakeholders, and partners.
- To build capacity in the private, local, state, and tribal sectors by transferring technology and providing technical assistance and knowledge to its customers and partners.
- To conduct the anticipatory science necessary to manage potential impacts of multiple stressors on coastal ecosystems.

The NOAA6301 system:

- provides support to the program areas which are responsible for conducting research in the areas of marine bio-toxins; eco-toxicology; forensics; biotechnology; marine mammal stranding and necropsies; risk analysis; DNA sequencing; and marine related viruses and pathogens;
- provides an operational environment supporting the mission and staff of the program offices located on the Silver Spring Metro Center Campus - NCCOS Head Quarters (HQ), Center for Sponsored Coastal Ocean Research (CSCOR), and Center for Coastal Monitoring and Assessment (CCMA); Beaufort, NC - Center for Coastal Fisheries and Habitat Research (CCFHR); Charleston, SC - Center for Coastal Environmental Health and Biomolecular Research (CCEHBR) and Hollings Marine Laboratory (HML); and Oxford, MD - Cooperative Oxford Laboratory (COL);
- provides all resources related to data management, electronic file, COTS, printing, computer and software, field data acquisition, backup and restoration, LAN, helpdesk, specialty applications for GIS and statistical analysis, moderate programming, Web design and Web product delivery, video conferencing, and other media support services; and
- Provides continued service to the local area network (LAN) connections for non-SSMC locations.

In addition to the general purposes office automation support (file/printer sharing, application

hosting, collaboration, etc.) provided by NOAA6301, the system provides help desk services and supports a number of web sites and internal minor applications, one of which stores PII for the purpose of conducting the external grant review process as defined within the NOAA Grants Online System, (FISMA system ID, NOAA1101, PIA signed 7/6/2017). Grant applications are downloaded from Grants Online on a case by case basis, for review. They are stored by opportunity or grant number.

As detailed in the information sharing section below, NCCOS gathers and stores PII related to employees and contractors for Human Resource-related issues such as the hiring process as well as workforce planning, COOP Operations, and documentation. The NCCOS collects BII during the pre and post activities associated with the acquisition and management of contracts.

Information Sharing

NOAA6301 NCCOS Research Support System General Support System (GSS) collects and collects and stores limited PII, specifically, names, telephone numbers and email addresses (voluntarily submitted by staff, partners, volunteers, and government and non-government collaborators) to facilitate internal and external communications to facilitate business and collaborative functions. This is not a central collection, but rather separated by function or individual project or person.

NOAA6301 is a general support system for NCCOS and stores information about individuals during the application and hiring of (electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase), including standard HR information (such as Travel authorization and vouchers, passports and international travel forms (completed by the employee through the travel portal), information for security badging process (contact information only the employee completed the badge application on paper forms, which are taken to the NOAA Office of Security), and performance appraisal ranking).

NCCOS' employee data is collected, stored and maintained for internal COOP, Human Resources, and workforce planning purposes (federal employee/contractor).

NCCOS collects BII during the pre and post activities associated with the acquisition and management of contracts. The storage is in the form of PDF forms or MS Word documents. There is no major application or database used to collect or store BII or employee PII information. NCCOS does not have a separate HR division since NCCOS utilizes the NOAA Workforce Management Office.

With exception of the CSCOR Review Application, all information is stored on supervisors' and acquisition managers' restricted access file storage available only to the specific employee(s). Access is restricted to those on a need to know basis, by permissions settings and/or passwords. The data is access controlled when on a supervisor's desktop machine or file share; if stored on a supervisor's laptop, the data is encrypted since all mobile devices have full encryption. The CSCOR Review Application although managed by NCCOS, is hosted by an NOAA6001 NOS Enterprise Services server and is restricted by username and password.

CSCOR Review Application Information in identifying form is made available by NOAA Grants Online (FISMA system ID, NOAA1101, PIA signed 7/6/2017) to NCCOS to accomplish Independent Individual Merit Reviews supporting the NOAA Grants Online system and process.

Information about the NOAA Grants Program may be found at: <http://www.corporateservices.noaa.gov/~grantsonline/index.html>. This is a non-public system. Information extracted from NOAA Grants Online to support the Independent Individual Merit Reviews is temporarily stored to facilitate the review process lifecycle. This information can include any general personal information and work related information. Although it is not the intent to extract PII information from the NOAA Grants Online system, it is possible the information could contain the Employer Identification Number (EIN). The EIN is a non-mandatory field which may be populated on the grants information made available by federal forms not managed by NCCOS. The NCCOS information system does not collect this identifying information directly.

A citation of the legal authority to collect PII and/or BII

The general legislation supporting the system is 5 U.S.C.301, one of the statutes concerning government organization and employees.

Additional authorities from DEPT-2, Accounts Receivable: H.R. 4613 (97th): Debt Collection Act of 1982, a bill to increase the efficiency of Government-wide efforts to collect debts owed the United States and to provide additional procedures for the collection of debts owed the United States and 5 U.S.C. 5701-09; 31 U.S.C. 951-953, 4 CFR 102.4, FPMR 101-7; Treasury Fiscal Requirements Manual.

Additional authorities from GSA/GOVT-9, System for Award Management: Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204, and 40 U.S.C. 121(c), Regulations by Administrator. For the Entity Management functional area of Systems Award Management, the authorities for collecting the information and maintaining the system are the Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204 and 2 CFR, Subtitle A, Chapter I, and Part 25, as well as 40 U.S.C. 121(c). For the exclusions portion of the Performance Information functional area, the authorities for collecting the information and maintaining the system are FAR Subparts 9.4 and 28.2, Executive Order 12549 (February 18, 1986), Executive Order 12689 (August 16, 1989).

The Federal Information Processing Standard (FIPS) 199 security impact category for NOAA6301 is moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- This is a new information system.
- This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	

b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

X This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID	X**	f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport	x	k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					
** Same data element checked for Grants Online, as in the NOAA1101 PIA.					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	x	o. Medical Information	
d. Gender		j. Telephone Number	x	p. Military Service	
e. Age		k. Email Address	x	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	x	d. Telephone Number	x	g. Salary	x
b. Job Title	x	e. Email Address	x	h. Work History	x
c. Work Address	x	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify): NCCOS does not capture photographs for badging since it is performed and stored by the NOAA badging office of security.					

System Administration/Audit Data (SAAD)					
a. User ID	x	c. Date/Time of Access	x	e. ID Files Accessed	
b. IP Address	x	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)
Pre and Post Acquisition. This BII information would be obtained and utilized during the pre acquisition obtained through deliverable BIDS package and contain specific company information. BII information would be maintained on specific secure network folders during the execution of awarded contract and other information from companies not receiving awards would be deleted, when appropriate. This information is protected under 41 USC 253, the FOIA Exemption 3 statute for contract proposals and collections associated with them.

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	x	Hard Copy: Mail/Fax	x	Online	
Telephone		Email	x		
Other (specify):					

Government Sources					
Within the Bureau	x	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify): NOAA Grants Online http://www.corporateservices.noaa.gov/~grantsonline/index.html .					

Non-government Sources					
Public Organizations	x	Private Sector	x	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): NCCOS does not acquire PII from other non-government sources other than associated through formal partnership agreements and for the purpose of facilities safety, security, and COOP. Other non-government sources would be only for BII associated with Pre/Post Acquisition Sensitive Information obtained through delivered bids on NCCOS Acquisitions.					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)					
Smart Cards		Biometrics			
Caller-ID		Personal Identity Verification (PIV) Cards			
Other (specify):					

x	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
---	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

x	There are not any IT system supported activities which raise privacy risks/concerns.		
---	--------------------------------------------------------------------------------------	--	--

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	x
For administrative matters	x	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Collected BII would be associated with determine qualification/eligibility for open acquisitions. PII would be collected for administrative actions, for HR and Workforce management. PII/BII: NOAA Grants Online - Grant Merit Reviews			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

In general, the laws that created the various NOS programs, specifically NCCOS, include provisions for the program to accomplish a mission. The mission may involve partnerships and educating the public. The collection and storage of information is part of accomplishing the legislated mission of the NCCOS, the NOS, and NOAA (members of the public and federal employees).

NOAA6301 stores PII on an ad hoc basis as part of the application and hiring of employees, including electronic copies of resumes and the processing of HR data about employees including hiring ranking. This information is stored temporarily during the hiring phase, as well as standard HR information such as travel authorization and vouchers, passports and international travel forms, information for the security badging process (name, work email address and work telephone number, and performance appraisal ranking).

NCCOS stores limited PII and potentially an EIN (BII), for grant review only, on an ad hoc basis about individuals or entities that are providing information in support of a grant application submitted through NOAA Grants Online which is retained for the review process lifecycle only.

BII Pre and Post Acquisition. This BII information would be obtained and utilized during the pre-acquisition obtained through deliverable BIDS package and contain specific company information. BII information would be maintained on specific secure network folders during the execution of awarded contract and other information from companies not receiving awards would be deleted, when appropriate.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	x		
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	-----------------------------------------------

- 6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NOAA6301 connects to the NOS Line Office information system NOAA6001 and other NOAA information systems for VPN, Security and Network Operations. NCCOS established security permissions based on NOS Active Directory Network account (enforced 2FA when possible), restrictions in firewall ACL and security permissions on specific network folders where documentation is stored.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

- 6.3 Identify the class of users who will have access to the IT system and the PII/BII. (*Check all that apply.*)

Class of Users			
General Public		Government Employees	x
Contractors	x		
Other (specify):			

Section 7: Notice and Consent

- 7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. (*Check all that apply.*)

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
x	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://coastalscience.noaa.gov/contact/privacy . A PAS for Grants Online has been finalized and has been posted at: https://grantsonline.rdc.noaa.gov/	
x	Yes, notice is provided by other means.	Specify how: (Specific to PII) Verbally by administrative appointed staff or supervisor OR this address is referenced: https://coastalscience.noaa.gov/contact/privacy . This is an NOS standard privacy policy and not specific to NCCOS. BII is provided for the purpose of acquisition consideration only through government managed acquisition processes and forms only. NCCOS does not generate or maintain additional forms or processes to support acquisition activities. BII provided within NOAA Grants Online utilized within the CSCOR Review Application is managed through the NOAA Grants Online application only.

	No, notice is not provided.	Specify why not:
--	-----------------------------	------------------

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

x	Yes, individuals have an opportunity to decline to provide PII/BII.	<p>Specify how: PII: No information collected is mandatory. Individuals are verbally told by administrative appointed staff or supervisor that they can decline or individuals are directed to review the privacy policy at this address: https://coastalscience.noaa.gov/contact/privacy, where it is stated all information collected is voluntary. This is an NOS standard privacy policy and not specific to NCCOS.</p> <p>BII provided for acquisition consideration is not mandatory. However, declining to provide the information necessary to evaluate them for an acquisition could result in non-award.</p> <p>PII provided within NOAA Grants Online, utilized within the CSCOR Review Application, is managed through the NOAA Grants Online application only. Completion of the Grants Online application would be needed for award consideration.</p>
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	<p>Specify how: Applicants for positions are providing their personal information on a voluntary basis through their resumes. There is only one use for this information. The employment application contains the Privacy Act notice. Applicants have the opportunity to consent to only particular uses of their PII, in writing, to the HR representative or their supervisor, but it may affect the overall processing of their employment.</p> <p>For ongoing employee business, such as travel, there is only one specific use for each PII collection.</p> <p>BII is submitted for a specific purpose which consent is implied with the submittal of the package. BII provided within NOAA Grants Online utilized within the CSCOR Review Application is managed through the NOAA Grants Online application only.</p>
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

x	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: (Specific to PII) NCCOS employees can contact HR staff or the federal employee personnel page to update their information, as they are informed as part of new employee
---	-----------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>orientation.</p> <p>BII is provided for the purpose of acquisition consideration through government managed acquisition processes and forms only. NCCOS does not generate or maintain additional forms or processes to support acquisition activities. BII provided within NOAA Grants Online utilized within the CSCOR Review Application is managed through the NOAA Grants Online application only.</p> <p>Regarding contracts and grants that are in process or awarded, the applicants or awardees would send updates to the stated NOAA contact.</p>
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to the PII/BII is restricted to authorized personnel only.
x	<p>Access to the PII/BII is being monitored, tracked, or recorded.</p> <p>Explanation: With exception to the CSCOR Review Application, access to storage folders are restricted by ACL and since PII/BII is not centralized in a database it cannot be easily monitored for access. The CSCOR Review Application has a database which is monitored, tracked and recorded.</p>
x	<p>The information is secured in accordance with FISMA requirements.</p> <p>Provide date of most recent Assessment and Authorization (A&A): 3/23/2017. Next one is no later than 3/22/2018.</p> <p><input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.</p>
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
x	Other (specify): All appropriate contractors and contract clauses include non-disclosure, but not all federal employees sign a confidentiality agreement or non-disclosure agreement.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

All information is stored within the accredited boundaries of NOAA6301 in network data shares controlled by established permission based on the organizational, project, or employee access rights. Any access to specific restricted files or folders must be requested through an access change request which is reviewed and documented by the NOAA6301 Information System Security Officer for authorization and mission ‘need-to-know’ requirement prior to implementation. Least privilege is implemented through file share permissions to ensure privacy and open only to those demonstrating a “need to know.”

Any PII information which is transmitted electronically must follow the federal government and NOAA standard procedure of secure packaging such as utilization of Department of Commerce (DOC) Accellion for encryption in transit.

NCCOS implements security controls listed in NIST Special Publication 800-53 R4 required for a moderate system. In compliance with NIST Special Publication 800-53 rev 4, NCCOS has a security program, with performance measures and goals, in order to complete continuous monitoring activities, which include annual security control reviews, quarterly vulnerability scanning, monthly review of security access control list, weekly review of audit logs, handling of access change requests and change control board activities. The risk assessment includes the possible threats and vulnerability to the confidentiality, integrity, and availability of mission and sensitive PII data along with the countermeasures.

The controls supporting the use of Microsoft Azure FedRamp approved system as a customer are in place in NOAA6301. There are currently Web applications, with no PII, hosted on Microsoft Azure. As noted in Section 12.2, we are transitioning CSCOR to Azure prior to December 2018. The same sharing controls that are in place currently for CSCOR will apply when it is moved to Azure.

Every year the IT system undergoes a thorough continuous monitoring for the assessment and authorization (A&A) process that is performed by an independent. The A&A process ensures that the security plan and operational, management, and technical controls meet Department of Commerce (DOC) and NOAA guidelines for continued operation.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C.

§ 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

x	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i> : COMMERCE/DEPT-18 - Employees Personnel Files Not Covered By Notices of Other Agencies; DEPT-2 , Accounts Receivable; GSA/GOVT-9 , System for Award Management.
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created:

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

x	<p>There is an approved record control schedule. Provide the name of the record control schedule: Chapters 1601 and 1607 of NOAA’s Records Schedules, http://www.corporateservices.noaa.gov/audit/records_management/schedules/, provide supplemental record retention guidance for the NCCOS Research Support System. Chapter 1601 pertains to general administration for the National Ocean Service and Chapter 1607 pertains to specific records managed by the NCCOS Research Support System. Specifically, 1601-02 Grants Working Files (N1-370-02-5), 1601-04 Electronic Copies (N1-370-02-5), 1601-05 NOS Annual Operating Plan (AOP) Information Tracking Systems (N1-370-04-4), 1609-06 in the NOAA Disposition Handbook and 1607-04 Program Funding Database.</p> <p>The retention period for these records is guided by the General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the federal government. In accordance with GRS 20, item 3, electronic versions of records scheduled for disposal may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. In accordance with GRS 20, item 3, the data is presently being retained indefinitely.</p> <p>For NCCOS administrative PII data, the records would be covered under the following NARA general records schedules: GRS 2 – payroll and pay administrative records GRS 20 – electronic records GRS 23 – records common to most offices within agencies</p> <p>NCCOS’ contact information (contractor and partner) is collected to provide a means for the Office of Coast Survey to communicate and respond to needs and requests. This data would be retained as long as the individual continued to request contact and information. It is technologically possible to delete information at the request of the individual. There is no scheduled records retention for this information.</p>
	<p>No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:</p>
x	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	x	Overwriting	x
Degaussing	x	Deleting	x
Other (specify): Compliant sanitization methods.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. (Check all that apply.)

X	Identifiability	Provide explanation: Evaluated how easily PII could be used to identify a specific individual. Based on contact information, individuals can be identified.
X	Quantity of PII	Provide explanation: Considered how many individuals can be identified from the PII. The PII is only temporarily stored for a limited amount of individuals, therefore reducing the breach impact.
X	Data Field Sensitivity	Provide explanation: Data fields are limited and only used when absolutely required. SSN is not one of these data fields. EIN is a field which can be populated within NOAA Grants Online, however, is not required and is not utilized. This field will not be extracted from NOAA Grants Online in the future revision of the CSCOR Review Application.
X	Context of Use	Provide explanation: Evaluated the context of use—the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated. The use of the PII is restricted to specific individuals, stored for a limited amount of time and is not utilized in more than one way reducing the impact.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: The PII is only temporarily stored in a protected location for a limited amount of individuals, therefore reducing the breach impact.
X	Other:	Provide explanation: The loss of a single individual's PII would have an impact on that individual through possible identify theft and NCCOS as a government identity BUT it would not have an impact on the NCCOS mission or have a serious impact on reputation.

Section 12: Analysis


12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
x	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

x	Yes, the conduct of this PIA results in required technology changes. Explanation: NOAA6301 is utilizing Azure SQL in the Microsoft Azure PaaS environment to store web application data. Although there is currently no PII/BII associated with the web/apps and transitioning to the new environment is not expected prior to December 2018, controls are already in place to encrypt at rest data through the Azure SQL TDE capability: https://msdn.microsoft.com/en-us/library/dn948096.aspx . All SQL databases will have this feature turned on at inception and it will remain on. This storage is currently planned only for CSCOR and will further secure the CSCOR Review Application Database.
	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

<p>Information System Security Officer or System Owner Name: Rohit Munjal Office: NOS/NCCOS Phone: 240-533-0289 Email: Rohit.Munjal@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: right;">MUNJAL.ROHIT.1500 Digitally signed by MUNJAL.ROHIT.1500946381 Date: 2018.01.05 09:46:15 -05'00'</p> <p>Signature: 946381</p> <p>Date signed:</p>	<p>Information Technology Security Officer Name: John D. Parker Office: NOS Phone: 240-533-0832 Email: John.D.parker@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: right;">PARKERJOHN.D.13658359 Digitally signed by PARKERJOHN.D.1365835914 Date: 2018.01.17 14:46:55 -05'00'</p> <p>Signature: 14</p> <p>Date signed:</p>
<p>Authorizing Official Name: Steven Thur Office: NOS/NCCOS Phone: 240-533-0146 Email: Steven.Thur@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: right;"> Digitally signed by THUR.STEVEN.M.1365841299 Date: 2018.01.19 07:50:30 -05'00'</p> <p>Signature:</p> <p>Date signed:</p>	<p>Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p style="text-align: right;">GRAFF.MARK. Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c U.S., o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447 892 Date: 2018.01.23 10:12:39 -05'00'</p> <p>Signature: HYRUM.15144</p> <p>Date signed: 47892</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NCCOS Research Support System

FISMA Name/ID (if different): NOAA6301

Name of IT System/ Program Owner: National Centers for Coastal Ocean Science

Name of Information System Security Officer: Rohit Munjal

Name of Authorizing Official(s): Steven Thur / Cheryl Marlin

Date of Last PIA Compliance Review Board (CRB): 3/16/2017

(This date must be within three (3) years.)

Date of PIA Review: 1/8/2018

Name of Reviewer: Rohit Munjal

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: MUNJAL.ROHIT.1500946381 Digitally signed by MUNJAL.ROHIT.1500946381
Date: 2018.01.08 12:19:26 05'00'

Date of Privacy Act (PA) Review: _____

Name of Reviewer: _____

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: _____

Date of BCPO Review: 1/23/18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF MARK HYRUM 1514447892
DN c US, o U.S. Government, ou DoD, ou PKI,
ou OTHER, cn GRAFF MARK HYRUM 1514447892
Date 2018.01.23 10:17:27 -0500

**U.S. Department of Commerce
NOAA**



**Privacy Threshold Analysis
for the
National Centers for Coastal Ocean Science (NCCOS) Research
Support System (NOAA6301)**

U.S. Department of Commerce Privacy Threshold Analysis
NOAA/National Centers for Coastal Ocean Science (NCCOS) Research
Support System (NOAA6301)

Unique Project Identifier: 006-00-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: The NOAA6301 National Centers for Coastal Ocean Science (NCCOS) Research Support System provides the network infrastructure, hardware and software necessary to enable the mission of NCCOS, the organization. NCCOS's mission is to provide coastal managers with scientific information and tools needed to balance society's environmental, social, and economic goals.

NCCOS is passionate about supporting NOAA's environmental and economic missions by providing valuable scientific information to its constituents. NCCOS's fundamental principles are:

- To deliver high quality science in a timely and consistent manner using productive and strong partnerships.
- To develop and maintain relevant research, long term data collection and analyses, and forecasting capabilities in support of its customers, stakeholders, and partners.
- To build capacity in the private, local, state, and tribal sectors by transferring technology and providing technical assistance and knowledge to its customers and partners.
- To conduct the anticipatory science necessary to manage potential impacts of multiple stressors on coastal ecosystems.

The NOAA6301 system:

- provides support to the program areas which are responsible for conducting research in the areas of marine bio-toxins; eco-toxicology; forensics; biotechnology; marine mammal stranding and necropsies; risk analysis; DNA sequencing; and marine related viruses and pathogens;
- provides an operational environment supporting the mission and staff of the program offices located on the Silver Spring Metro Center Campus - NCCOS Head Quarters (HQ), Center for

Sponsored Coastal Ocean Research (CSCOR), and Center for Coastal Monitoring and Assessment (CCMA); Beaufort, NC - Center for Coastal Fisheries and Habitat Research (CCFHR); Charleston, SC - Center for Coastal Environmental Health and Biomolecular Research (CCEHBR) and Hollings Marine Laboratory (HML); and Oxford, MD - Cooperative Oxford Laboratory (COL); Beaufort, NC (CCFHR); Charleston, SC (CCEHBRC and CHHR/HML); and Oxford, MD (CCEHBRO);

- provides all resources related to data management, electronic file, COTS, printing, computer and software, field data acquisition, backup and restoration, LAN and WAN, helpdesk, specialty applications for GIS and statistical analysis, moderate programming, Web design and Web product delivery, video conferencing, and other media support services; and

- Provides continued service to the local area network (LAN) and the wide area network (WAN) connections for non-SSMC locations.

Questionnaire:

1. What is the status of this information system?

This is a new information system. *Continue to answer questions and complete certification.*

This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

This is an existing information system in which changes do not create new privacy risks.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *Please describe the activities which may raise privacy concerns.*

No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

 X I certify the criteria implied by one or more of the questions above **apply** to the National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

 I certify the criteria implied by the questions above **do not apply** to the National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO): Rohit Munjal

Signature of ISSO: 381  Digitally signed by
MUNJAL.ROHIT.1500946
Date: 2018.01.05 09:43:16 -05'00' Date: _____


Name of Information Technology Security Officer (ITSO): John D. Parker

Signature of ITSO: 4  Digitally signed by
PARKER.JOHN.D.136583591
Date: 2018.01.17 14:18:00 -05'00' Date: _____

Name of Authorizing Official (AO): Steven Thur

Signature of AO:   Digitally signed by
THUR.STEVEN.M.1365841299
Date: 2018.01.19 07:49:11 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: M.1514447892  Digitally signed by
GRAFF.MARK.HYRU
DN: c US, o U.S. Government, ou DoD, ou PKI,
ou OTHER, cn GRAFF.MARK.HYRU.1514447892
Date: 2018.01.23 10:18:48 -05'00' Date: _____

Martin, Lisa (Federal)

From: Martin, Lisa (Federal)
Sent: Tuesday, January 23, 2018 11:06 AM
To: Graff, Mark (Federal); Jones, Stephen; Williams, Eric (Contractor); Neal, Donna A; Daniel, Tiffany
Subject: Document for TTX Planning
Attachments: Guide to Conducting a PII Breach Table Top Exercise.docx

Attached.

Lisa J. Martin

Lisa J. Martin
Deputy Director of Departmental Privacy Operations
U.S. Department of Commerce
Office of Privacy and Open Government
Office: (202) 482-2459
Email: LMartin1@doc.gov

Guide to Conducting a PII Breach Table Top Exercise (TTX)

Prior to Conducting this TTX

1. Review the DOC PA, PII, and BII Breach Response Plan.
2. Review OMB Memorandum 17 12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.

Breach Response Team Members

1. Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)
2. General Counsel (legal counsel)
3. Chief Information Officer (CIO) or the CIO's designee
4. Senior Agency Information Security Officer (SAISO) or the SAISO's designee
5. Chief Financial Officer/Assistant Secretary for Administration
6. Assistant Secretary for Legislative and Intergovernmental Affairs (OLIA) (legislative affairs official)
7. Chief of Staff, Office of the Secretary
8. Director, Office of Public Affairs (OPA) (communication official)
9. Director, Office of Policy and Strategic Planning
10. Director, Office of Human Resources Management
11. Office of Security (OSY), Attends on an as needed basis
12. Office of Inspector General (OIG), Advisory Role
13. Bureau Chief Privacy Officers
14. Privacy Act Officers
15. Deputy Director for Departmental Privacy Operations
16. Departmental FOIA/PA Officer

Planning

1. Establish the objectives of the TTX. Some of your objectives may be:
 - a. Improve the understanding of the DOC Breach Response Plan.
 - b. Identify opportunities to improve the DOC Breach Response Plan and the Department's preparedness.
 - c. Identify interdependencies among agency organizations and third party service providers.
2. Plan the TTX logistics.
 - a. Determine the date.
 - b. Reserve a space with an appropriate clearance level, as well as any materials or multimedia support you may need, such as computer and display, whiteboard and markers, butcher block paper, handouts, and dial in capabilities.
 - c. Set a time limit for the TTX. This will help you choose an appropriate scenario and focus the conversation appropriately during the TTX.
 - d. Assign support staff roles.

- i. Determine what role you want your privacy program to play in the exercise. Individuals who are deeply involved in planning the TTX may need to take a step back during the exercise to avoid accidentally influencing the course of the exercise. In a TTX, privacy office representatives often act in an advisor or consultant role, responding to questions from other participants, rather than the active leaders they often are in an actual breach.
- ii. Identify a facilitator (Consider using a neutral facilitator). The facilitator has the primary responsibility for exercise conduct. This includes introducing and providing scenario updates, moderating the discussions to ensure players address exercise objectives and core capabilities, and ensuring everyone contributes to the discussion and relevant issues are explored as thoroughly as possible within the allotted time.
- iii. In addition to a facilitator, you will also need staff dedicated to:
 - 1. Taking notes. These notes will form the basis of the after action report.
 - 2. Tracking “parking lot” issues.
 - 3. Documenting when Breach Response Plan steps are completed.
- e. Create a participant roster to track attendance at the TTX.
- f. Consider what role you want Senior Executive Service (SES) members and other senior leaders to play. SES member participation may stifle the conversation. Consider using SES members or other senior leaders as floaters who give out real time feedback.

A sample agenda is below:

Time	Activity
[Month Day, Year]	
0000 - 0000	Registration
0000 - 0000	Welcome and Introductions
0000 - 0000	Exercise Overview
0000 - 0000	Module 1: Initial Response – Scenario Background
0000 - 0000	Break
0000 - 0000	Module 2: Response
0000 - 0000	Module 3: Recovery
0000 - 0000	Break
0000 - 0000	Hot Wash

Time	Activity
0000 - 0000	Closing Comments
0000 - 0000	Debrief (Facilitators and Evaluators only)

3. Develop a realistic breach scenario.

a. Choosing a scenario.

- i. Consider which high value assets, applications, or processes you may want to include in the scenario.
 1. You do not have to limit yourself to high value assets, but you want to make sure the scenario has stakes. A high profile system or program, or a scenario that involves risks to the reputation or operations of the agency may be more engaging and offer more avenues for the participants to explore.
- ii. Look at the Department's recent breaches, as well as any major breaches, for ideas.
- iii. Review the Department's breach metrics to see where there are trends that may indicate a weakness or identify an issue about which you receive questions or complaints and consider developing a scenario around those fact patterns.
- iv. Consider breaches that will engage all of the participants. For example, a loss of hardcopy documents may not effectively engage a participant from the cybersecurity team. A scenario that requires cross functional collaboration (e.g., between staff supporting Freedom of Information Act (FOIA), privacy, cybersecurity, and human resources) is often a more effective TTX.
- v. Balance the complexity of the TTX with the knowledge and experience the BRT members have with handling a breach. A too simple scenario may not be an effective use of this training and awareness opportunity; a too complex scenario may make it difficult for participants to engage in the TTX.

b. Refining the scenario.

- i. After you have chosen the breach you would like to test, speak with the relevant program office and/or system owners to ensure that you understand their data and processes. The scenario should be grounded in reality.
- i. Create a scenario that evolves over time. Create injects that complicate the scenario by adding additional facts. Provide a realistic timestamp for each update to help participants track their compliance with reporting requirements and understand how long actual breach response activities may take.
- ii. You should be able to map the DOC Breach Response Plan steps to the steps in your TTX; this will help you ensure that you have not forgotten any aspects of the DOC Breach Response Plan in the development of the scenario. Consider creating a table or grid citing back to the plan to ensure you know each BRT member's role and responsibility.
- iii. Try to make the TTX as interactive as possible. Break the scenario into modules with injects to keep participant attention and focus the discussion.

4. Create supporting artifacts, such as breach reports, supplemental reports, and after action reports.

- a. Use the Department’s breach reporting forms, including supplemental reports and after action reports, for the exercise. Using existing artifacts may highlight areas that need clarification or improvement.
 - b. You may want to create additional artifacts, such as dummy data file examples and external press reports.
 - c. Be sure to label all documents created for the TTX with “For exercise purposes only.”
 - d. It can be helpful to have packets available to the participants that include your agency’s breach response policy, the initial scenario, the injects, and any other supporting materials. The participants should not view the injects until they are directed to by the facilitator.
5. Provide an executive summary of the goals of the breach response program, its importance, and the goals and relevance of the TTX for senior leadership prior to TTX.

Execution

1. Share the TTX ground rules with the participants.
 - a. Stress that this is a learning exercise and that participants should feel comfortable asking questions or throwing out ideas. There are no wrong answers and everyone’s opinion will be considered.
 - b. Emphasize that participants should not “fight the scenario.” Every effort will have been made to ensure that the scenario is realistic and reflects actual practices.

Examples of TTX Ground Rules
<ul style="list-style-type: none"> Silence cell phones and other mobile devices during the exercise. Accept that the circumstances surrounding the event are real. This is a “no-fault” environment where varying viewpoints and disagreements are to be expected. There are no wrong answers.

2. Present the initial facts of the scenario to the participants. Use prompts to encourage interaction if the conversation is slow to start.
3. Participants should begin to identify immediate actions that should be taken, including establishing a communications plan and, if appropriate, Congressional notification plan.

Examples of Questions the BRT Should Consider
<ul style="list-style-type: none"> Is there a SORN or PIA? What other agency stakeholders or partners should be made aware of the breach? Who reports the breach to Congress? Who will need to approve any notices, notifications, and other communications? Who would be the source of the notification? Is any official designation required? How and who will fund identity protection services (IPS)? Does the CFO need to be engaged before securing IPS? Is there a vendor engaged for call center and IPS?

4. Start to provide injects to the scenario that reflect the types of information you would learn from a breach investigation.
 - a. With each inject, participants should identify the actions that should be taken based on the updated information.
 - b. You can also ask questions that explore other potential aspects of the breach. For example, if your breach involves information about members of the public only, you can ask them whether they would do anything differently if employee information was included.
5. Have participants complete a post TTX survey before leaving to get their input on the quality and strengths of the TTX, suggestions for improvement, and recommendations for future TTX scenarios.

Close-out

1. Develop an after action report/improvement plan that documents lessons learned and follow up actions for strengthening the DOC breach response process and/or the system, program, or processes that were tested in the TTX. The report/plan must provide timelines for improvement recommendation implementation and assignment to responsible parties.
 - a. Also document lessons learned for the next tabletop exercise. You can include these in the same report or a separate document.
 - b. Share the report with the BRT.
2. Review the DOC Breach Response Plan for any needed changes based on the lessons learned from the TTX.
3. If appropriate, conduct an out brief for senior leadership. The briefing should identify any unresolved issues to allow leadership to determine if any unmitigated risks are within the Department's risk tolerance.

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Tuesday, January 23, 2018 1:03 PM
To: Mark Graff NOAA Federal
Subject: Fwd: NOAA8884 PIA and PTA for your signature
Attachments: NOAA8884 PIA 011618 Final_SO ITSO Signature.pdf; NOAA8884 PTA 01162018 Final_SO ITSO Signed.pdf

Mark, please sign when you have time. The ATO is 4 30 18. thx

Forwarded message

From: **Sarah Brabson - NOAA Federal** <sarah.brabson@noaa.gov>
Date: Tue, Jan 23, 2018 at 10:23 AM
Subject: NOAA8884 PIA and PTA for your signature
To: Mark Graff NOAA Federal <mark.graff@noaa.gov>
Cc: Gary Petroski NOAA Federal <gary.petroski@noaa.gov>

Revised per your comments, and okay'd for signatures by you. Despite the file names, the AO did sign as well.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Tuesday, January 23, 2018 3:09 PM
To: Mark Graff NOAA Federal
Subject: NOAA8850 PIA and PTA for your signature DOC wants by COB today, thx
Attachments: NOAA8850 EMES PIA 010918 for mhg sig.pdf; NOAA8850 Privacy Threshold Analysis for mhg signature.pdf

Almost sent to Kathy by mistake!

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751

Ce (b)(6)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Mark Graff - NOAA Federal

From: Mark Graff NOAA Federal
Sent: Tuesday, January 23, 2018 3:18 PM
To: Robert Swisher NOAA Federal; Ed Kearns NOAA Federal; Sarah Brabson NOAA Federal
Cc: Dennis Morgan NOAA Federal; Eric Williams NOAA Affiliate; Robert Hembrook NOAA Federal
Subject: Fwd: Hypothetical for Privacy Incident Tabletop Exercise
Attachments: Department of Commerce PII, BII, and PA Breach Response and Notification Plan v3.pdf; Guide to Conducting a PII Breach Table Top Exercise.docx

FYI Below

This is a NOAA Privacy led activity with DOC wide visibility.

As part of the new obligations under OMB M 17 12, DOC is preparing to conduct its first Privacy Incident Tabletop Exercise across all DOC Bureaus (b)(5)

[REDACTED]. A copy of the most recent DOC Breach Response Notification Plan and guide to table top exercises is attached.

Let me know if you guys have any questions or issues you want raised to the group our next working group meeting to prepare the exercise will be Thursday afternoon.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

Forwarded message

From: **Mark Graff - NOAA Federal** <mark.graff@noaa.gov>

Date: Tue, Jan 23, 2018 at 1:55 PM

Subject: Hypothetical for Privacy Incident Tabletop Exercise

To: "Neal, Donna A" <donna.a.neal@census.gov>, Eric Williams NOAA Affiliate <eric.d.williams@noaa.gov>, "Martin, Lisa" <lmartin1@doc.gov>, "Jones, Stephen" <sjones@oig.doc.gov>, "Murphy, Tahira" <TMurphy2@doc.gov>, "Daniel, Tiffany" <Tiffany.Daniel@bis.doc.gov>

Cc: "Purvis, Katrina" <cpurvis@doc.gov>

Hello All,

(b)(5)
[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
[\(301\) 628 5658](tel:3016285658) (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

United States Department of Commerce

Privacy Act, Personally Identifiable Information (PII), and Business Identifiable Information (BII) Breach Notification Plan

The goal of the Department of Commerce is to ensure that all Departmental Information Processes are compliant with and adhere to all Privacy Laws, Mandates, and Best Practices.

**Version 3.0
July 2017**



Department of Commerce PII, BII, and PA Breach Response and Notification Plan



COMMERCE PRIVACY MISSION STATEMENT

The Department of Commerce is committed to safeguarding personal privacy. Individual trust in the privacy and security of personally identifiable information is a foundation of trust in government and commerce in the 21st Century. As an employer, a collector of data on millions of individuals and companies, the developer of information-management standards and a federal advisor on information management policy, the Department strives to be a leader in best privacy practices and privacy policy. To further this goal, the Department assigns a high priority to privacy considerations in all systems, programs, and policies.

This Plan establishes governing policies and procedures for privacy incident handling at the Department of Commerce (DOC). The policies and procedures are based on applicable laws, Presidential Directives, and Office of Management and Budget (OMB) directives. It was originally developed in response to memoranda issued by the OMB and has been revised according to the most recent memoranda issued in 2017.¹

Please contact the DOC Senior Agency Official for Privacy (SAOP)/ Chief Privacy Officer (CPO) in the Office of Privacy and Open Government (OPOG) at cpo@doc.gov or (202) 482-1190 concerning questions about this Plan or the DOC Privacy Program.

¹ OMB Memorandum regarding “Preparing for and Responding to a Breach of Personally Identifiable Information”, issued on January 3, 2017 ([OMB M-17-12](#)).



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Table of Contents

1.0 INTRODUCTION.....	1
1.1 PURPOSE	1
1.2 BACKGROUND.....	1
1.3 SCOPE	2
1.4 AUTHORITIES	2
2.0 DEFINITIONS AND EXAMPLES	3
3.0 ROLES AND RESPONSIBILITIES	7
3.1 BUREAU/OPERATING UNIT CIRT (BOU CIRT).....	7
3.2 BUREAU CHIEF PRIVACY OFFICER (BCPO)	9
3.3 ENTERPRISE SECURITY OPERATIONS CENTER (ESOC)	11
3.4 SENIOR AGENCY OFFICIAL FOR PRIVACY (SAOP)/CHIEF PRIVACY OFFICER (CPO)	11
3.5 DOC PII BREACH RESPONSE TASK FORCE	12
3.6 OFFICE OF THE CHIEF INFORMATION OFFICER (OCIO)	13
3.7 OFFICE OF GENERAL COUNSEL (OGC)/BUREAU CHIEF COUNSEL (BCC).....	13
3.8 OFFICE OF INSPECTOR GENERAL (OIG)	13
3.9 OFFICE OF LEGISLATIVE AND INTERGOVERNMENTAL AFFAIRS (OLIA).....	13
3.10 PRIVACY COUNCIL.....	14
3.11 OFFICE OF PUBLIC AFFAIRS (OPA)	14
3.12 SUPERVISOR/MANAGER	14
3.13 EMPLOYEE/CONTRACTOR	14
4.0 DOC PII/BII/PA INCIDENT RESPONSE PROCESS	15
5.0 RISK OF HARM ANALYSIS FACTORS AND RATING ASSIGNMENT.....	17
6.0 BREACH NOTIFICATION AND REMEDIATION	19
6.1 NOTIFYING INDIVIDUALS	19
6.2 METHOD OF NOTIFICATION.....	20
6.3 NOTIFICATION/REPORTING REQUIREMENTS	21
7.0 CONSEQUENCES	21
APPENDIX A – DOC PII INCIDENT REPORT CONTENT	22
APPENDIX B – RISK LEVEL EVALUATION MATRIX	24
RISK LEVEL EVALUATION MATRIX	25
EXAMPLES: HOW TO USE RISK LEVEL EVALUATION MATRIX	26
Scenario 1: Resulting from PII Owner Action and/or Personal Use	26
Scenario 2: Valid Need to Know and Authorized User	26
Scenario 3: Authorized User, but One or More Recipients has no Need to Know.....	27

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



Scenario 4: Not Authorized, Greater than 10 PII Fields, and Affecting More than 2500
Individuals 27

APPENDIX C – DELEGATION OF AUTHORITY MEMORANDUM 28

APPENDIX D – FLOWCHART 29

**APPENDIX E – SENIOR AGENCY OFFICIAL FOR PRIVACY/CHIEF PRIVACY
OFFICER AND COMMERCE OPERATING UNIT CIRT REPORTING OFFICES
..... 30**

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



1.0 Introduction

1.1 Purpose

The Department of Commerce (DOC, Commerce, or the Department) has a duty to appropriately safeguard personally identifiable information (PII) in its possession and to prevent its compromise in order to maintain the public's trust. This Breach Response and Notification Plan (the Plan) serves this purpose by informing DOC and its bureaus, employees, and contractors of their obligation to protect PII and by establishing procedures defining how they must prepare for and respond to a PII incident.

The Plan also addresses response and notification procedures for business identifiable information (BII) and Privacy Act (PA) incidents.

1.2 Background

The Office of Management and Budget (OMB) regularly issues memoranda which require agencies to assess and mitigate the risk of harm to individuals potentially affected by a breach and develop guidance on whether and how to provide notification and services to those individuals. This Plan establishes appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records for any individual on whom information is maintained. Further, OMB requires each agency to develop a breach notification policy and plan, and to establish a core management team responsible for responding to the breach of PII/BII.

Pursuant to these OMB requirements, this Plan:

- Outlines procedures for reporting a DOC breach;
- Provides guidance for assessing and mitigating the risk of harm to individuals potentially affected by a breach;
- Delineates the investigation process, notification and remediation plan;
- Identifies applicable privacy compliance documentation;
- Lists the appropriate information sharing when responding to a breach; and
- Establishes the breach response team, called the DOC PII Breach Response Task Force (Task Force).

This Plan supplements current requirements for reporting and handling incidents pursuant to the Federal Information Security Modernization Act (FISMA), National Institute of Standards and Technology (NIST) [Special Publication 800-61](#), Computer Security Incident Handling Guide, and the concept of operations for Department of Homeland Security (DHS), United States



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Computer Emergency Readiness Team (US-CERT). All Bureaus, Operating Units, and contractors are responsible for compliance with this Plan.

1.3 Scope

The DOC PII, BII, and PA Breach Response and Notification Plan applies to all DOC and Bureau personnel including contractors, and to all DOC and Bureau information systems and information in any format (e.g., paper, electronic, etc.).

1.4 Authorities

- The [Privacy Act of 1974, 5 U.S.C. § 552a](#), provides privacy protections for records containing information about individuals (i.e., citizen and legal permanent resident) that are collected and maintained by the federal government and are retrieved by a personal identifier. The Act requires agencies to safeguard information contained in a system of records.
- The [Federal Information Security Modernization Act of 2014, Public Law No. 113-283](#), requires agencies to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of an agency.
- [US-CERT Federal Incident Notification Guidelines](#), effective April 1, 2017, provides guidance for notifying the computer emergency readiness team of any incident that jeopardizes the integrity, confidentiality, or availability of information or an information system.
- [OMB Memorandum M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 \(September 26, 2003\)](#), requires agencies to conduct reviews of how information about individuals is handled when information technology (IT) is used to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information, and to describe how the agency handles information that individuals provide electronically.
- [OMB Memorandum M-06-16, Protection of Sensitive Agency Information \(June 23, 2006\)](#), requires agencies to implement encryption protections for PII being transported and/or stored offsite.
- [OMB Memorandum M-11-02, Sharing Data While Protecting Privacy \(November 3, 2010\)](#), requires agencies to develop and implement solutions that allow data sharing to move forward in a manner that complies with applicable privacy laws, regulations, and policies.
- [OMB Memorandum M-16-04, Cybersecurity Strategy and Implementation Plan \(CSIP\) for the Federal Civilian Government \(October 30, 2015\)](#), requires agencies to take immediate

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



steps to further protect Federal information and assets and improve the resilience of Federal networks.

- [OMB Memorandum M-17-05, Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements \(November 4, 2016\)](#), requires oversight and reporting requirements for Information Security and Privacy Programs and updates major incident definition and US-CERT notification guidelines.
- [OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information \(January 3, 2017\)](#).

2.0 Definitions and Examples

- **Authorized User** - A person or persons granted permission to manage, access or make decisions regarding PII.
- **Breach/Incident** - For the purposes of this document, a PII breach incident includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses sensitive PII, or (2) an authorized user accesses or potentially accesses sensitive PII for other than an authorized purpose. A PII breach incident is not limited to an occurrence where a person other than an authorized user potentially accesses sensitive PII by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A breach incident may also include:
 - The loss or theft of physical documents that include sensitive PII and portable electronic storage media that stores sensitive PII. This could be a laptop or portable storage device storing sensitive PII which is lost or stolen, or a box of documents with sensitive PII which is lost or stolen during shipping;
 - The inadvertent disclosure of sensitive PII. Examples include an email containing PII/BII which is inadvertently sent to the wrong person or sensitive PII that should not be widely disseminated is posted inadvertently on a public website;
 - An employee sending their own sensitive PII via an unencrypted email;
 - An oral disclosure of sensitive PII to a person who is not authorized to receive that information. For example, an unauthorized third party overhears agency employees discussing sensitive PII about an individual seeking employment or Federal benefits;
 - An authorized user accessing sensitive PII for other than an authorized purpose. An example is a user with authorized access to sensitive PII sells it for personal gain or disseminates it to embarrass an individual.



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

- **Business Identifiable Information (BII)** Information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person and privileged or confidential." Commercial or financial information is considered confidential if disclosure is likely to cause substantial harm to the competitive position of the person from whom the information was obtained.
- **Close-out** The process by which the Bureau Privacy Officer (BPO) or BPO designee closes a PII incident report. Close-out is warranted after completion of the investigation of the incident, issuance of external notification if appropriate, and implementation of all suitable privacy and IT security mitigation, corrective, and/or remedial actions. If a portion of one or more of these stages is ongoing, the incident cannot be closed. Written SAOP/CPO concurrence is required for close-out of Moderate and High risk PII incidents.
- **Computer Incident Response Team (CIRT)²** A capability set up for the purpose of assisting in responding to computer security-related incidents. [[NIST SP 800-61](#)]. This capability may include resources, such as staff, tools, monitoring, and intrusion detection/prevention services.
- **Corrective/Remedial Actions** Steps taken to mitigate losses and protect against any further breaches.
- **Enterprise Security Operations Center (ESOC)** – the committee that provides the Department of Commerce with cybersecurity status information and decision-making regarding cyber threat risks of various types.
- **Harm** Any adverse effects that would be experienced by an individual whose sensitive PII was the subject of a breach, as well as any adverse effects experienced by the organization that maintains the PII. Harm to an individual includes any negative or unwanted effects (i.e., anything that may be socially, physically, or financially damaging). Examples of types of harm to individuals include, but are not limited to, the potential for blackmail, identity theft, physical harm, discrimination, or emotional distress. Organizations may also experience harm as a result of a loss of sensitive PII maintained by the organization, including but not limited to administrative burden, financial losses, loss of public reputation and public confidence, and legal liability.

² Throughout the Plan, the term CIRTs refer to both the DOC CIRT and Bureau/Operating Unit (BOU) CIRT, except where otherwise specified.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



[[NIST SP 800-122](#)].

➤ **Major Incident** Incidents requiring a report to Congress no later than seven (7) days after the date on which the Department has considered the totality of circumstances of the affects the risk poses to the Department or Bureau/Operating Unit (BOU) and individuals and concluded a major incident has occurred. Incidents are considered major when:

- The information involved is Classified, Controlled Unclassified Information (CUI), or PII; the incident resulted in the loss of critical service availability for all users or for at least 10,000 users, for eight hours or more; and the potentially compromised information poses a risk of harm to the Department or BOU and individuals.
 - a. The Department CIO shall document a determination that potentially compromised information does not pose a risk of harm to the affected organizations and individuals as well as any risk mitigations in place.

Or

- The information involved is Classified, CUI, or PII; the incident resulted in the unauthorized modification, deletion, exfiltration of, or access to any records:
 - a. Related to 10,000 or more individuals; or
 - b. Compromised or likely to result in a significant impact to Department mission, public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence;and the potentially compromised information poses a risk of harm to the affected organizations and individuals.
 - a. The Department CIO shall document a determination that potentially compromised information does not pose a risk of harm to the Department or BOU and individuals, as well as any risk mitigations in place.

➤ **Need to Know** - Information or data that is restricted due to its sensitive nature and the information is only given when needed or authorized.

➤ **Personally Identifiable Information (PII)** Information that can be used to distinguish or trace an individual's identity, such as name, Social Security number (SSN), biometric records, etc., alone, or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

- Sensitive PII is personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.
- Some forms of PII are sensitive as stand-alone data elements. Examples of such



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

PII include: SSN, driver's license or state identification number, passport number, Alien Registration Number, or financial account number. SSNs including truncated SSNs revealing only the last four digits are considered sensitive PII, both stand-alone and when associated with any other identifiable information.

- Other data elements such as citizenship or immigration status; medical information; ethnic, religious, sexual orientation, or lifestyle information; and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred), are also sensitive PII.
 - Additionally, the context of the PII may determine whether it is sensitive, such as a list of names of employees with poor performance ratings.
- **Privacy Act (PA) Incident** Disclosure of official records containing individually identifiable information that is prohibited by 5 U.S.C. § 552a, or regulations established thereunder. A PA incident occurs when an officer or employee of the Department, who by virtue of employment or official position with possession of, or access to records, discloses the material in any manner to any person or agency not entitled to receive it. NOTE: PA protection is based on how an individual's personal information is maintained by the government. If personal information is maintained by the government in a manner that is searchable by a personal identifier, it is PA information that must be covered under a published System of Records Notice (SORN). Disclosure of a PA record covered by a particular SORN without an identified routine use or another PA exception is considered a PA incident.³
- **Risk** The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. [[NIST FIPS 200](#)].
- **Low** is defined as the loss of confidentiality, integrity, or availability that is expected to have a **limited** adverse effect on organizational operations, organization assets or individuals. Breach incidents resulting from the following may be defined as Low if there was no failure of a Commerce IT security control:
 - a. An individual exposed his/her own sensitive PII.
 - b. A PII incident resulted from personal use of Commerce IT.

³ The twelve exceptions to the “No Disclosure Without Consent Rule” are: 1) “need to know” within agency; 2) required FOIA disclosure; 3) routine uses; 4) Bureau of the Census; 5) statistical research; 6) National Archives and Records Administration; 7) law enforcement request; 8) health or safety of an individual; 9) Congress; 10) General Accountability Office; 11) court order; and 12) Debt Collection Act. Additional information is available on the U.S. Department of Justice website: [Overview of the Privacy Act of 1974](#).

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



- **Moderate** is defined as the loss of confidentiality, integrity, or availability that is expected to have a **serious** adverse effect on organizational operations, organization assets or individuals.
 - **High** is defined as the loss of confidentiality, integrity, or availability that is expected to have a **severe or catastrophic** adverse effect on organizational operations, organization assets or individuals.
- **Security Control** The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [NIST FIPS 200]. For the protection of PII, security controls may include password protection, data encryption, full-disk encryption, or “auto-wipe” and “remote kill” features that provide the ability to protect a lost device by remotely disabling accessibility to data.
 - **Substitute Notification** A supplemental notification of an incident breach which keeps potentially affected individuals informed when there is insufficient contact information or a means by which affected individuals are informed collectively. A substitute notification consists of a conspicuous posting of the notification on the home page of the Department’s website and/or notification to major print and broadcast media, including major media in areas where the potentially affected individuals reside. Substitute notification includes phone numbers and email for affected individuals to use.

3.0 Roles and Responsibilities

3.1 Bureau/Operating Unit CIRT (BOU CIRT)⁴

- Reports all sensitive PII breach incidents within one (1) hour of discovery/detection to the SAOP/CPO, **AND** Enterprise Security Operations Center (ESOC).
- Reports all incidents to the SAOP/CPO at: cpo@doc.gov.
- Reports all incidents to the ESOC at: ESOC@doc.gov or 202-482-4000.
- Provides information on all sensitive PII breach incidents in the initial incident report (or as much of the information as known) in the format provided in [Appendix A](#)
- Ensures an initial risk of harm rating (Low, Moderate, or High) is assigned by the BCPO as part of the initial reporting for each PII incident using [Appendix B](#) - Risk Level Evaluation Matrix.

⁴Throughout this Plan, Bureau/Operating Unit CIRT (BOU CIRT) may refer to the Bureau’s/Operating Unit’s Privacy Office, Information Technology Security Officer (ITSO), or Information System Security Officer (ISSO) as prescribed by the Bureau’s/Operating Unit’s policies/processes, Service Level Agreement (SLA), and/or Memorandum of Understanding (MOU).



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

- Investigates all sensitive PII breach incidents within 48 hours of the incident discovery/detection and provides a follow-up report to the SAOP/CPO, ESOC, and BCPO. Investigates means that the following information has been documented in an incident report and submitted to the ESOC and SAOP/CPO: initial risk rating, mitigation and corrective/remedial actions, and any details/special circumstances missing from the initial report.
- Continues to investigate the incident, as necessary, and follows-up on all open incidents as part of the weekly SAOP/CPO reporting until the incident is closed out.
- Ensures the Privacy Task Force Package is built by the BCPO with coordination of the SAOP/CPO for Moderate and High risk incidents, if required.
- Ensures all applicable compliance documentation is identified, such as SORNs, Privacy Impact Assessments, and privacy notices, when responding to a breach incident.
- For PA and BII incidents involving no breach of sensitive PII, ensures PA incident without PII is turned over to the Bureau Chief Counsel (BCC) for investigation.
- Coordinates with BCPO to consult with the BCC as appropriate on BII incidents without sensitive PII to determine if a Trade Secrets Act violation occurred, dates of referral to the BCC for investigation are documented and sensitive PII portion of breach is closed.
- For PA and BII incidents which do involve breach of sensitive PII, ensures BCC notification of BII/PA aspects of incident, continuation of PII processing noting BII/PA efforts in parallel, and BCC instructions are followed to close BII/PA portion of incident.
- In instances where a PA violation occurs solely because an individual sends PA information via an unencrypted email, the BCPO's investigation clearly indicates that the violation via the unencrypted email was inadvertent, and remedial measures have already been taken to mitigate the PII breach, ensures that the BCPO does not refer the matter to the BCC for further review.
- Ensures the appropriate Property Management Office is notified of the loss when it involves network server, desktop computer, laptop computer, notebook computer, or other media and/or storage equipment, so that appropriate property management controls can be considered.
- Ensures notification to the Office of Inspector General (OIG), when necessary (e.g., intentional acts, criminal acts).
 - The OIG has discretion to contact the Attorney General/Department of Justice.
- Ensures notification to the appropriate law enforcement authorities:
 - Office of Security (OSY) and/or the Bureau-managed police force, when applicable;
 - Local law enforcement (Police Department), if incident involves theft from locations other than the workplace (e.g., laptop stolen from personal or government vehicle, laptop stolen from home); or

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



- Federal Protective Service (FPS), if incident involves theft from workplace locations that include facilities managed by the General Services Administration (GSA).
- Documents completion of all appropriate corrective/remedial actions in the incident report prior to close-out of PII incident.
- Supports and participates in tabletop exercise with the Task Force in order to practice a coordinated response to a breach, assist to refine and validate the Plan, and assist to further identify potential weaknesses in the Department's response capabilities.

3.2 Bureau Chief Privacy Officer (BCPO)⁵

- Ensures effective BOU execution of each breach response.
- Represents BOU in all Commerce Privacy Program meetings/events.
- Ensures all BOU sensitive PII incidents are reported within one (1) hour of discovery/detection to the SAOP/CPO, and ESOC.⁶
- Ensures the BOU PII incident reporting process requires collection of all [Appendix A](#) identified fields of information.
- Evaluates all BOU PII incidents in accordance with [Appendix B](#) Risk Level Evaluation Matrix and assigns a risk of harm rating at initial report, changing as necessary upon completion of the investigation.
- Notifies the appropriate Property Management Office of the loss when it involves network server, desktop computer, laptop computer, notebook computer, or other media and/or storage equipment, so that appropriate property management controls can be considered.
- Notifies the OIG, when necessary (e.g., intentional acts, criminal acts)
 - The OIG has discretion to contact the Attorney General/Department of Justice.
- Notifies to the appropriate law enforcement authorities:
 - Office of Security (OSY) and/or the Bureau-managed police force, when applicable;
 - Local law enforcement (Police Department), if incident involves theft from locations other than the workplace (e.g., laptop stolen from personal or government vehicle, laptop stolen from home); or
 - Federal Protective Service (FPS), if incident involves theft from workplace locations that include facilities managed by the General Services Administration (GSA).
- Ensures all BOU PII incidents are under investigation within 48 hours of the incident discovery/detection and a follow-up report has been submitted to the SAOP/CPO and

⁵ Includes privacy officers in Operating Units.

⁶ As indicated in [OMB Memorandum M-17-05](#), "Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements (November 4, 2016).



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

ESOC. Under investigation means that the following information has been documented in an incident report and submitted to the ESOC and SAOP/CPO: initial risk rating, mitigation and corrective/remedial actions, and any details/special circumstances missing from the initial report.

- Builds the Privacy Task Force Package in coordination with the SAOP/CPO for Moderate and High risk incidents, if required.
- Identifies all applicable compliance documentation, such as SORNs, Privacy Impact Assessments, and privacy notices, when responding to a breach.
- Ensures appropriate management attention is given to repeat offenders.
- Maintains thorough records of PII incidents from the initial report through the completed response.
- Ensures completion of corrective/remedial actions for each PII incident and ensures BOU CIRT has documented completion of these actions in the incident report prior to close-out of PII incident.
- Closes Low risk incidents and provides closure notification to SAOP/CPO and ESOC.
- Sends closure concurrence requests for Moderate and High risk PII incidents to the SAOP/CPO.
- For PA and BII incidents involving no breach of PII, turns over PA incidents without PII to the BCC for investigation, coordinates with BOU CIRT to consult with the BCC as appropriate on BII incidents without PII to determine if a Trade Secrets Act violation occurred, documents dates of referral to the BCC for investigation, and closes PII portion of breach.
- For PA and BII incidents which do involve breach of PII, notifies the BCC of BII/PA aspects of incident, continues PII processing noting BII/PA efforts in parallel, and follows BCC instructions to close BII/PA portion of incident.
 - In instances where a PA violation occurs solely because an individual sends PA information via an unencrypted email, the BCPO's investigation clearly indicates that the violation via the unencrypted email was inadvertent, and remedial measures have already been taken to mitigate the PII breach, the BCPO is not required to refer the matter to the BCC for further review.
- Provides training to BOU personnel regarding the handling of PII breach response, as needed.
- Delegates a BCPO responsibility only to fully qualified individuals and designation is made in writing to the SAOP/CPO (Sample delegation of authority memorandum is provided in [Appendix C](#)).
- Ensures BOU policies and training are updated, as appropriate, in response to problems identified by a specific incident or trends indicated by several incidents.
- Ensures that contract terms necessary for the Department to respond to a breach are included in contracts when a contractor collects or maintains Federal information on

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



behalf of the Department or uses or operates an information system on behalf of the Department.

- Provides reporting to the Bureau Senior Management as necessary.
- Supports and participates in tabletop exercise with the Task Force in order to practice a coordinated response to a breach, assist to refine and validate the Plan, and assist to further identify potential weaknesses in the Department's response capabilities

3.3 Enterprise Security Operations Center (ESOC)

- Reports all cyber PII incidents within one (1) hour of notification to the SAOP/CPO and the US-CERT by completing the US-CERT Incident Reporting System form.
- Ensures all non-cyber PII incidents have been reported to the SAOP/CPO within one (1) hour of notification.
- Requests status updates when needed from the BCPO and/or BOU CIRT.
- Provides closure notification to US-CERT and SAOP/CPO for all cyber low risk PII incidents; provides closure notification to US-CERT for all cyber moderate/high risk PII incidents; and provides closure notification to SAOP/CPO for all non-cyber low risk PII incidents.
- Provides a quarterly report to the SAOP/CPO detailing the status of each breach reported to the ESOC.

3.4 Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)

- Serves as Chair of the Task Force.
- Provides reports about Task Force actions to the Privacy Council, ensuring lessons learned are used to implement preventative actions.
- Convenes mandatory Task Force meetings when a breach constitutes a major incident and determines frequency of all other Task Force meetings.
- Holds a tabletop exercise annually with the Task Force in order to practice a coordinated response to a breach, further refine and validate the Plan, and identify potential weaknesses in the Department's response capabilities.
- Receives reports of all PII incidents at: cpo@doc.gov.
- Ensures effective execution of each breach response.
- Meets regularly with the Privacy Council to ensure effective execution of BOU level breach response.
- Provides closure concurrence for Moderate and High risk PII incident reports.
- Provides quarterly PII metrics.
- Maintains thorough records of PII incidents from the initial report through the completed response.
- Provides training to DOC employees and contractors regarding preparing for and the handling of PII breach response, as needed.
- Reviews the quarterly status report received from the ESOC and validates the reports accurately reflect the status of each reported breach.
- Reviews reports and determines appropriate action, such as developing new policy,



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

- updating existing policies, improving training and awareness, etc.
- Provides reporting to the Secretary, Deputy Secretary, and the Executive Management Team (EMT), as necessary.
- Develops training for individuals with access to Federal information and information systems on how to identify, report, and respond to a breach.
- Ensures routine uses are in all PA System of Records Notices (SORNs) for the disclosure of information necessary to respond to a breach either of the Department's PII or to assist another agency in its response to a breach.

3.5 DOC PII Breach Response Task Force

Consistent with the OMB guidance, the Task Force will consist of the following permanent members (or their designees):

- Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), Chair
- General Counsel (legal counsel)
- Chief Information Officer (CIO) or the CIO's designee
- Senior Agency Information Security Officer (SAISO) or the SAISO's designee
- Chief Financial Officer/Assistant Secretary for Administration
- Assistant Secretary for Legislative and Intergovernmental Affairs (OLIA) (legislative affairs official)
- Chief of Staff, Office of the Secretary
- Director, Office of Public Affairs (OPA) (communication official)
- Director, Office of Policy and Strategic Planning
- Director, Office of Human Resources Management
- Office of Security (OSY), Attends on an as needed basis
- Office of Inspector General (OIG), Advisory Role

Each member shall participate in Task Force meetings when convened by the SAOP/CPO and shall provide his/her expertise as needed to provide the best response and lessons learned for each incident. Decisions and recommendations are made by consensus. In addition, the Task Force members must participate in the tabletop exercise held annually.

The Bureau/Operating Unit (BOU) that initially reported an incident may be asked to attend a Task Force meeting to discuss the specific details of the incident, help to formulate an appropriate response, and assist in executing the breach response.

The Task Force, or a designated representative, may also work closely with other Federal agencies, offices, or teams to share lessons learned or help to develop government-wide guidance for handling PII incidents.

If a breach involves DOC employee PII, then the Task Force has the discretion to notify the relevant and affected senior management while the response is being developed and executed.

As Chair of the Task Force, the CPO shall provide reports to the Privacy Council, as appropriate.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



In order to effectively and efficiently respond to a breach, the breach response team may need to consult with the following personnel:

- Budget and procurement personnel who can provide expertise when a breach involves contractors or an acquisition, or who may help procure services such as computer forensics, cybersecurity experts, services, or call center support;
- Human resources personnel who may assist when employee misconduct results in a breach or when an employee is suspected of intentionally causing a breach or violating agency policy;
- Law enforcement personnel who may assist when a breach involves the violation or suspected violation of law or when a breach is the subject of a law enforcement investigation;
- Physical security personnel who may investigate a breach involving unauthorized physical access to a facility or when additional information regarding physical access to a facility is required; and,
- Other agency personnel who may be necessary according to specific agency missions, authorities, circumstances, and identified risks.

3.6 Office of the Chief Information Officer (OCIO)

- Provides information technology guidance in responding to suspected or known breaches, such as an evaluation of controls or computer forensics investigation and analysis.
- Working with the affected BOU, takes steps to control and contain the breach, such as:
 - Monitor, suspend, or terminate affected accounts;
 - Modify computer access or physical access controls; and
- Takes other necessary and appropriate action without undue delay and consistent with current requirements under FISMA.

3.7 Office of General Counsel (OGC)/Bureau Chief Counsel (BCC)

- Provides legal support and guidance in responding to a PII incident.
- Provides legal review of BII and PA incidents.

3.8 Office of Inspector General (OIG)

- Determines whether to notify the Department of Justice or other law enforcement authorities following a breach.
- Advises the Task Force about ongoing investigations and the timing of external notifications that may affect such investigations.

3.9 Office of Legislative and Intergovernmental Affairs (OLIA)

- Coordinates all communications and meetings with members of Congress and their staff when necessary.
- Ensures major incidents are reported to Congress within the established seven (7) days.



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

3.10 Privacy Council

- Receives reports about the actions of the Task Force.
- Analyzes reports from the Task Force to make recommendations for privacy policy changes.
- Approves changes to this Plan as recommended by the SAOP/CPO.

3.11 Office of Public Affairs (OPA)

- Coordinates notifications to individuals, the media, and other third parties as appropriate.

3.12 Supervisor/Manager

- Ensures compliance to Federal laws, rules, regulations, and Departmental privacy policy.
- Ensures employee/contractor completes training to properly safeguard information.
- Takes steps to prevent a breach from occurring (e.g., ensuring laptops are password protected and encrypted, and providing shredder for staff, etc.).
- Recognizes a privacy incident and upon discovery/detection, immediately reports a suspected or confirmed breach incident to the BCPO and BOU CIRT (NOTE: Supervisor/manager does not forward sensitive PII when reporting incident). Information to report verbally or by email includes:
 - Name
 - Contact information
 - Description of incident
 - Date, time, and place incident occurred
 - Type of media or device involved
 - Any controls enabled to mitigate loss
 - Number of individuals potentially affected
- Maintains or documents records of information and/or actions relevant to the incident.
- Provides advice, expertise, and assistance to the BCPO and/or BOU CIRT, as needed.
- Assists with the investigation and corrective/remedial actions, as needed.
- Ensures appropriate consequences for repeat offenders.

3.13 Employee/Contractor

- Adheres to Federal laws, rules, regulations, and Departmental privacy policy and is aware of the consequences for violating such directives.
- Successfully completes training regarding his/her respective responsibilities relative to safeguarding information.
- Takes steps to prevent a breach from occurring (e.g., encrypting sensitive PII in emails and on mobile computers, media, and devices, destroying paper containing sensitive PII, and locking computer system when leaving it unattended, etc.).
- Recognizes a privacy incident and upon discovery/detection, immediately reports a suspected or confirmed breach incident to his/her supervisor, BCPO, and BOU CIRT

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



(NOTE: Employee/contractor does not forward sensitive PII when reporting incident).
Information to report verbally or by email includes:

- Name
- Contact information
- Description of incident
- Date, time, and place incident occurred
- Type of media or device involved
- Any controls enabled to mitigate loss
- Number of individuals potentially affected
- Maintains or documents records of information and/or actions relevant to the incident.
- Completes corrective/remedial actions, if appropriate.

4.0 DOC PII/BII/PA Incident Response Process

(See [Appendix D](#) for process flowchart)

- A) DOC employee or contractor suspects or becomes aware of a PII/BII/PA incident.
- B) DOC employee or contractor reports the incident immediately to his/her BCPO/BOU CIRT⁷ **AND** to his/her immediate supervisor.
- C) The BCPO/BOU CIRT reports the PII incident to the SAOP/CPO and ESOC within one (1) hour of discovery/detection. Simultaneously the following occurs:
 - 1) The BCPO and BOU CIRT continue to investigate the incident.
 - 2) The BCPO/BOU CIRT determines if the incident is a BII or PA incident.
 - i. If the incident is a BII or PA incident which DOES NOT contain PII
 - (1) BCPO/BOU CIRT turns over the PA incident without PII to the BCC for investigation and consults with the BCC as appropriate on BII incidents without PII to determine if a Trade Secrets Act violation occurred.
 - (2) BCPO/BOU CIRT documents date of referral to BCC for investigation and closes PII portion of the incident.
 - ii. If the incident is BII or PA incident and DOES contain PII
 - (1) BCPO/BOU CIRT continues with PII incident processing **AND**

⁷ Some BOUs report directly to the ESOC (See Appendix E for additional information).

Department of Commerce PII, BII, and PA Breach Response and Notification Plan

- (2) BCPO/BOU CIRT notifies the BCC of the BII/PA aspects of the incident and follows BCC instructions to close BII/PA portion of the incident while proceeding with the PII incident response in parallel.
 - 3) The BCPO uses [Appendix B](#) Risk Level Evaluation Matrix to assign an initial risk of harm rating for the PII incident.
 - 4) The BCPO/BOU CIRT notifies the Property Management Office, OIG, and/or law enforcement, if applicable.
 - 5) The BCPO/BOU CIRT documents planned and completed corrective/remedial actions.
 - 6) The BCPO/BOU CIRT provides a report of the results of the investigation to the SAOP/CPO and the ESOC within 48 hours of initial incident reporting.
 - i. If an incident is handled directly by the ESOC, then the ESOC shall provide the report to the SAOP/CPO.
 - ii. Low risk of harm rated incidents may be closed by the BCPO only after fully documenting the incident in accordance with [Appendix A](#) of this plan and updating the incident report with confirmation that corrective/remedial actions have been completed.
 - iii. Moderate and High risk of harm rated incidents require SAOP/CPO concurrence for closure.
 - iv. All major incidents require SAOP/CPO concurrence for closure.
- D) When reviewing privacy compliance documentation in response to a breach, the SAOP considers the following:
- 1) Which SORNs, PIAs, and privacy notices apply to the potentially compromised information.
 - 2) If PII maintained as part of a system of records needs to be disclosed as part of the breach response, is the disclosure permissible under the Privacy Act and how the Department will account for the disclosure.
 - 3) If additional PII is necessary to contact or verify the identity of individuals potentially affected by the breach, will new or revised SORNs or PIAs be required.
 - 4) Whether all relevant SORNs, PIAs, and privacy notices are accurate and up-to-date.
- E) When determining the potential information sharing that may be required in response to a breach, the SAOP considers the following:
- 1) Is the information sharing consistent with existing agreements;
 - 2) How the PII is transmitted, protected, and retained during this phase; and
 - 3) If the information may be shared with third parties.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



- F) The SAOP/CPO determines whether to convene a meeting of the Task Force for Moderate and High Risk of harm and Major incidents based on several factors, including:
- Risk and type of harm to the affected individuals and/or the DOC
 - Whether the acts leading to the breach were intentional or accidental
 - Number of affected individuals
 - Security controls applied to the affected PII
 - Other factors enumerated in the section entitled “Risk of Harm Analysis Factors and Rating Assignment”
 - Any other basis on which the SAOP/CPO believes the incident warrants attention of the Task Force
- 1) If the SAOP/CPO determines that the Task Force needs to be convened
- i. The BCPO builds a Privacy Task Force Package in coordination with the SAOP/CPO. The Privacy Task Force Package includes:
 - PII summary of incident
 - Notification letter
 - OPA talking points
 - Additional documents as requested
 - ii. The Task Force concurs, modifies, and/or approves corrective/remedial actions to be taken.
 - iii. The BCPO/BOU CIRT confirms and documents completion of corrective/remedial actions directed by the Task Force in close coordination with the SAOP/CPO and submits a request for closure.
 - iv. The SAOP/CPO follows up to ensure that the breach response is carried out effectively and approves closure request.
 - v. The BCPO/BOU CIRT notifies ESOC to close incident.
- 2) If the SAOP/CPO determines that the Task Force DOES NOT need to be convened
- i. The BCPO/BOU CIRT confirms and documents completion of corrective/remedial actions and submits a request for closure to the SAOP/CPO at CPO@doc.gov.
 - ii. The SAOP/CPO follows up to ensure that the breach response is carried out effectively and approves closure request.
 - iii. The BCPO/BOU CIRT notifies ESOC to close incident.

5.0 Risk of Harm Analysis Factors and Rating Assignment

Based on the risk of potential harm and other factors provided in this section, the BCPO shall assign an initial rating level of the risk of harm Low, Moderate, or High for each



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

reported PII incident. The rating level of the risk of harm will be used to assist the SAOP/CPO in making a determination as to whether the Task Force should be convened. The analysis and risk rating should be used by the Task Force to determine the appropriate response.

In assessing the risk of harm, it is important to consider all potential harm to both the affected individuals and the Department.

Potential harm to the individual may include, but is not limited to:

- Identity theft
- Blackmail
- Embarrassment
- Physical harm
- Discrimination
- Emotional distress
- Inappropriate denial of benefits

Potential harm to the Department may include, but is not limited to:

- Administrative burden
- Cost of remediation
- Loss of public trust
- Legal liability

Additional factors the SAOP considers for determining the rating level for the risk of harm include:⁸

- Security controls in place at the time of the breach.
- Type of breach and evaluation of each data element as well as evaluation of the sensitivity of all the data elements combined.
- Number of individuals affected by the breach.
- Sensitivity of the PII and the context in which it was used.
- Likelihood the information is accessible and usable which includes:
 - **Security safeguards** for whether the PII was properly encrypted or rendered partially or completely inaccessible by other means;
 - **Format and media** if the format of the PII makes it difficult and resource-intensive to use;
 - **Duration of exposure** to find out how long the PII was exposed; and
 - **Evidence of misuse** to indicate or confirm that the PII is being misused or never accessed.
- Likelihood that the breach may lead to harm.

⁸ See NIST SP 800-122, [Guide to Protecting the Confidentiality of PII \(Section 3\)](#) for additional information about assessing the impact level for a particular collection of PII.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



- Specific legal obligations to protect the PII or report its loss.
- Whether the acts leading to the breach were intentional or accidental.
- The extent to which the PII identifies or disproportionately impacts a vulnerable population (e.g., children, senior citizens, active duty military, confidential informants, individuals with disabilities, victims, or other populations considered vulnerable).
- The permanence of the breach including the continued relevance and utility of the PII over time and whether it is easily replaced or substituted.

6.0 Breach Notification and Remediation

The appropriate response to a breach of PII may include notification to the affected individuals or third parties, as well as specific corrective/remedial actions. The SAOP/CPO (and/or Task Force, if convened) shall recommend a response plan to mitigate risks to the individual and the Department. The SAOP/CPO and/or Task Force should consider the options available to protect potential victims of identity theft and other harm.

Options may include:

- Providing notice of the breach to affected individuals.
- Engaging a third party to conduct a data breach analysis to determine whether a particular data loss appears to be resulting in identity theft.
- Providing credit monitoring services.⁹
- Referring individuals to websites providing guidance about ID Theft, such as the [Federal Trade Commission Consumer Information](#) site.
- Providing a toll-free hotline or website for affected individuals to obtain additional information.

6.1 Notifying Individuals

The SAOP/CPO (and/or Task Force, if convened) shall determine whether individuals should be notified based on the rating level of the risk of harm, as well as the analysis leading to the assigned rating level. The OIG shall notify the SAOP/CPO and/or Task Force and request a delay if notice to individuals or third parties would compromise an ongoing law enforcement investigation. Unless notification to individuals is delayed or barred for law enforcement or national security reasons, the notice should be provided within 30 days or as expeditiously as practicable and without unreasonable delay.

⁹ If a decision is made to retain monitoring services, the SAOP/CPO and/or Task Force should consult the OMB Memorandum M-07-04, [Use of Commercial Credit Monitoring Services Blanket Purchase Agreements](#), (December 22, 2006).



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

The SAOP/CPO and/or Task Force shall consider the following elements in the notification process:

- Timing of the notice
- Source of the notice
- Contents of the notice
- Method of notification
- Special Considerations
- Preparation for follow-on inquiries

The contents of the notice to individuals shall include:

- A brief description of what happened, including the date(s) of the breach and of its discovery.
- To the extent possible, a description of the types of information involved in the breach.
- A statement of whether the information was encrypted or protected by other means, when it is determined that disclosing such information would be beneficial to the potentially affected individuals and would not compromise the security of the information system.
- A brief description of what the Department is doing to investigate the breach, mitigate losses, and protect against further breaches.
- Contact information for individuals who have questions or need more information, such as a toll-free number, website, or postal address.
- Steps for individuals to undertake in order to protect themselves from the risk of ID theft.
- Information about how to take advantage of credit monitoring or other service(s) that the Department or BOU intends to offer.
- The signature of the relevant senior Department management official (Head of Operating Unit or Secretarial Officer).

6.2 Method of Notification

The SAOP/CPO will determine the method of notification to the potentially affected individuals. The best method for providing notification will be dependent upon the number of individuals affected, available contact information for the potentially affected individuals, and the urgency in which the individuals need to receive the notification. Notification should be provided by:

- First-Class Mail
- Telephone
- Email¹⁰

¹⁰ While email notification may be appropriate, it is not recommended as the primary form of notification.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



- Substitute Notification

6.3 Notification/Reporting Requirements

The SAOP/CPO (and/or Task Force, if convened) shall determine whether notification to any third parties is necessary. Potential third parties may include:

- **Law Enforcement** Local law enforcement or Federal Protective Services; the IG may notify the FBI.
- **Media and the Public** The Director of the Office of Public Affairs, in coordination with the SAOP/CPO and/or Task Force and the affected Bureau public affairs staff, will be responsible for directing all communications with the news media and public. This includes the issuance of press releases and related materials on www.commerce.gov or a BOU website.
- **Financial Institutions** If the breach involves government-authorized credit cards, the DOC must notify the issuing bank promptly.¹¹ The SAOP/CPO and/or Task Force shall coordinate with the Department's Acquisitions Branch regarding such notification and suspension of the account.
- **Appropriate Members of Congress** The Assistant Secretary for Legislative and Intergovernmental Affairs, in consultation with the Task Force, shall be responsible to coordinate all communications and meetings with members of Congress and their staff.
- **Attorney General/Department of Justice** The Inspector General shall determine when to contact the Attorney General.
- **Others** – The SAOP/CPO and/or Task Force shall have the discretion to determine if any additional third parties should be notified.

7.0 Consequences

Employees are expected to familiarize themselves with their responsibilities with respect to the protection of PII, as well as their responsibilities in the event of a breach. Likewise, managers and supervisors should ensure that their employees have access to adequate training with respect to these responsibilities.

Failure to adhere to the requirements of this Plan may result in administrative or disciplinary action, up to and including removal from the Federal service.

¹¹ OMB M-07-16 requires bank notification in the event that PII related to government-authorized credit cards is involved in a breach.



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Appendix A – DOC PII Incident Report Content

The Department requires that the following elements be included in a PII Incident Report:

- Incident number
- Contact Person and Phone number
 - Breach reported by
 - Contact information
 - B/OU
 - Email
 - Phone Number
- Incident date/time
- Major Incident (Yes/No)
- Contractor System (Yes/No)
- Date/Time Reported to BOU-CIRT
- Date/Time Reported to US-CERT
- Date/Time Reported to Law Enforcement
- Repeat Offender (Yes/No) If Yes, include 2nd, 3rd offense
- Region
- Status (Open/Closed)
- Follow-up within 48 Hours (Yes/No)
- Summary of Circumstances Summarize the facts or circumstances of the theft, loss, or compromise of PII as currently known, including:
 - A description of the parties involved in the breach;
 - The physical or electronic storage location of the information at risk;
 - If steps were immediately taken to contain the breach;
 - Whether the breach is an isolated occurrence or a systematic problem;
 - Who conducted the investigations of the breach, if applicable; and
 - Any other pertinent information.
- Type(s) of PII Disclosed or Compromised (e.g., SSN, truncated or partial SSN, DOB, address, driver's license number, passport number, or credit card)
 - Lost information or equipment, (e.g., laptop or table, desktop, smartphone, external storage devices, or paper files).
 - Stolen information or equipment, (e.g., laptop or table, desktop, smartphone, external storage devices, or paper files).
 - Unauthorized equipment (e.g., using an unauthorized personal device server or email account to store PII).
 - Unauthorized disclosure (e.g., email sent to incorrect address, oral or written disclosure to unauthorized person, or disclosing documents publicly with sensitive information not redacted).
 - Unauthorized access (e.g., an unauthorized employee or contractor access information or an information system).
 - Unauthorized use (e.g., employee with agency-authorized access to database or

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



file access and uses information for personal purposes rather than for official purposes).

- Storage Medium (e.g., unencrypted, email, or unsecure website)
- Controls Enabled- Password Protection and/or Encryption
- Number of Individuals Affected (internal or external to DOC)
- FISMA System ID Number(s)
- Identify Relevant Specific PIA or SORNs
- BII or Privacy Act Violation (BII/PA/No)
- Risk Assessment and Employee Making Assessment
- Corrective and Remedial Actions (include status e.g., pending, confirmed)



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Appendix B – Risk Level Evaluation Matrix

In analyzing a PII incident, the BCPO must consider the following six (6) critical risk of harm factors:

- The nature of the data compromised, level of risk in light of the context of the data, and broad range of potential harm that may result from disclosure;
- Whether the incident occurred during the performance of an official “Commerce work related activity”;
- The likelihood that the PII will be or has been used in an unauthorized manner;
- DOC’s ability to mitigate the risk of harm to affected individuals;
- The likelihood that the breach may lead to harm (e.g., mental or emotional distress, financial harm, embarrassment, harassment or identity theft); and
- The number of individuals affected by the breach.

To address the first of the six (6) critical factors, the BCPO must evaluate whether the type of breached PII data elements constitute the type of information that may pose a risk of identity theft and whether a significant and immediate identity theft risk exists. Examples of data which present an identity theft risk include: (1) SSN, including truncated form; (2) date of birth, place of birth, or mother’s maiden name; (3) passport number, financial account number, credit card number, medical information, or biometric information; (4) potentially sensitive employment information (e.g., personnel ratings, disciplinary actions, and results of background investigations) and criminal history; or (5) any information that may stigmatize or adversely affect an individual. If there is a significant and immediate risk of identity theft, the BCPO must immediately contact the Commerce SAOP/CPO who will determine whether to convene the Privacy Task Force and advise on how to proceed. If no significant and immediate risk of identity theft is implicated, the BCPO will use the Commerce Risk Level Evaluation Matrix to assess the five (5) remaining factors and assign an initial incident risk of harm rating.

Using the Risk Level Evaluation Matrix:

Step 1: From left to right, select the first “Breach Category” section of the Matrix that describes the general fact pattern of the incident.

Step 2: Then, from top to bottom, use the detailed facts of the incident to determine the appropriate response (Y/N/NDF) for each evaluation statement of the Matrix until all answers are documented. NOTE: Y (Yes); N (No); and NDF (Not Determining Factor)

Step 3: Finally, use the “Recommended Initial Risk Rating” row of the appropriate “Breach Category” with Y/N/NDF selections that match those of the incident to determine the risk of harm rating.

The risk of harm rating may be adjusted by the BPO to a higher rating as appropriate to reflect a unique mission impact. However, Commerce CPO concurrence is required prior to lowering an initial risk of harm rating. If PII was encrypted, the incident may be rated a Low risk of harm.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



Risk Level Evaluation Matrix

Critical Factors	Evaluation Statement	Breach Category																				Automatic Moderate Trigger	Automatic High Trigger
		PII Incidents Resulting for PII Owner Action and/or Personal Use						All Recipients Have Valid Need to Know and are Authorized to						All Recipients are Authorized, However One or More Recipient Does NOT have a Need to Know									
Association with an Official Duty	Sent by PII Owner and/or PII Owner is Sender's Family Member	Y	Y	N	N	N	Y														All Incidents with One or More Recipients NOT Authorized	All Incidents with One or More Recipients NOT Authorized Affecting Greater than 2500 Individuals	
	Personal Use (excludes Official Commerce Business)	Y	N	Y	Y	Y	N																
Likelihood PII will be used in Unauthorized Manner	Recipients have Need to Know	NDF	NDF	Y	N	NDF	NDF	YES						NO									
	Recipients are Authorized	NDF	Y	Y	Y	N	N	YES						YES									
Ability to Mitigate Risk of Harm	Exposed Only to DOC Personnel	NDF	Y	NDF	Y	NDF	NDF	Y	N	Y	Y	Y	N	N	Y	N	Y	Y	Y	N			N
	Exposed on Internet, non DOC system, or public/non DOC controlled facility	NDF	NDF	NDF	NDF	NDF	NDF	N	N	N	N	Y	Y	Y	N	N	N	N	Y	Y			Y
Likelihood Incident may lead to Harm	Quantity of PII (# of exposed fields of PII per person)	NDF	NDF	<10	<5	NDF	NDF	<10	>10	NDF	>10	NDF	NDF	<10	<5	>5	<5	>5	NDF	NDF	>3		
	# of Individuals Affected	NDF	NDF	<500	<250	NDF	NDF	<500	NDF	>500	NDF	>500	<500	NDF	<250	<250	>250	<250	>250	>100	NDF		
	Recommended Initial Risk Rating	LOW	LOW	LOW	LOW	MOD	MOD	LOW	LOW	MOD	MOD	MOD	MOD	MOD	LOW	LOW	MOD	MOD	MOD	MOD	MOD	MOD	HIGH

NOTE: If PII was encrypted, the incident may be rated a "Low" risk of harm.
 Y Yes
 N No
 NDF Not Determining Factor



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Examples: How to Use Risk Level Evaluation Matrix

Scenario 1: Resulting from PII Owner Action and/or Personal Use

John Doe, DOC employee, faxed his Form 1040 to the Loan Department at Capitol One Bank without notifying his loan officer to expect the document. Approximately four hours later, the loan officer informed John that he received the form from a contractor who was repairing the shredder in the bank. John was concerned that his identity had the potential of being compromised and notified his supervisor who reported the incident to his bureau CIRT since a DOC fax machine was used.

Analysis:

- Fax sent by PII owner (Y)
- Faxed document for personal use (Y)
- First recipient had need to know (NDF)
- First recipient authorized to receive information (NDF)
- Fax exposed only to DOC personnel (NDF)
- Fax exposed on Internet, non-DOC system, or public/non-DOC controlled facility (NDF)
- Quantity of PII (NDF)
- Number of individuals affected (NDF)

Rating: Low Risk

Scenario 2: Valid Need to Know and Authorized User

A supervisory payroll specialist sent an unencrypted email with attachments to a payroll specialist in the same division to ensure notification letters were sent to certain employees. The attachments contained information regarding child support payments which included sensitive PII (SSN, DOB) of 20 DOC employees.

Analysis:

- Recipient had need to know (Y)
- Recipient authorized to receive information (Y)
- Email exposed only to DOC personnel (Y)
- Email exposed on Internet, non-DOC system, or public/non-DOC controlled facility (N)
- Quantity of PII (<10)
- Number of individuals affected (<500)

Rating: Low Risk

Department of Commerce

Privacy Breach Notification Plan



Scenario 3: Authorized User, but One or More Recipients has no Need to Know

25 supervisors in the Los Angeles Field Office were granted access to the electronic Employee Relations files of 200 employees located in the Denver Field Office. These files contained sensitive PII (SSN, DOB, medical information, performance ratings, performance grievances, and disciplinary actions).

Analysis:

- Recipients had need to know (N)
- Recipients authorized to receive information (Y)
- Exposed only to DOC personnel (Y)
- Exposed on Internet, non-DOC system, or public/non-DOC controlled facility (N)
- Quantity of PII (>5)
- Number of individuals affected (<250)

Rating: Moderate Risk

Scenario 4: Not Authorized, Greater than 10 PII Fields, and Affecting More than 2500 Individuals

An employee incorrectly mailed Standard Form (SF)-85P, Questionnaire for Public Trust Positions, to 10 survey respondents, rather than to employees at the U.S. Office of Personnel Management. Each SF-85P contained SSN, DOB, POB, mother's maiden name, passport number, alien registration number, reason employment ended, police record, illegal drug activity, financial record, and delinquency on loans or financial obligations. 2,842 employees were affected.

Analysis:

- Recipients had need to know (N)
- Recipients authorized to receive information (N)
- Exposed only to DOC personnel (N)
- Exposed on Internet, non-DOC system, or public/non-DOC controlled facility (Y)
- Quantity of PII (>10)
- Number of individuals affected (>2500)

Rating: High Risk



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Appendix C – Delegation of Authority Memorandum

Bureau Chief Privacy Officer (BCPO) Delegation of Authority Memorandum

MEMORANDUM FOR: *(Insert name of current SAOP/CPO)*
Senior Agency Official for Privacy/Chief Privacy Officer

FROM:
(Name of bureau) Bureau Chief Privacy Officer

SUBJECT: Delegation of Privacy Breach Authority for Bureau Chief Privacy Officer

In accordance with the Department of Commerce (DOC) PII, BII, and PA Breach Response and Notification Plan, I hereby appoint *(insert name of employee)* to act on behalf of the Bureau Chief Privacy Officer (BCPO) for privacy breaches. The employee identified above is qualified to manage the daily operations for privacy breaches and hereby delegated authority to *(check all that apply)*:

- Evaluate all Bureau/Operating Unit PII incidents in accordance with the Risk Level Evaluation Matrix and assign a risk of harm rating
- Ensure all Bureau/Operating Unit PII incidents are under investigation within 48 hours of the incident discovery/detection and a follow-up report has been submitted to the SAOP/CPO and ESOC
- Maintain thorough records of Bureau/Operating Unit PII incidents from the initial report through the completed response
- Ensure Bureau/Operating Unit CIRT has documented completion of all appropriate corrective/remedial actions in the incident report prior to close-out of the PII incident
- Close Low risk incidents and send closure concurrence requests for Moderate and High risk PII incidents to the SAOP/CPO

The delegation may be terminated at any time by written notice by the BCPO.

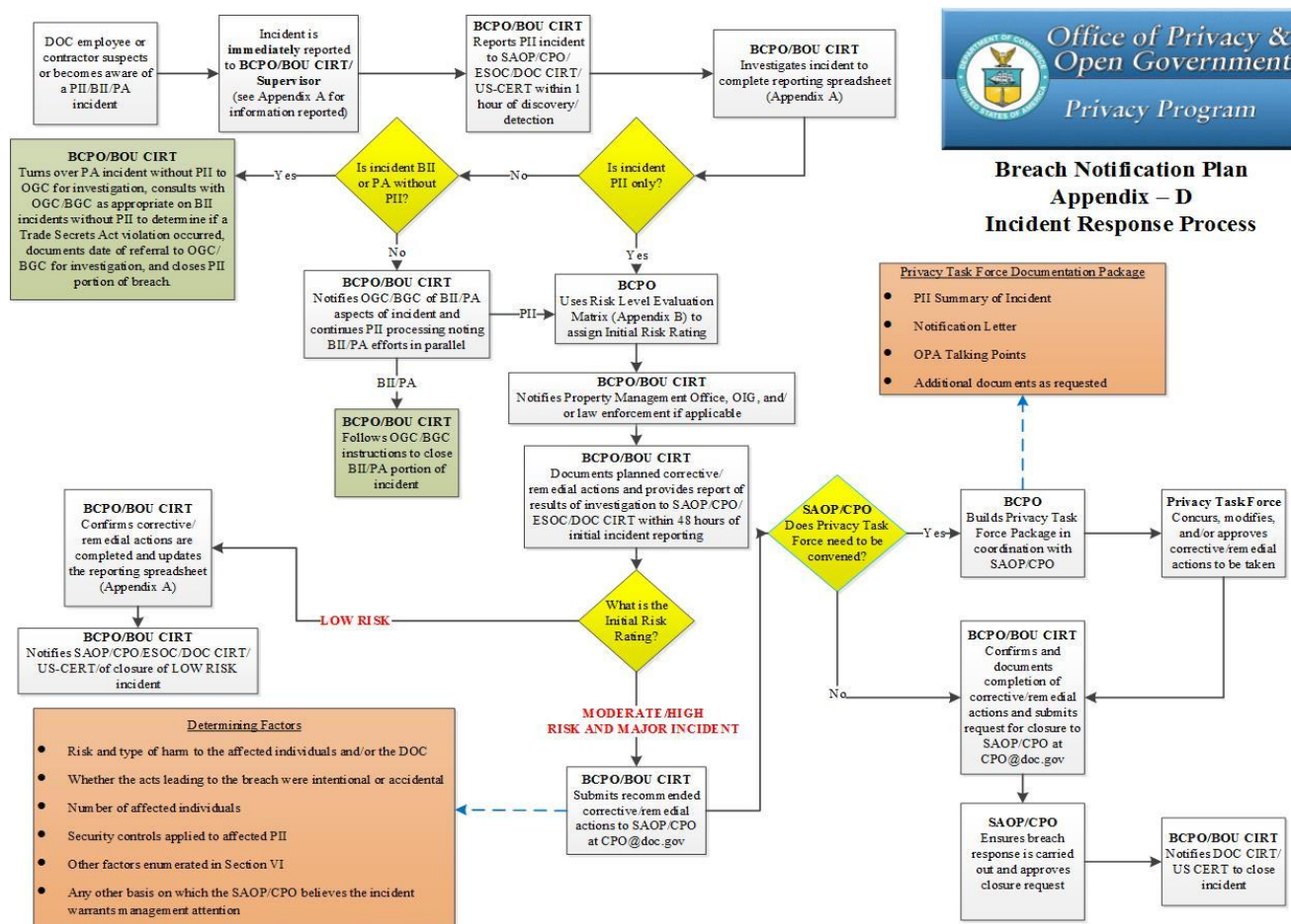
EMPLOYEE SIGNATURE

[Employee signature indicates that he/she has read, understands, and agrees to comply with the BCPO role and responsibilities.]

Department of Commerce PII, BII, and PA Breach Notification Plan



Appendix D Flowchart





Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Appendix E – Senior Agency Official for Privacy/Chief Privacy Officer and Commerce Operating Unit CIRT Reporting Offices

The ESOC and Bureau CIRTs shall report PII incidents directly to the SAOP/CPO.

- **Senior Agency Official for Privacy/Chief Privacy Officer (SAOP/CPO)**
 - cpo@doc.gov
 - (202) 482-1190, for immediate assistance only
- **Enterprise Security Operations Center (ESOC)**
 - ESOC@doc.gov
 - (202) 482-4000
 - <https://connection.commerce.gov/overview/about-doc-cirt>

PII incidents occurring in EDA, ESA, MBDA, NTIA, OIG, and OS shall be reported directly to ESOC.
- **Bureau of Economic Analysis (BEA) CIRT**
 - helpdesk@bea.gov
 - (301) 278-9407
- **Bureau of Industry and Security (BIS) IT Security**
 - BISITSecurity@bis.doc.gov
 - (202) 482-0623 or (202) 482-1188
- **Bureau of the Census (BOC) CIRT**
 - boc.cirt@census.gov
 - (301) 763-3333 or (877) 343-2010 (after hours)
- **International Trade Administration (ITA) CIRT**
 - CSC@trade.gov
 - (202) 482-1955 or (877) 206-0645 (toll free)
- **National Institute of Standards and Technology (NIST) CIRT**
 - itac@nist.gov
 - (301) 975-5375 (Gaithersburg, MD); (303) 497-5375 (Boulder, CO)
- **National Oceanic and Atmospheric Administration (NOAA) CIRT**
 - ncirt@noaa.gov
 - (301) 713-9111

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



- **National Technical Information Service (NTIS) CIRT**
 - secops@ntis.gov
 - (703) 605-6519

- **U.S. Patent and Trademark Office (USPTO) CIRT**
 - CyberSecurityInvestigations@uspto.gov
 - (571) 272-6700



U.S. Department of Commerce
Personally Identifiable Information (PII),
Business Identifiable Information (BII)
and Privacy Act (PA)
Breach Response and Notification Plan

Published July 2017

Guide to Conducting a PII Breach Table Top Exercise (TTX)

Prior to Conducting this TTX

1. Review the DOC PA, PII, and BII Breach Response Plan.
2. Review OMB Memorandum 17 12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.

Breach Response Team Members

1. Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)
2. General Counsel (legal counsel)
3. Chief Information Officer (CIO) or the CIO's designee
4. Senior Agency Information Security Officer (SAISO) or the SAISO's designee
5. Chief Financial Officer/Assistant Secretary for Administration
6. Assistant Secretary for Legislative and Intergovernmental Affairs (OLIA) (legislative affairs official)
7. Chief of Staff, Office of the Secretary
8. Director, Office of Public Affairs (OPA) (communication official)
9. Director, Office of Policy and Strategic Planning
10. Director, Office of Human Resources Management
11. Office of Security (OSY), Attends on an as needed basis
12. Office of Inspector General (OIG), Advisory Role
13. Bureau Chief Privacy Officers
14. Privacy Act Officers
15. Deputy Director for Departmental Privacy Operations
16. Departmental FOIA/PA Officer

Planning

1. Establish the objectives of the TTX. Some of your objectives may be:
 - a. Improve the understanding of the DOC Breach Response Plan.
 - b. Identify opportunities to improve the DOC Breach Response Plan and the Department's preparedness.
 - c. Identify interdependencies among agency organizations and third party service providers.
2. Plan the TTX logistics.
 - a. Determine the date.
 - b. Reserve a space with an appropriate clearance level, as well as any materials or multimedia support you may need, such as computer and display, whiteboard and markers, butcher block paper, handouts, and dial in capabilities.
 - c. Set a time limit for the TTX. This will help you choose an appropriate scenario and focus the conversation appropriately during the TTX.
 - d. Assign support staff roles.

- i. Determine what role you want your privacy program to play in the exercise. Individuals who are deeply involved in planning the TTX may need to take a step back during the exercise to avoid accidentally influencing the course of the exercise. In a TTX, privacy office representatives often act in an advisor or consultant role, responding to questions from other participants, rather than the active leaders they often are in an actual breach.
- ii. Identify a facilitator (Consider using a neutral facilitator). The facilitator has the primary responsibility for exercise conduct. This includes introducing and providing scenario updates, moderating the discussions to ensure players address exercise objectives and core capabilities, and ensuring everyone contributes to the discussion and relevant issues are explored as thoroughly as possible within the allotted time.
- iii. In addition to a facilitator, you will also need staff dedicated to:
 - 1. Taking notes. These notes will form the basis of the after action report.
 - 2. Tracking “parking lot” issues.
 - 3. Documenting when Breach Response Plan steps are completed.
- e. Create a participant roster to track attendance at the TTX.
- f. Consider what role you want Senior Executive Service (SES) members and other senior leaders to play. SES member participation may stifle the conversation. Consider using SES members or other senior leaders as floaters who give out real time feedback.

A sample agenda is below:

Time	Activity
[Month Day, Year]	
0000 - 0000	Registration
0000 - 0000	Welcome and Introductions
0000 - 0000	Exercise Overview
0000 - 0000	Module 1: Initial Response – Scenario Background
0000 - 0000	Break
0000 - 0000	Module 2: Response
0000 - 0000	Module 3: Recovery
0000 - 0000	Break
0000 - 0000	Hot Wash

Time	Activity
0000 - 0000	Closing Comments
0000 - 0000	Debrief (Facilitators and Evaluators only)

3. Develop a realistic breach scenario.

a. Choosing a scenario.

- i. Consider which high value assets, applications, or processes you may want to include in the scenario.
 1. You do not have to limit yourself to high value assets, but you want to make sure the scenario has stakes. A high profile system or program, or a scenario that involves risks to the reputation or operations of the agency may be more engaging and offer more avenues for the participants to explore.
- ii. Look at the Department's recent breaches, as well as any major breaches, for ideas.
- iii. Review the Department's breach metrics to see where there are trends that may indicate a weakness or identify an issue about which you receive questions or complaints and consider developing a scenario around those fact patterns.
- iv. Consider breaches that will engage all of the participants. For example, a loss of hardcopy documents may not effectively engage a participant from the cybersecurity team. A scenario that requires cross functional collaboration (e.g., between staff supporting Freedom of Information Act (FOIA), privacy, cybersecurity, and human resources) is often a more effective TTX.
- v. Balance the complexity of the TTX with the knowledge and experience the BRT members have with handling a breach. A too simple scenario may not be an effective use of this training and awareness opportunity; a too complex scenario may make it difficult for participants to engage in the TTX.

b. Refining the scenario.

- i. After you have chosen the breach you would like to test, speak with the relevant program office and/or system owners to ensure that you understand their data and processes. The scenario should be grounded in reality.
- ii. Create a scenario that evolves over time. Create injects that complicate the scenario by adding additional facts. Provide a realistic timestamp for each update to help participants track their compliance with reporting requirements and understand how long actual breach response activities may take.
- iii. You should be able to map the DOC Breach Response Plan steps to the steps in your TTX; this will help you ensure that you have not forgotten any aspects of the DOC Breach Response Plan in the development of the scenario. Consider creating a table or grid citing back to the plan to ensure you know each BRT member's role and responsibility.
- iv. Try to make the TTX as interactive as possible. Break the scenario into modules with injects to keep participant attention and focus the discussion.

4. Create supporting artifacts, such as breach reports, supplemental reports, and after action reports.

- a. Use the Department’s breach reporting forms, including supplemental reports and after action reports, for the exercise. Using existing artifacts may highlight areas that need clarification or improvement.
 - b. You may want to create additional artifacts, such as dummy data file examples and external press reports.
 - c. Be sure to label all documents created for the TTX with “For exercise purposes only.”
 - d. It can be helpful to have packets available to the participants that include your agency’s breach response policy, the initial scenario, the injects, and any other supporting materials. The participants should not view the injects until they are directed to by the facilitator.
5. Provide an executive summary of the goals of the breach response program, its importance, and the goals and relevance of the TTX for senior leadership prior to TTX.

Execution

1. Share the TTX ground rules with the participants.
 - a. Stress that this is a learning exercise and that participants should feel comfortable asking questions or throwing out ideas. There are no wrong answers and everyone’s opinion will be considered.
 - b. Emphasize that participants should not “fight the scenario.” Every effort will have been made to ensure that the scenario is realistic and reflects actual practices.

Examples of TTX Ground Rules
<ul style="list-style-type: none"> Silence cell phones and other mobile devices during the exercise. Accept that the circumstances surrounding the event are real. This is a “no-fault” environment where varying viewpoints and disagreements are to be expected. There are no wrong answers.

2. Present the initial facts of the scenario to the participants. Use prompts to encourage interaction if the conversation is slow to start.
3. Participants should begin to identify immediate actions that should be taken, including establishing a

Examples of Questions the BRT Should Consider
<ul style="list-style-type: none"> Is there a SORN or PIA? What other agency stakeholders or partners should be made aware of the breach? Who reports the breach to Congress? Who will need to approve any notices, notifications, and other communications? Who would be the source of the notification? Is any official designation required? How and who will fund identity protection services (IPS)? Does the CFO need to be engaged before securing IPS? Is there a vendor engaged for call center and IPS?

- communications plan and, if appropriate, Congressional notification plan.
4. Start to provide injects to the scenario that reflect the types of information you would learn from a breach investigation.
 - a. With each inject, participants should identify the actions that should be taken based on the updated information.
 - b. You can also ask questions that explore other potential aspects of the breach. For example, if your breach involves information about members of the public only, you can ask them whether they would do anything differently if employee information was included.
 5. Have participants complete a post TTX survey before leaving to get their input on the quality and strengths of the TTX, suggestions for improvement, and recommendations for

future TTX scenarios.

Close-out

1. Develop an after action report/improvement plan that documents lessons learned and follow up actions for strengthening the DOC breach response process and/or the system, program, or processes that were tested in the TTX. The report/plan must provide timelines for improvement recommendation implementation and assignment to responsible parties.
 - a. Also document lessons learned for the next tabletop exercise. You can include these in the same report or a separate document.
 - b. Share the report with the BRT.
2. Review the DOC Breach Response Plan for any needed changes based on the lessons learned from the TTX.
3. If appropriate, conduct an out brief for senior leadership. The briefing should identify any unresolved issues to allow leadership to determine if any unmitigated risks are within the Department's risk tolerance.

Mark Graff - NOAA Federal

From: Mark Graff NOAA Federal
Sent: Tuesday, January 23, 2018 3:48 PM
To: Sarah Brabson NOAA Federal
Subject: Re: NOAA8850 PIA and PTA for your signature DOC wants by COB today, thx
Attachments: NOAA8850 Privacy Threshold Analysis for mhg signature mhg.pdf; NOAA8850 EMES PIA 010918 for mhg sig mhg.pdf

Both signed and good to go thanks for including the integration of 8205 note right at Sec. 1.1. Very easy to follow

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Tue, Jan 23, 2018 at 3:08 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
Almost sent to Kathy by mistake!

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)

Ce (b)(6)

**U.S. Department of Commerce Privacy Threshold Analysis
NWS Enterprise Mission Enabling System (EMES)
NOAA8850**

**U.S. Department of Commerce
National Oceanic and Atmospheric Administration
National Weather Service**



**Privacy Threshold Analysis
for the**

**NWS Enterprise Mission Enabling System
(EMES; NOAA8850)**

August 4, 2017

**U.S. Department of Commerce Privacy Threshold Analysis
NWS Enterprise Mission Enabling System (EMES)
NOAA8850**

Unique Project Identifier: NOAA8850

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

The NWS Enterprise Mission Enabling System (EMES) is a group of complimentary enterprise services that provide a secure and reliable infrastructure throughout the NWS organization. Providing central management of these services is more reliable, efficient and customer friendly. EMES consists of Microsoft Active Directory, McAfee ePolicy Orchestrator, Centralized Certificate Authority and Enterprise Cyber security Monitoring and Operations (ECMO). Each of these separate products work together to provide Authentication, Security, Reliability, Inventory and an overall continuity of enterprise service for NWS staff. These tools ensure that only properly identified network devices connect to the NWS Network; run the latest software; run in a secure environment; and only correctly identified and authorized NWS staff gain network access. The system uses redundancy to ensure reliability and availability while reducing latency and bandwidth.

Microsoft Active Directory

Microsoft Active Directory is a special purpose database that authenticates and authorizes all users and computers in a Windows domain network. It is responsible for assigning and enforcing security policies for all computers. Active Directory checks the submitted password and authorizes user access to the system. Multiple Domain Controllers maintain copies of the AD Database and provide redundancy if another Domain Controller is unavailable. Domain Controllers are located in regional offices and key field offices to provide user access and reduce bandwidth.

McAfee ePolicy Orchestrator (ePO)

McAfee ePolicy Orchestrator is an integrated security software program designed to integrate the numerous security programs and to provide real time monitoring of security programs through a single console. McAfee EPO provides end-to-end visibility with a unified view of your security posture, simplified security operations, real-time security status, and an open architecture enabling faster response times.

**U.S. Department of Commerce Privacy Threshold Analysis
NWS Enterprise Mission Enabling System (EMES)
NOAA8850**

Enterprise Cybersecurity Monitoring and Operations (ECMO)

U.S. Office of Management and Budget (OMB) memoranda M-10-15 and M-10-19 require all Federal agencies to continuously monitor security-related information from across the enterprise and present this information to the various levels of agency-wide management to enable timely decision making. The ECMO initiative will fulfill this requirement, providing essential, near real-time security status and remediation, increasing visibility into system operations and helping security personnel make risk-management decisions based on increased situational awareness. ECMO will also provide performance metrics to support the administration priority performance areas for continuous monitoring, automated asset management, automated configuration management, and automated vulnerability management.

Centralized Certificate Authority (CCA)

Centralized Certificate Authority issues thousands of certificates for day-to-day encryption needs, for encrypting local files and file systems, encrypting the communications between client workstation and servers, as well as server to server communication encryption. The internal Certificate Authority is a key component to NWS HSPD-12 implementation. The CCA enables the NWS to effectively implement Single Sign On internally.

We presently issue nine types of certificates:

- (1) SSL for internal web protocols such as for SharePoint and service oriented Architecture applications;
- (2) Domain Controller certificates for enabling Smartcard protocols for client and server cascaded protocols such as Terminal Servers and Remote Desktops and OS to OS communications;
- (3) PKI/IKE certificates for various Public Key Infrastructure;
- (4) Domain Controller Authentication for chaining authentication for non-web protocol applications;
- (5) File Service Encryption certificates useful for enabling Windows-based client equipment to encrypt disk drives, thumb drives, and files and folders. This service includes and administrative back up certificate provision allowing NWS administrators to administratively unencrypt drives that were otherwise locked out by individual certificate damage, corruption or compromise.

**U.S. Department of Commerce Privacy Threshold Analysis
NWS Enterprise Mission Enabling System (EMES)
NOAA8850**

- (6) McAfee Virus Scan, Malware, ePolicy Orchestrator, Rogue System Detection and Endpoint Encryption are services for multiple platforms (Windows, Macintosh, Linux, etc.) that use these certificates for various client and application communications;
- (7) Microsoft Systems Center Configuration Manager (SCCM) uses these certificates in the NWS implementation for communicating with clients to distributed OS Patches, applications patches, and inventory of configurations;
- (8) Microsoft Group Policy uses these certificates for the communications between clients and servers for distributing USGCB compliant policies for user and machine configurations
- (9) Centrify implementation allows Active Directory to more tightly manage non-Microsoft equipment and user accounts, and provides HSPD-12 implementation more readily with better management and administration leveraging Active Directory, and therefore leveraging the internal Certificate Authority for many of the day-to-day encryption tasks.

EMES is a system in production. Currently EMES has included all components within its boundary. EMES expects to continue to expand and offer new products and services. In the near future EMES will provide NETWRIX software and IMET laptops. All new services that EMES provide will be brought into the system boundary following the SDLC framework and will incorporate Security from the beginning.

EMES is defined as a group of complementary enterprise services that provide a secure and reliable infrastructure throughout the NWS organization. EMES consists of Microsoft Active Directory (AD), McAfee ePolicy Orchestrator (ePO), Centralized Certificate Authority (CCA), and Enterprise Cybersecurity Monitoring and Operations (ECMO). Each of these separate products work together to provide authentication, security, reliability, inventory and an overall continuity of enterprise service for NWS staff. These tools ensure that only properly identified network devices connect to the NWS Network; run the latest software; run in a secure environment; and only properly identified and authorized NWS staff gain network access. The system employs redundancy to ensure reliability and availability while reducing latency and bandwidth.

The National Weather Service Headquarters Local Area Network (NWSHQNet), Infrastructure, is a general support system consisting of domain controllers, servers, desktop/workstation, laptops, printers and network infrastructure components. The Infrastructure is located within the Silver Spring Metro Complex Building 2 (SSMC-2) and supports approximately 250 users and 1,500 network devices.

**U.S. Department of Commerce Privacy Threshold Analysis
NWS Enterprise Mission Enabling System (EMES)
NOAA8850**

The network infrastructure provides the support, management and connectivity services for administrative functions to include: Service Desk support, Active Directory, file and print, file backup and restoration, storage, Dynamic Host Configuration Protocol, Windows Internet Name Services, Domain Name Service, IP address space allocation, application distribution and patch management, backup and disaster recovery to the desktop and server customers within the accreditation boundary. In addition, it provides system-level support for servers, desktops/workstations, and laptops and a test lab mimicking the production environment for systems and network engineers to develop and test new technologies. Lastly, active directory user base receives electronic mail and calendar services from the NOAA Messaging Operations Center.

Questionnaire:

1. What is the status of this information system?

- This is a new information system. *Continue to answer questions and complete certification.*
- This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

- This is an existing information system in which changes do not create new privacy risks. *Continue to answer questions, and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

- Yes. *Please describe the activities which may raise privacy concerns.*
- No

**U.S. Department of Commerce Privacy Threshold Analysis
NWS Enterprise Mission Enabling System (EMES)
NOAA8850**

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

**U.S. Department of Commerce Privacy Threshold Analysis
NWS Enterprise Mission Enabling System (EMES)
NOAA8850**

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.


**U.S. Department of Commerce Privacy Threshold Analysis
NWS Enterprise Mission Enabling System (EMES)
NOAA8850**

CERTIFICATION

I certify the criteria implied by one or more of the questions above **apply** to the NOAA8850 EMES and as a consequence of this applicability, I will perform and document a PIA for this IT system.


I certify the criteria implied by the questions above **do not apply** to the NOAA8850 EMES and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): **Tommy Thompson, Sr.**

THOMPSON.THOMAS.PAUL.SR.1200327841  Digitally signed by THOMPSON.THOMAS.PAUL.SR.1200327841
Date: 2018.01.08 14:42:41 05'00'


Signature of SO

Name of Information Technology Security Officer (ITSO): **Andrew Browne**

BROWNE.ANDREW.PATRICK.1472149349  Digitally signed by BROWNE.ANDREW.PATRICK.1472149349
Date: 2018.01.08 12:15:40 05'00'


Signature of ITSO

Name of Authorizing Official (AO): **Richard Varn**

VARN.RICHARD.ALAN.II.1073462041  Digitally signed by VARN.RICHARD.ALAN.II.1073462041
Date: 2018.01.23 09:19:36 -05'00'

Signature of AO

Name of Bureau Chief Privacy Officer (BCPO): **Mark Graff**

GRAFF.MARK.HYRUM.1514447892  Digitally signed by GRAFF.MARK.HYRUM.1514447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER,
cn=GRAFF.MARK.HYRUM.1514447892
Date: 2018.01.23 15:46:23 -05'00'

Signature of BCPO

**U.S. Department of Commerce
National Oceanic and Atmospheric Administration National
Weather Service**



**Privacy Impact Assessment
for the**

**NWS Enterprise Mission Enabling System (EMES)
NOAA8850**

Reviewed by: _____, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment NOAA8850

Unique Project Identifier: NOAA8850

Introduction: System Description

The NWS Enterprise Mission Enabling System (EMES) is a group of complimentary enterprise services that provide a secure and reliable infrastructure throughout the NWS organization. Providing central management of these services is more reliable, efficient and customer friendly. EMES consists of Microsoft Active Directory, McAfee ePolicy Orchestrator, Centralized Certificate Authority and Enterprise Cyber security Monitoring and Operations (ECMO). Each of these separate products work together to provide Authentication, Security, Reliability, Inventory and an overall continuity of enterprise service for NWS staff. These tools ensure that only properly identified network devices connect to the NWS Network; run the latest software; run in a secure environment; and only correctly identified and authorized NWS staff gain network access. The system uses redundancy to ensure reliability and availability while reducing latency and bandwidth.

Microsoft Active Directory

Microsoft Active Directory is a special purpose database that authenticates and authorizes all users and computers in a Windows domain network. It is responsible for assigning and enforcing security policies for all computers. Active Directory checks the submitted password and authorizes user access to the system. Multiple Domain Controllers maintain copies of the AD Database and provide redundancy if another Domain Controller is unavailable. Domain Controllers are located in regional offices and key field offices to provide user access and reduce bandwidth.

McAfee ePolicy Orchestrator (ePO)

McAfee ePolicy Orchestrator is an integrated security software program designed to integrate the numerous security programs and to provide real time monitoring of security programs through a single console. McAfee EPO provides end-to-end visibility with a unified view of your security posture, simplified security operations, real-time security status, and an open architecture enabling faster response times.

Enterprise Cybersecurity Monitoring and Operations (ECMO)

U.S. Office of Management and Budget (OMB) memoranda M-10-15 and M-10-19 require all Federal agencies to continuously monitor security-related information from across the enterprise and present this information to the various levels of agency-wide management to enable timely decision making. The ECMO initiative will fulfill this requirement, providing essential, near

real-time security status and remediation, increasing visibility into system operations and helping security personnel make risk-management decisions based on increased situational awareness. ECMO will also provide performance metrics to support the administration priority performance areas for continuous monitoring, automated asset management, automated configuration management, and automated vulnerability management.

Centralized Certificate Authority (CCA)

Centralized Certificate Authority issues thousands of certificates for day-to-day encryption needs, for encrypting local files and file systems, encrypting the communications between client workstation and servers, as well as server to server communication encryption. The internal Certificate Authority is a key component to NWS HSPD-12 implementation. The CCA enables the NWS to effectively implement Single Sign On internally.

We presently issue nine types of certificates:

- (1) SSL for internal web protocols such as for SharePoint and service oriented Architecture applications;
- (2) Domain Controller certificates for enabling Smartcard protocols for client and server cascaded protocols such as Terminal Servers and Remote Desktops and OS to OS communications;
- (3) PKI/IKE certificates for various Public Key Infrastructure;
- (4) Domain Controller Authentication for chaining authentication for non-web protocol applications;
- (5) File Service Encryption certificates useful for enabling Windows-based client equipment to encrypt disk drives, thumb drives, and files and folders. This service includes and administrative back up certificate provision allowing NWS administrators to administratively unencrypt drives that were otherwise locked out by individual certificate damage, corruption or compromise.
- (6) McAfee Virus Scan, Malware, ePolicy Orchestrator, Rogue System Detection and Endpoint Encryption are services for multiple platforms (Windows, Macintosh, Linux, etc.) that use these certificates for various client and application communications;
- (7) Microsoft Systems Center Configuration Manager (SCCM) uses these certificates in the NWS implementation for communicating with clients to distributed OS Patches, applications patches, and inventory of configurations;

- (8) Microsoft Group Policy uses these certificates for the communications between clients and servers for distributing USGCB compliant policies for user and machine configurations
- (9) Centrify implementation allows Active Directory to more tightly manage non-Microsoft equipment and user accounts, and provides HSPD-12 implementation more readily with better management and administration leveraging Active Directory, and therefore leveraging the internal Certificate Authority for many of the day-to-day encryption tasks.

Future

EMES is a system in production. Currently EMES has included all components within its boundary. EMES expects to continue to expand and offer new products and services. In the near future, EMES will provide NETWRIX software and IMET laptops. All new services that EMES provide will be brought into the system boundary following the SDLC framework and will incorporate Security from the beginning.

EMES also contains the National Weather Service Headquarters Local Area Network (NWSHQNet) a general support system consisting of domain controllers, servers, desktop/workstation, laptops, printers and network infrastructure components. NWSHQNet is located within the Silver Spring Metro Complex Building 2 (SSMC-2) and supports approximately 250 users and 600 network devices. NNWSHQNet provides network infrastructure support, management and connectivity services for administrative functions to include: Service Desk support, Active Directory, file and print, file backup and restoration, storage, Dynamic Host Configuration Protocol, Windows Internet Name Services, Domain Name Service, IP address space allocation, application distribution and patch management, backup and disaster recovery to the desktop and server customers within the NOAA8850 accreditation boundary. In addition, it provides system-level support for servers, desktops/workstations, and laptops and a test lab mimicking the production environment for systems and network engineers to develop and test new technologies. Lastly, the active directory user base receives electronic mail and calendar services from the NOAA Messaging Operations Center.

Multi Year Planning System (MYPS)

The Multi Year Planning System (MYPS) is comprised of three General Services Systems (GSS) and includes 20 servers (CFO1 servers). The GSS are the MYPS Labor Projection Model, Management Analysis and Reporting System Business Intelligence (BI) Maintenance Platform (MARS), and the General Forecaster Vacancy System. The Labor Projection Model and the General Forecaster Vacancy System are operational production systems. MARS BI Maintenance

Platform is used only for maintenance efforts related to the production and pre-production MARS systems which are housed at the NOAA Information Technology Center.

The MYPS Labor Projection Model is a tool used to compute the multi-year total NWS labor model (5 years) using a detailed site-by-site, bottom-up cost approach. It calculates labor costs by site by position with the impact of changes in staffing levels. The model applies a labor lapse, calculates FTE, benefits, premium pay (shift differential), overtime, locality pay, cost of living allowance (COLA), special IT pay, awards, and annual pay raises. Costs are calculated using OPM-published salary and rates tables. All costs are categorized by Accounting Classification Code Structure (ACCS), cost category, funding source, and portfolio. In addition, the model is used in “what-if” analyses to answer questions about proposed changes in labor such as lapse, labor rates, inflation, and table of organization changes. The resulting five year answer sets are used to answer detailed questions about labor planning for NWS, NOAA, DOC, OMB, and Congressional requests without any PII data. The labor data contained in the model’s database is the master authorized (funded) position data for NWS. The model has its own user logon system and is accessed by its sole Federal user and its maintenance support contractor staff via the NOAA Silver Spring Metro Campus (SSMC) trusted campus network. The MYPS system retains user name, job title, and budgeted salary information for the purposes of budget forecast modeling.

MARS is a NOAA enterprise system that provides a common Business Intelligence (BI) platform to all NOAA Line Offices for financial reporting and querying, budget planning and commitment tracking. It consists of two modules, Reporting and Querying and Data Entry. The Data Entry module is not supported by MYPS. The MARS Reporting and Querying module is a business intelligence maintenance environment used for ongoing design, creation and testing of new reports; new extract, transform and load (ETL) jobs; and software patches and upgrades for eventual deployment to the Reporting and Querying module of MARS. MARS BI Maintenance Platform is accessible only via the NOAA Silver Spring Metro Campus (SSMC) trusted campus network. PII related information is collected solely for regression testing purposes within the MARS system. Once testing has been completed, the sample data will be retained for a time, and deleted within 3 years or sooner. Our mandate is to make sure any revisions to our processes operate correctly and produce correct answers on the MARS reports before promoting the revisions forward to TEST where yet another testing cycle occurs. Once the Federal client approves the system fix(es) on TEST, the final solution is only then migrated to PROD, with another final confirmation things worked in PROD before closing our Software Design Request (SDR) ticket.

Sample data is extracted from production to use during various development cycles that include previous fiscal year (FY) data and the current FY data. The resultant differences are compared between DEV or TEST to the PROD environment to prove the expected system modifications actually repaired the process or MARS report.

If dummy data was implemented, live data would still need to be extracted, but then systematically be revised to substitute real values for dummy values across multiple fiscal years and multiple database tables many of which enforce primary/foreign key relational constraints. After this exercise, the MARS team would still need to map backwards to the original data for direct comparison to our production system data or reports for validation of the changes. These steps would be costly in team resources with multiple developers working on multiple SDRs, but yet allowing correlated comparison of before and after change modification to the operational MARS production system as proof of task completion. Since the Government doesn't want to pay for these steps in time or dollars, the additional developer, system, and user controls have been added on all MARS developers and users giving them the responsibility to protect data from all unauthorized disclosures (e.g. NDAs mentioned previously above).

Government stakeholders need the MARS Financial Data Warehouse and they imposed the best possible security measures given the exigent trade-offs and limited available resources available (CPU speed, disk space, contract dollars, time, and staff).

The General Forecaster Vacancy System is a notification application that is used by regional workforce managers to make regional meteorological (met) interns (Met Interns) aware of upcoming general forecaster vacancies at NWS Weather Forecast Offices (WFOs), per an agreement between NWS management and the National Weather Service Employees Organization (NWSEO). The system contains a database of all the Met Interns in the regions. The database is maintained by the regional workforce managers using a web application which is accessed using LDAP authentication. Prior to posting a vacancy for a general forecaster (meteorologist) at a WFO, the workforce manager in the region uses the system too automatically send an email to all the met interns listed in the database. An intern who is interested in the listed vacancy clicks on an HTML hyperlink imbedded in the email to express their interest. The system counts the responses and a determination is made at the regional level, based on the number of responses, whether the vacancy will be advertised to status candidates only or to all hiring sources (USAJOBS, etc.). The web portal uses session cookies to time-out any open workforce manager sessions within five minutes to maintain security of the process. PII in the form of user name and email address is collected and retained as part of the application process.

The NOAA8850 Trusted Agent collects and stores Form CD591 (PIV request form) for government issued IDs, LDAP and Active Directory. The Trusted Agent processes security and badging forms for contractors only, not federal employees. The processing package includes fingerprints and a photograph, both taken by the badging office (but not stored in NOAA8850), driver's license and passport number. Once the Eastern Region Security Office approves a contractor for a CAC, it returns the CD-591s for the sponsored contractors and they are stored electronically. OF306 Declaration for Federal Employment is stored temporarily when the form needs to be scanned and saved to a drive prior to uploading into Accellion Secure File transfer to

send to the Security Office. *Contractors are advised to remove the form from their desktops after the transfer, but there is no current way to check this. The system is investigating courses of action to discover PII data within NOAA8850, including user terminals, but in the meantime, we are changing the confidentiality level to 'High' based on possible SSN retention on desktops.* A paper copy of the Security Coversheet/Request for Investigation Coversheet is also stored after removing Birth Date and SSN.

No PII is shared outside of the Department of Commerce (DOC) except in these cases: 1) only PII directly related to an individual's clearance is shared with DOC; if there is a security or privacy breach, applicable PII may be shared with the Department and other Federal agencies.

Authorities

U.S.C. § 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

15 U.S.C. § 1512, which confers general powers and duties authority to executive agencies, vesting jurisdiction and control of departments, bureaus, offices and branches.

Federal Information Security Management Act (Pub. L. 107 296, Sec. 3544).

E-Government Act (Pub. L. 107 347, Sec. 203).

From DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.

From DEPT-18: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

From DEPT-25: 5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 (HSPD 12), Federal Property and Administrative Services Act of 1949, as amended.

From GSA/GOVT-7: 5 U.S.C. 301; Federal Information Security Management Act of 2002 (44 U.S.C. 3554); E-Government Act of 2002 (Pub. L. 107-347, Sec. 203); Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et al.) and Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504 note); Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

From OPM/GOVT-1: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

This system has been classified as FIPS 199 moderate level.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

This is a new information system.

This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection*	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

***NOAA8205 integrated into this system.**

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (Check all that apply.)

Identifying Numbers (IN)					
a. Social Security*	X	e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License	X	j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
* Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					
* For MARS testing: A three tier approach (DEV, TEST, PROD) is implemented so that any new bug fixes or new developments are moved forward to TEST tier first, run in mock production setting on TEST, then once all regression testing has been validated and approvals given from Federal agent, the "code" is migrated into production. During testing periods, the TEST tier has PROD data to assure everything works as though it were in production. Afterwards housecleaning is conducted on TEST until the next testing cycle.					
There is also temporary storage of the OF306 before transmitting to the security office.					
Authorities: see DEPT 18 authorities in the system description.					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					
Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

* For badging purposes only

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run	X	f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)					

2.2 Indicate sources of the PII/BII in the system. (Check all that apply.)

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify)					

Non-government Sources			
Public Organizations		Private Sector	Commercial Data Brokers
Third Party Website or Application			
Other (specify):			

- 2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X\	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
----	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

- 3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

x	There are not any IT system supported activities which raise privacy risks/concerns.
---	--------------------------------------------------------------------------------------

Section 4: Purpose of the System

- 4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The NOAA8205 Trusted Agent collects and stores Form CD591 (PIV request form) for government issued IDs, LDAP and Active Directory. The Trusted Agent processes security and badging forms for contractors only, not federal employees. The processing package includes fingerprints and a photograph, both taken by the badging office (*but not stored in the system*), driver's license and passport number. Once the Eastern Region Security Office approves a contractor for a CAC, it returns the CD-591s for the sponsored contractors and they are stored electronically. Trusted agents are instructed to complete only Section A of the CD-591. They do not include the I-9 form and have never been requested to do so by OSY.

OF306 Declaration for Federal Employment is stored temporarily when the form needs to be scanned and saved to a drive prior to uploading into Accellion Secure File transfer to send to the Security Office. A paper copy of the Security Coversheet/Request for Investigation Coversheet is also stored after removing Birth Date and SSN. The only forms stored are redacted Coversheets and CD-591s which do not contain PII.

The MYPS system retains user name, job title and budgeted salary information for the purposes of budget forecast models.

The Forecaster Vacancy system retains name and email only for federal employees.

The MARS system retains sample PII for testing purposes only and discards after each testing cycle.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*In case of breach.

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	-----------------------------------------------

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input type="checkbox"/>	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at:	
X	Yes, notice is provided by other means.	<p>Specify how:</p> <p>Form CD591, the DOC PIV request form, provides notice in that the request for information comes from the sponsor and registrar. The information comes from the applicant, who completes the form and provides it to the sponsor. There is also a privacy act statement on this form.</p> <p>https://mars.rdc.noaa.gov/docs/forms/NOAA MARS Rules of Behavior.pdf https://mars.rdc.noaa.gov/docs/forms/DOC NOAA MARS ND A v2.pdf</p> <p>Form OF306 states that the Office of Personnel Management is authorized to request this information under sections 1302, 3301, 3304, 3328, and 8716 of title 5, U. S. Code and addresses and Routine Uses.</p> <p>The MYPS, Forecaster Vacancy System, and MARS: Federal workers sign a privacy release pursuant to the Privacy Act of 1974 during on-boarding with NOAA/NWS; see https://www.justice.gov/opcl/privacy-act-1974 ; Conditions of disclosure; "For routine uses within a U.S. government agency" and "Other administrative purposes."</p>
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	<p>Specify how: Individuals can decline by not providing requested information to receive NOAA ID. However, without a NOAA ID, they cannot work at NOAA as a Federal Employee or Contractor.</p> <p>The information collected Forecaster Vacancy System is</p>
---	---------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		provided only if the service is desired. The information collected by MYPS is solely for budget purposes (no opt out) and MARS collects information solely for testing applications (no opt out).
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: If no consent is granted, no ID will be issued as in 7.2 above. This is the only purpose for this information. There is only one use for each of these: MYPS (budget) and MARS (testing) Forecaster Vacancy is voluntary for job openings and solely consists of user name and email address. There is only one use of the information.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Users are informed in person or in writing by their supervisors at time of onboarding, that they can update PII/information via NOAA LDAP or NOAA Locator. https://nsd.rdc.noaa.gov/ Forecaster Vacancy user name, email address and MYPS information updates are not applicable for the individual. However, updates may be implemented by HQ and FMC administrators at an individual's request in writing to one or the other. MARS PII is used solely for testing and thus the individual does not need to review/update PII/BII pertaining to them.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: MARS has built-in auditor for who accessed what report and when.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 11/20/2017 <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

<p>User name, Office location, and Telephone Number of NOAA employees and contractors are collected and maintained in NOAA8205 Active Directory and LDAP. NOAA8205 Administrators can access or alter this information; the Active Directory is not publicly accessible and has internal boundary controls in place to include firewall and Access Control Lists (ACLs).</p> <p>The NWS HQ Trusted agent (TA) collects and maintains CD591 information. This information is stored by the TA in a locked secure location; after three months, the information is shredded in accordance with NOAA Records Management schedule. (Contains name, phone number and email address.)</p> <p>The MYPS and MARS information is maintained in encrypted files and protected through Role Based Access Controls (RBAC).</p>

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i> : DEPT-13 , Investigative and Security Records, DEPT-18 , Employees Information Not Covered by Notices of Other Agencies; DEPT-25 , Access Control
---	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	and Identity Management System, GSA./GOVT-7 , Personal Identity Verification Identity Management System. OPM/GOVT-1 , General Personnel Records
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Schedule Series Chapter: 900 904-01 Building Identification Credential Files NOAA Chapter 100: Enterprise-Wide Functions Electronic Records schedule: NARA General Records Schedule 20, Electronic Records
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels.
(Check all that apply.)

X	Identifiability	Provide explanation: The loss of confidentiality could lead to identity theft for individuals affected.
X	Quantity of PII	Provide explanation: No access for average MARS user; limited access for MARS power users as needed to do their job function; and more access for top level managers who require access for those they manage.
X	Data Field Sensitivity	Provide explanation: In some cases, the CD306 containing a contractor SSN may not have been removed from a desktop. The system is working on addressing this issue.
X	Context of Use	Provide explanation: MARS links some PII data using natural keys for SQL table joins which report users cannot see.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: The information collected for badging purposes contains two forms of personal identification (ie Passport, Driver's license, etc.) which, if exposed during the course of collection and verification, could have an adverse impact to user confidentiality.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: The possibility of retention of the SSN, as stored electronically in the OF306, caused us to change our confidentiality rating from "moderate" to "high."
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

<p>System Owner</p> <p>Name: Tommy Thompson Sr. Office: NWS/ACIO Phone: (301) 427-6987 Email: Tommy.Thompson@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: THOMPSON.THOMAS.PAUL.SR.1200327841 <small>Digitally signed by THOMPSON.THOMAS.PAUL.SR.1200327841 Date: 2018.01.23 14:04:02 -05'00'</small></p>	<p>Information Technology Security Officer</p> <p>Name: Andrew Browne Office: NWS/ACIO Phone: (301) 427-9033 Email: Andrew.Browne@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: BROWNE.ANDREW.PATRICK.1472149349 <small>Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2018.01.23 10:36:05 -05'00'</small></p>
<p>Authorizing Official</p> <p>Name: Richard Varn Office: NWS/ACIO Phone: (301) 427-0927 Email: Richard.Varn@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: VARN.RICHARD.ALAN.II.1073462041 <small>Digitally signed by VARN.RICHARD.ALAN.II.1073462041 Date: 2018.01.23 14:51:31 -05'00'</small></p>	<p>Bureau Chief Privacy Officer</p> <p>Name: Mark Graff Office: NOAA/OCIO Phone: (301) 628-5658 Email: Mark.Graff@noaa.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>Signature: GRAFF.MARK.HYRUM.1514447892 <small>Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.23 15:45:26 -05'00'</small></p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Tuesday, January 23, 2018 3:56 PM
To: Gioffre, Kathy (Federal); CPO
Cc: Ferguson, Dorrie; Toland, Michael; Mark Graff NOAA Federal; John Soule NOAA Affiliate; Tommy Thompson
Subject: NOAA8850 PIA and PTA signed, pls see attached
Attachments: NOAA8850 EMES PIA 010918 for mhg sig mhg.pdf; NOAA8850 Privacy Threshold Analysis for mhg signature mhg.pdf

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

**U.S. Department of Commerce Privacy Threshold Analysis
NWS Enterprise Mission Enabling System (EMES)
NOAA8850**

**U.S. Department of Commerce
National Oceanic and Atmospheric Administration
National Weather Service**



**Privacy Threshold Analysis
for the**

**NWS Enterprise Mission Enabling System
(EMES; NOAA8850)**

August 4, 2017

**U.S. Department of Commerce Privacy Threshold Analysis
NWS Enterprise Mission Enabling System (EMES)
NOAA8850**

Unique Project Identifier: NOAA8850

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

The NWS Enterprise Mission Enabling System (EMES) is a group of complimentary enterprise services that provide a secure and reliable infrastructure throughout the NWS organization. Providing central management of these services is more reliable, efficient and customer friendly. EMES consists of Microsoft Active Directory, McAfee ePolicy Orchestrator, Centralized Certificate Authority and Enterprise Cyber security Monitoring and Operations (ECMO). Each of these separate products work together to provide Authentication, Security, Reliability, Inventory and an overall continuity of enterprise service for NWS staff. These tools ensure that only properly identified network devices connect to the NWS Network; run the latest software; run in a secure environment; and only correctly identified and authorized NWS staff gain network access. The system uses redundancy to ensure reliability and availability while reducing latency and bandwidth.

Microsoft Active Directory

Microsoft Active Directory is a special purpose database that authenticates and authorizes all users and computers in a Windows domain network. It is responsible for assigning and enforcing security policies for all computers. Active Directory checks the submitted password and authorizes user access to the system. Multiple Domain Controllers maintain copies of the AD Database and provide redundancy if another Domain Controller is unavailable. Domain Controllers are located in regional offices and key field offices to provide user access and reduce bandwidth.

McAfee ePolicy Orchestrator (ePO)

McAfee ePolicy Orchestrator is an integrated security software program designed to integrate the numerous security programs and to provide real time monitoring of security programs through a single console. McAfee EPO provides end-to-end visibility with a unified view of your security posture, simplified security operations, real-time security status, and an open architecture enabling faster response times.

**U.S. Department of Commerce Privacy Threshold Analysis
NWS Enterprise Mission Enabling System (EMES)
NOAA8850**

Enterprise Cybersecurity Monitoring and Operations (ECMO)

U.S. Office of Management and Budget (OMB) memoranda M-10-15 and M-10-19 require all Federal agencies to continuously monitor security-related information from across the enterprise and present this information to the various levels of agency-wide management to enable timely decision making. The ECMO initiative will fulfill this requirement, providing essential, near real-time security status and remediation, increasing visibility into system operations and helping security personnel make risk-management decisions based on increased situational awareness. ECMO will also provide performance metrics to support the administration priority performance areas for continuous monitoring, automated asset management, automated configuration management, and automated vulnerability management.

Centralized Certificate Authority (CCA)

Centralized Certificate Authority issues thousands of certificates for day-to-day encryption needs, for encrypting local files and file systems, encrypting the communications between client workstation and servers, as well as server to server communication encryption. The internal Certificate Authority is a key component to NWS HSPD-12 implementation. The CCA enables the NWS to effectively implement Single Sign On internally.

We presently issue nine types of certificates:

- (1) SSL for internal web protocols such as for SharePoint and service oriented Architecture applications;
- (2) Domain Controller certificates for enabling Smartcard protocols for client and server cascaded protocols such as Terminal Servers and Remote Desktops and OS to OS communications;
- (3) PKI/IKE certificates for various Public Key Infrastructure;
- (4) Domain Controller Authentication for chaining authentication for non-web protocol applications;
- (5) File Service Encryption certificates useful for enabling Windows-based client equipment to encrypt disk drives, thumb drives, and files and folders. This service includes and administrative back up certificate provision allowing NWS administrators to administratively unencrypt drives that were otherwise locked out by individual certificate damage, corruption or compromise.

**U.S. Department of Commerce Privacy Threshold Analysis
NWS Enterprise Mission Enabling System (EMES)
NOAA8850**

- (6) McAfee Virus Scan, Malware, ePolicy Orchestrator, Rogue System Detection and Endpoint Encryption are services for multiple platforms (Windows, Macintosh, Linux, etc.) that use these certificates for various client and application communications;
- (7) Microsoft Systems Center Configuration Manager (SCCM) uses these certificates in the NWS implementation for communicating with clients to distributed OS Patches, applications patches, and inventory of configurations;
- (8) Microsoft Group Policy uses these certificates for the communications between clients and servers for distributing USGCB compliant policies for user and machine configurations
- (9) Centrify implementation allows Active Directory to more tightly manage non-Microsoft equipment and user accounts, and provides HSPD-12 implementation more readily with better management and administration leveraging Active Directory, and therefore leveraging the internal Certificate Authority for many of the day-to-day encryption tasks.

EMES is a system in production. Currently EMES has included all components within its boundary. EMES expects to continue to expand and offer new products and services. In the near future EMES will provide NETWRIX software and IMET laptops. All new services that EMES provide will be brought into the system boundary following the SDLC framework and will incorporate Security from the beginning.

EMES is defined as a group of complementary enterprise services that provide a secure and reliable infrastructure throughout the NWS organization. EMES consists of Microsoft Active Directory (AD), McAfee ePolicy Orchestrator (ePO), Centralized Certificate Authority (CCA), and Enterprise Cybersecurity Monitoring and Operations (ECMO). Each of these separate products work together to provide authentication, security, reliability, inventory and an overall continuity of enterprise service for NWS staff. These tools ensure that only properly identified network devices connect to the NWS Network; run the latest software; run in a secure environment; and only properly identified and authorized NWS staff gain network access. The system employs redundancy to ensure reliability and availability while reducing latency and bandwidth.

The National Weather Service Headquarters Local Area Network (NWSHQNet), Infrastructure, is a general support system consisting of domain controllers, servers, desktop/workstation, laptops, printers and network infrastructure components. The Infrastructure is located within the Silver Spring Metro Complex Building 2 (SSMC-2) and supports approximately 250 users and 1,500 network devices.

**U.S. Department of Commerce Privacy Threshold Analysis
NWS Enterprise Mission Enabling System (EMES)
NOAA8850**

The network infrastructure provides the support, management and connectivity services for administrative functions to include: Service Desk support, Active Directory, file and print, file backup and restoration, storage, Dynamic Host Configuration Protocol, Windows Internet Name Services, Domain Name Service, IP address space allocation, application distribution and patch management, backup and disaster recovery to the desktop and server customers within the accreditation boundary. In addition, it provides system-level support for servers, desktops/workstations, and laptops and a test lab mimicking the production environment for systems and network engineers to develop and test new technologies. Lastly, active directory user base receives electronic mail and calendar services from the NOAA Messaging Operations Center.

Questionnaire:

1. What is the status of this information system?

- This is a new information system. *Continue to answer questions and complete certification.*
- This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

- This is an existing information system in which changes do not create new privacy risks. *Continue to answer questions, and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

- Yes. *Please describe the activities which may raise privacy concerns.*
- No

**U.S. Department of Commerce Privacy Threshold Analysis
NWS Enterprise Mission Enabling System (EMES)
NOAA8850**

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

**U.S. Department of Commerce Privacy Threshold Analysis
NWS Enterprise Mission Enabling System (EMES)
NOAA8850**

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

**U.S. Department of Commerce Privacy Threshold Analysis
NWS Enterprise Mission Enabling System (EMES)
NOAA8850**

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the NOAA8850 EMES and as a consequence of this applicability, I will perform and document a PIA for this IT system.

I certify the criteria implied by the questions above **do not apply** to the NOAA8850 EMES and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): **Tommy Thompson, Sr.**

THOMPSON.THOMAS.PAUL.SR.1200327841

Digitally signed by THOMPSON.THOMAS.PAUL.SR.1200327841
Date: 2018.01.08 14:42:41 05'00'

Signature of SO

Name of Information Technology Security Officer (ITSO): **Andrew Browne**

BROWNE.ANDREW.PATRICK.1472149349

Digitally signed by BROWNE.ANDREW.PATRICK.1472149349
Date: 2018.01.08 12:15:40 05'00'

Signature of ITSO

Name of Authorizing Official (AO): **Richard Varn**

VARN.RICHARD.ALAN.II.1073462041

Digitally signed by VARN.RICHARD.ALAN.II.1073462041
Date: 2018.01.23 09:19:36 -05'00'

Signature of AO

Name of Bureau Chief Privacy Officer (BCPO): **Mark Graff**

GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF.MARK.HYRUM.1514447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER,
cn=GRAFF.MARK.HYRUM.1514447892
Date: 2018.01.23 15:46:23 -05'00'

Signature of BCPO

**U.S. Department of Commerce
National Oceanic and Atmospheric Administration National
Weather Service**



**Privacy Impact Assessment
for the**

**NWS Enterprise Mission Enabling System (EMES)
NOAA8850**

Reviewed by: _____, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment NOAA8850

Unique Project Identifier: NOAA8850

Introduction: System Description

The NWS Enterprise Mission Enabling System (EMES) is a group of complimentary enterprise services that provide a secure and reliable infrastructure throughout the NWS organization. Providing central management of these services is more reliable, efficient and customer friendly. EMES consists of Microsoft Active Directory, McAfee ePolicy Orchestrator, Centralized Certificate Authority and Enterprise Cyber security Monitoring and Operations (ECMO). Each of these separate products work together to provide Authentication, Security, Reliability, Inventory and an overall continuity of enterprise service for NWS staff. These tools ensure that only properly identified network devices connect to the NWS Network; run the latest software; run in a secure environment; and only correctly identified and authorized NWS staff gain network access. The system uses redundancy to ensure reliability and availability while reducing latency and bandwidth.

Microsoft Active Directory

Microsoft Active Directory is a special purpose database that authenticates and authorizes all users and computers in a Windows domain network. It is responsible for assigning and enforcing security policies for all computers. Active Directory checks the submitted password and authorizes user access to the system. Multiple Domain Controllers maintain copies of the AD Database and provide redundancy if another Domain Controller is unavailable. Domain Controllers are located in regional offices and key field offices to provide user access and reduce bandwidth.

McAfee ePolicy Orchestrator (ePO)

McAfee ePolicy Orchestrator is an integrated security software program designed to integrate the numerous security programs and to provide real time monitoring of security programs through a single console. McAfee EPO provides end-to-end visibility with a unified view of your security posture, simplified security operations, real-time security status, and an open architecture enabling faster response times.

Enterprise Cybersecurity Monitoring and Operations (ECMO)

U.S. Office of Management and Budget (OMB) memoranda M-10-15 and M-10-19 require all Federal agencies to continuously monitor security-related information from across the enterprise and present this information to the various levels of agency-wide management to enable timely decision making. The ECMO initiative will fulfill this requirement, providing essential, near

real-time security status and remediation, increasing visibility into system operations and helping security personnel make risk-management decisions based on increased situational awareness. ECMO will also provide performance metrics to support the administration priority performance areas for continuous monitoring, automated asset management, automated configuration management, and automated vulnerability management.

Centralized Certificate Authority (CCA)

Centralized Certificate Authority issues thousands of certificates for day-to-day encryption needs, for encrypting local files and file systems, encrypting the communications between client workstation and servers, as well as server to server communication encryption. The internal Certificate Authority is a key component to NWS HSPD-12 implementation. The CCA enables the NWS to effectively implement Single Sign On internally.

We presently issue nine types of certificates:

- (1) SSL for internal web protocols such as for SharePoint and service oriented Architecture applications;
- (2) Domain Controller certificates for enabling Smartcard protocols for client and server cascaded protocols such as Terminal Servers and Remote Desktops and OS to OS communications;
- (3) PKI/IKE certificates for various Public Key Infrastructure;
- (4) Domain Controller Authentication for chaining authentication for non-web protocol applications;
- (5) File Service Encryption certificates useful for enabling Windows-based client equipment to encrypt disk drives, thumb drives, and files and folders. This service includes and administrative back up certificate provision allowing NWS administrators to administratively unencrypt drives that were otherwise locked out by individual certificate damage, corruption or compromise.
- (6) McAfee Virus Scan, Malware, ePolicy Orchestrator, Rogue System Detection and Endpoint Encryption are services for multiple platforms (Windows, Macintosh, Linux, etc.) that use these certificates for various client and application communications;
- (7) Microsoft Systems Center Configuration Manager (SCCM) uses these certificates in the NWS implementation for communicating with clients to distributed OS Patches, applications patches, and inventory of configurations;

- (8) Microsoft Group Policy uses these certificates for the communications between clients and servers for distributing USGCB compliant policies for user and machine configurations
- (9) Centrify implementation allows Active Directory to more tightly manage non-Microsoft equipment and user accounts, and provides HSPD-12 implementation more readily with better management and administration leveraging Active Directory, and therefore leveraging the internal Certificate Authority for many of the day-to-day encryption tasks.

Future

EMES is a system in production. Currently EMES has included all components within its boundary. EMES expects to continue to expand and offer new products and services. In the near future, EMES will provide NETWRIX software and IMET laptops. All new services that EMES provide will be brought into the system boundary following the SDLC framework and will incorporate Security from the beginning.

EMES also contains the National Weather Service Headquarters Local Area Network (NWSHQNet) a general support system consisting of domain controllers, servers, desktop/workstation, laptops, printers and network infrastructure components. NWSHQNet is located within the Silver Spring Metro Complex Building 2 (SSMC-2) and supports approximately 250 users and 600 network devices. NNWSHQNet provides network infrastructure support, management and connectivity services for administrative functions to include: Service Desk support, Active Directory, file and print, file backup and restoration, storage, Dynamic Host Configuration Protocol, Windows Internet Name Services, Domain Name Service, IP address space allocation, application distribution and patch management, backup and disaster recovery to the desktop and server customers within the NOAA8850 accreditation boundary. In addition, it provides system-level support for servers, desktops/workstations, and laptops and a test lab mimicking the production environment for systems and network engineers to develop and test new technologies. Lastly, the active directory user base receives electronic mail and calendar services from the NOAA Messaging Operations Center.

Multi Year Planning System (MYPS)

The Multi Year Planning System (MYPS) is comprised of three General Services Systems (GSS) and includes 20 servers (CFO1 servers). The GSS are the MYPS Labor Projection Model, Management Analysis and Reporting System Business Intelligence (BI) Maintenance Platform (MARS), and the General Forecaster Vacancy System. The Labor Projection Model and the General Forecaster Vacancy System are operational production systems. MARS BI Maintenance

Platform is used only for maintenance efforts related to the production and pre-production MARS systems which are housed at the NOAA Information Technology Center.

The MYPS Labor Projection Model is a tool used to compute the multi-year total NWS labor model (5 years) using a detailed site-by-site, bottom-up cost approach. It calculates labor costs by site by position with the impact of changes in staffing levels. The model applies a labor lapse, calculates FTE, benefits, premium pay (shift differential), overtime, locality pay, cost of living allowance (COLA), special IT pay, awards, and annual pay raises. Costs are calculated using OPM-published salary and rates tables. All costs are categorized by Accounting Classification Code Structure (ACCS), cost category, funding source, and portfolio. In addition, the model is used in “what-if” analyses to answer questions about proposed changes in labor such as lapse, labor rates, inflation, and table of organization changes. The resulting five year answer sets are used to answer detailed questions about labor planning for NWS, NOAA, DOC, OMB, and Congressional requests without any PII data. The labor data contained in the model’s database is the master authorized (funded) position data for NWS. The model has its own user logon system and is accessed by its sole Federal user and its maintenance support contractor staff via the NOAA Silver Spring Metro Campus (SSMC) trusted campus network. The MYPS system retains user name, job title, and budgeted salary information for the purposes of budget forecast modeling.

MARS is a NOAA enterprise system that provides a common Business Intelligence (BI) platform to all NOAA Line Offices for financial reporting and querying, budget planning and commitment tracking. It consists of two modules, Reporting and Querying and Data Entry. The Data Entry module is not supported by MYPS. The MARS Reporting and Querying module is a business intelligence maintenance environment used for ongoing design, creation and testing of new reports; new extract, transform and load (ETL) jobs; and software patches and upgrades for eventual deployment to the Reporting and Querying module of MARS. MARS BI Maintenance Platform is accessible only via the NOAA Silver Spring Metro Campus (SSMC) trusted campus network. PII related information is collected solely for regression testing purposes within the MARS system. Once testing has been completed, the sample data will be retained for a time, and deleted within 3 years or sooner. Our mandate is to make sure any revisions to our processes operate correctly and produce correct answers on the MARS reports before promoting the revisions forward to TEST where yet another testing cycle occurs. Once the Federal client approves the system fix(es) on TEST, the final solution is only then migrated to PROD, with another final confirmation things worked in PROD before closing our Software Design Request (SDR) ticket.

Sample data is extracted from production to use during various development cycles that include previous fiscal year (FY) data and the current FY data. The resultant differences are compared between DEV or TEST to the PROD environment to prove the expected system modifications actually repaired the process or MARS report.

If dummy data was implemented, live data would still need to be extracted, but then systematically be revised to substitute real values for dummy values across multiple fiscal years and multiple database tables many of which enforce primary/foreign key relational constraints. After this exercise, the MARS team would still need to map backwards to the original data for direct comparison to our production system data or reports for validation of the changes. These steps would be costly in team resources with multiple developers working on multiple SDRs, but yet allowing correlated comparison of before and after change modification to the operational MARS production system as proof of task completion. Since the Government doesn't want to pay for these steps in time or dollars, the additional developer, system, and user controls have been added on all MARS developers and users giving them the responsibility to protect data from all unauthorized disclosures (e.g. NDAs mentioned previously above).

Government stakeholders need the MARS Financial Data Warehouse and they imposed the best possible security measures given the exigent trade-offs and limited available resources available (CPU speed, disk space, contract dollars, time, and staff).

The General Forecaster Vacancy System is a notification application that is used by regional workforce managers to make regional meteorological (met) interns (Met Interns) aware of upcoming general forecaster vacancies at NWS Weather Forecast Offices (WFOs), per an agreement between NWS management and the National Weather Service Employees Organization (NWSEO). The system contains a database of all the Met Interns in the regions. The database is maintained by the regional workforce managers using a web application which is accessed using LDAP authentication. Prior to posting a vacancy for a general forecaster (meteorologist) at a WFO, the workforce manager in the region uses the system too automatically send an email to all the met interns listed in the database. An intern who is interested in the listed vacancy clicks on an HTML hyperlink imbedded in the email to express their interest. The system counts the responses and a determination is made at the regional level, based on the number of responses, whether the vacancy will be advertised to status candidates only or to all hiring sources (USAJOBS, etc.). The web portal uses session cookies to time-out any open workforce manager sessions within five minutes to maintain security of the process. PII in the form of user name and email address is collected and retained as part of the application process.

The NOAA8850 Trusted Agent collects and stores Form CD591 (PIV request form) for government issued IDs, LDAP and Active Directory. The Trusted Agent processes security and badging forms for contractors only, not federal employees. The processing package includes fingerprints and a photograph, both taken by the badging office (but not stored in NOAA8850), driver's license and passport number. Once the Eastern Region Security Office approves a contractor for a CAC, it returns the CD-591s for the sponsored contractors and they are stored electronically. OF306 Declaration for Federal Employment is stored temporarily when the form needs to be scanned and saved to a drive prior to uploading into Accellion Secure File transfer to

send to the Security Office. *Contractors are advised to remove the form from their desktops after the transfer, but there is no current way to check this. The system is investigating courses of action to discover PII data within NOAA8850, including user terminals, but in the meantime, we are changing the confidentiality level to 'High' based on possible SSN retention on desktops.* A paper copy of the Security Coversheet/Request for Investigation Coversheet is also stored after removing Birth Date and SSN.

No PII is shared outside of the Department of Commerce (DOC) except in these cases: 1) only PII directly related to an individual's clearance is shared with DOC; if there is a security or privacy breach, applicable PII may be shared with the Department and other Federal agencies.

Authorities

U.S.C. § 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

15 U.S.C. § 1512, which confers general powers and duties authority to executive agencies, vesting jurisdiction and control of departments, bureaus, offices and branches.

Federal Information Security Management Act (Pub. L. 107 296, Sec. 3544).

E-Government Act (Pub. L. 107 347, Sec. 203).

From DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.

From DEPT-18: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

From DEPT-25: 5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 (HSPD 12), Federal Property and Administrative Services Act of 1949, as amended.

From GSA/GOVT-7: 5 U.S.C. 301; Federal Information Security Management Act of 2002 (44 U.S.C. 3554); E-Government Act of 2002 (Pub. L. 107-347, Sec. 203); Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et al.) and Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504 note); Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

From OPM/GOVT-1: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

This system has been classified as FIPS 199 moderate level.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

This is a new information system.

This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection*	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

***NOAA8205 integrated into this system.**

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (Check all that apply.)

Identifying Numbers (IN)					
a. Social Security*	X	e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License	X	j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
* Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					
* For MARS testing: A three tier approach (DEV, TEST, PROD) is implemented so that any new bug fixes or new developments are moved forward to TEST tier first, run in mock production setting on TEST, then once all regression testing has been validated and approvals given from Federal agent, the "code" is migrated into production. During testing periods, the TEST tier has PROD data to assure everything works as though it were in production. Afterwards housecleaning is conducted on TEST until the next testing cycle.					
There is also temporary storage of the OF306 before transmitting to the security office.					
Authorities: see DEPT 18 authorities in the system description.					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					
Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

* For badging purposes only

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run	X	f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)					

2.2 Indicate sources of the PII/BII in the system. (Check all that apply.)

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify)					

Non-government Sources			
Public Organizations		Private Sector	Commercial Data Brokers
Third Party Website or Application			
Other (specify):			

- 2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X\	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
----	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

- 3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

x	There are not any IT system supported activities which raise privacy risks/concerns.
---	--------------------------------------------------------------------------------------

Section 4: Purpose of the System

- 4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The NOAA8205 Trusted Agent collects and stores Form CD591 (PIV request form) for government issued IDs, LDAP and Active Directory. The Trusted Agent processes security and badging forms for contractors only, not federal employees. The processing package includes fingerprints and a photograph, both taken by the badging office (*but not stored in the system*), driver's license and passport number. Once the Eastern Region Security Office approves a contractor for a CAC, it returns the CD-591s for the sponsored contractors and they are stored electronically. Trusted agents are instructed to complete only Section A of the CD-591. They do not include the I-9 form and have never been requested to do so by OSY.

OF306 Declaration for Federal Employment is stored temporarily when the form needs to be scanned and saved to a drive prior to uploading into Accellion Secure File transfer to send to the Security Office. A paper copy of the Security Coversheet/Request for Investigation Coversheet is also stored after removing Birth Date and SSN. The only forms stored are redacted Coversheets and CD-591s which do not contain PII.

The MYPS system retains user name, job title and budgeted salary information for the purposes of budget forecast models.

The Forecaster Vacancy system retains name and email only for federal employees.

The MARS system retains sample PII for testing purposes only and discards after each testing cycle.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*In case of breach.

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	-----------------------------------------------

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input type="checkbox"/>	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. (*Check all that apply.*)

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. (*Check all that apply.*)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at:	
X	Yes, notice is provided by other means.	<p>Specify how:</p> <p>Form CD591, the DOC PIV request form, provides notice in that the request for information comes from the sponsor and registrar. The information comes from the applicant, who completes the form and provides it to the sponsor. There is also a privacy act statement on this form.</p> <p>https://mars.rdc.noaa.gov/docs/forms/NOAA MARS Rules of Behavior.pdf https://mars.rdc.noaa.gov/docs/forms/DOC NOAA MARS ND A v2.pdf</p> <p>Form OF306 states that the Office of Personnel Management is authorized to request this information under sections 1302, 3301, 3304, 3328, and 8716 of title 5, U. S. Code and addresses and Routine Uses.</p> <p>The MYPS, Forecaster Vacancy System, and MARS: Federal workers sign a privacy release pursuant to the Privacy Act of 1974 during on-boarding with NOAA/NWS; see https://www.justice.gov/opcl/privacy-act-1974 ; Conditions of disclosure; "For routine uses within a U.S. government agency" and "Other administrative purposes."</p>
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	<p>Specify how: Individuals can decline by not providing requested information to receive NOAA ID. However, without a NOAA ID, they cannot work at NOAA as a Federal Employee or Contractor.</p> <p>The information collected Forecaster Vacancy System is</p>
---	---------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		provided only if the service is desired. The information collected by MYPS is solely for budget purposes (no opt out) and MARS collects information solely for testing applications (no opt out).
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: If no consent is granted, no ID will be issued as in 7.2 above. This is the only purpose for this information. There is only one use for each of these: MYPS (budget) and MARS (testing) Forecaster Vacancy is voluntary for job openings and solely consists of user name and email address. There is only one use of the information.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Users are informed in person or in writing by their supervisors at time of onboarding, that they can update PII/information via NOAA LDAP or NOAA Locator. https://nsd.rdc.noaa.gov/ Forecaster Vacancy user name, email address and MYPS information updates are not applicable for the individual. However, updates may be implemented by HQ and FMC administrators at an individual's request in writing to one or the other. MARS PII is used solely for testing and thus the individual does not need to review/update PII/BII pertaining to them.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: MARS has built-in auditor for who accessed what report and when.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 11/20/2017 <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

<p>User name, Office location, and Telephone Number of NOAA employees and contractors are collected and maintained in NOAA8205 Active Directory and LDAP. NOAA8205 Administrators can access or alter this information; the Active Directory is not publicly accessible and has internal boundary controls in place to include firewall and Access Control Lists (ACLs).</p> <p>The NWS HQ Trusted agent (TA) collects and maintains CD591 information. This information is stored by the TA in a locked secure location; after three months, the information is shredded in accordance with NOAA Records Management schedule. (Contains name, phone number and email address.)</p> <p>The MYPS and MARS information is maintained in encrypted files and protected through Role Based Access Controls (RBAC).</p>

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i> : DEPT-13 , Investigative and Security Records, DEPT-18 , Employees Information Not Covered by Notices of Other Agencies; DEPT-25 , Access Control
---	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	and Identity Management System, GSA./GOVT-7 , Personal Identity Verification Identity Management System. OPM/GOVT-1 , General Personnel Records
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Schedule Series Chapter: 900 904-01 Building Identification Credential Files NOAA Chapter 100: Enterprise-Wide Functions Electronic Records schedule: NARA General Records Schedule 20, Electronic Records
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels.
(Check all that apply.)

X	Identifiability	Provide explanation: The loss of confidentiality could lead to identity theft for individuals affected.
X	Quantity of PII	Provide explanation: No access for average MARS user; limited access for MARS power users as needed to do their job function; and more access for top level managers who require access for those they manage.
X	Data Field Sensitivity	Provide explanation: In some cases, the CD306 containing a contractor SSN may not have been removed from a desktop. The system is working on addressing this issue.
X	Context of Use	Provide explanation: MARS links some PII data using natural keys for SQL table joins which report users cannot see.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: The information collected for badging purposes contains two forms of personal identification (ie Passport, Driver's license, etc.) which, if exposed during the course of collection and verification, could have an adverse impact to user confidentiality.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: The possibility of retention of the SSN, as stored electronically in the OF306, caused us to change our confidentiality rating from "moderate" to "high."
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

<p>System Owner</p> <p>Name: Tommy Thompson Sr. Office: NWS/ACIO Phone: (301) 427-6987 Email: Tommy.Thompson@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: THOMPSON.THOMAS.PAUL.SR.1200327841 <small>Digitally signed by THOMPSON.THOMAS.PAUL.SR.1200327841 Date: 2018.01.23 14:04:02 -05'00'</small></p>	<p>Information Technology Security Officer</p> <p>Name: Andrew Browne Office: NWS/ACIO Phone: (301) 427-9033 Email: Andrew.Browne@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: BROWNE.ANDREW.PATRICK.1472149349 <small>Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2018.01.23 10:36:05 -05'00'</small></p>
<p>Authorizing Official</p> <p>Name: Richard Varn Office: NWS/ACIO Phone: (301) 427-0927 Email: Richard.Varn@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: VARN.RICHARD.ALAN.II.1073462041 <small>Digitally signed by VARN.RICHARD.ALAN.II.1073462041 Date: 2018.01.23 14:51:31 -05'00'</small></p>	<p>Bureau Chief Privacy Officer</p> <p>Name: Mark Graff Office: NOAA/OCIO Phone: (301) 628-5658 Email: Mark.Graff@noaa.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>Signature: GRAFF.MARK.HYRUM.1514447892 <small>Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.23 15:45:26 -05'00'</small></p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

Mark Graff - NOAA Federal

From: Mark Graff NOAA Federal
Sent: Wednesday, January 24, 2018 9:31 AM
To: Sarah Brabson NOAA Federal
Subject: Re: Reminders
Attachments: NOAA0500 PIA_Annual_Review_Certification_Form 14Dec17_ISSO Signed mhg.pdf; NOAA0500_PTA_Updated_14Dec17 LBH (2) mhg.pdf; NOAA0500 PIA_17Jan18 ISSO_Signed mhg.pdf

Here is NOAA0500, all docs signed

(b)(5)
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted] I'd defer to you.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Wed, Jan 24, 2018 at 8:54 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
Mark, Nancy D. reminded me that NOAA5045 no longer has PII other than user ID. So I have changed the color code and put "no" for PII, on the spreadsheet. Now I'll email DOC and ask them to remove the PII and the old PTA from their page, sending them the Sept PTA as evidence. I must have been especially distracted when this change occurred.

Please sign the NOAA0500 PIA and PTA that Zach sent you, as well as the certification I sent you.

Please also sign the NOAA8884 PIA and PTA. I need to get this CRB scheduled, as the ATO is 4 30 18.

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)

(b)(6)

Ce

(b)(6)

**U.S. Department of Commerce
NOAA**



**Privacy Impact Assessment
for the
NOAA Research & Development High Performance Computing
System (R&D HPCS) – NOAA0500**

Reviewed by: _____, Bureau Chief Privacy Officer
Mark Graff

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment NOAA Research & Development High Performance Computing System (R&D HPCS) – NOAA0500

Unique Project Identifier: NOAA0500

Introduction: System Description

NOAA0500 system provides research and development weather models in support of NOAA's operational mission. The R&D HPCS operates large scale, extreme computing environments that encompass multiple geographic sites, and heterogeneous supercomputing architectures. This system supports NOAA's mission by providing cutting edge technology for weather and climate model developers. These models eventually form the basis for NOAA's daily weather forecasts, storm warnings, and climate change forecasts. System users include scientists from multiple NOAA Line Offices, and their research collaborators, including some foreign nationals.

NOAA's R&D HPC system (R&D HPCS) provides four fundamental HPC functions:

1. Large-scale computing provides computing for development, testing, and production integrations of NOAA environmental models. The workload that runs on this subsystem is characterized by computer-intensive codes with I/O characterized by regular snapshots of diagnostic fields.
2. Analysis and interactive computing provides computing for the post-processing of data from production runs and the analysis of post-processed data, code development, and debugging. The workload that runs on this subsystem is characterized by data-intensive codes requiring high I/O bandwidth.
3. Data archiving provides long-term storage of post-processed model runs and analyses.
4. Networking links these subsystems together.

The users of the system are primarily, but not exclusively, NOAA employees who represent the following offices:

1. NOAA/ESRL Global Systems Division, Boulder, Colorado
2. NOAA National Weather Service (NWS), National Centers for Environmental Prediction (NCEP), Environmental Modeling Center (EMC), Camp Springs, Maryland
3. NOAA Geophysical Fluid Dynamics Laboratory (GFDL), Princeton, New Jersey

These users access the system and submit weather or climate modeling application program runs via job scheduling software. These models contain parallelized code to take advantage of the large scale, highly parallelized environment offered by the HPCS. This is necessary to support the science. Modeling jobs can be extremely large (e.g., 1200 processors required), because they incorporate different local, regional, or global atmospheric and ocean models to create an ensemble model program. The scheduling software automatically identifies and collects the necessary processors to run the job, and controls its execution. Therefore, the user never has any direct interaction with the compute nodes of the system.

In accordance with applicable security controls, users of the R&D HPCS must first request an account prior to access approvals. Those users who would like an account must supply the requested/required data on a web-based form. Those requests and associated data supplied by the user are stored in a database and only accessible by authorized privileged account administrators. The user-supplied data is used only for identification and creation of unique accounts as well as for contact purposes if there should be a problem with the account. The user base consists of Federal employees, contractors, foreign nationals and casual collaborators.

Weather and climate data is collected from a variety of sources and fed into the system by the user community. All of this data is vetted by the NOAA scientific community through processes outside of this system, to guarantee its authenticity and integrity. Once entered into the R&D HPCS, the system security controls are designed to guarantee the integrity of this data.

The current configuration of the R&D HPCS is architected along organizational lines. Large-scale computing, analysis computing, and storage are located at the following locations:

1. NOAA Earth System Research Laboratory (ESRL), David Skaggs Research Center (DSRC325 N. Broadway Street, Boulder, Colorado 80305,
2. NOAA Geophysical Fluid Dynamics Laboratory (GFDL), Princeton University Forrestal Campus, 201 Forrestal Road, Princeton, New Jersey 08450,
3. NOAA Environmental, Security Computing Center (NESCC), 1000 Galliher Drive, Fairmont, WV 26554,
4. NOAA Center for Weather and Climate Prediction (NCWCP), 5830 University Research Court, College Park, MD 20740.

The R&D HPCS system boundary encompasses these locations. Interconnection Security Agreements with ORNL, N-Wave, NCEP, GFDL, and ESRL provide general support and services such a LAN/WAN connectivity, authentication and identification controls, DNS, WEB and other IT infrastructure support.

The National Centers for Environmental Prediction (NCEP) utilize data acquired from commercial, other U.S Government and International sources to execute NCEP mission. A subset of this data, referred to as “restricted data” is made available to NCEP with restrictions on further dissemination.* As a direct or indirect party to the agreements governing the use of this Restricted Data, NCEP is charged with protecting restricted data during use and identifying restricted data to managers, users, staff and partners supporting NCEP mission.

*NOAA has agreements with ships and planes, which collect local weather data while at sea/in the air and share with NOAA. The data includes the positions of those ships and planes, because the two types of information cannot be separated. The location data is considered proprietary.

Authority for collection of information: 5 U.S.C. 301 5 U.S.C. 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Information sharing: The PII in the system will not be shared. The BII (restricted data), NCEP receives and shares with RDHPC.

NCEP FIPS 199 Impact Level: HIGH

R&D HPCS FIPS 199 Impact Level: MODERATE

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- This is a new information system.
- This is an existing information system with changes that create new privacy risks.

(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify):			

- This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)			
a. Social Security*		e. File/Case ID	i. Credit Card
b. Taxpayer ID		f. Driver's License	j. Financial Account
c. Employer ID		g. Passport	k. Financial Transaction
d. Employee ID		h. Alien Registration	l. Vehicle Identifier
m. Other identifying numbers (specify):			
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:			

General Personal Data (GPD)			
a. Name	X	g. Date of Birth	m. Religion
b. Maiden Name		h. Place of Birth	n. Financial Information

c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	
e. Age		k. Email Address		q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	
b. Job Title		e. Email Address	X	h. Work History	
c. Work Address		f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)					
WCOS proprietary and restricted data (locations of ships and planes providing weather data).					

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	X
Telephone		Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify: NWS NCEP program owns the data and is responsible for its distribution.)					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	

Third Party Website or Application			
Other (specify):			

- 2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

<input checked="" type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
-------------------------------------	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

- 3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

<input checked="" type="checkbox"/>	There are not any IT system supported activities which raise privacy risks/concerns.
-------------------------------------	--------------------------------------------------------------------------------------

Section 4: Purpose of the System

- 4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Archive and Storage only –no dissemination or processing within the R&D HPCS environment			

Section 5: Use of the Information

5.1 The National Centers for Environmental Prediction (NCEP) utilize data acquired from commercial, other U.S Government and International sources to execute NCEP mission. A subset of this data, referred to as “restricted data” is made available to NCEP with restrictions on further dissemination. As a direct or indirect party to the agreements governing the use of this Restricted Data, NCEP is charged with protecting restricted data during use and identifying restricted data to managers, users, staff and partners supporting NCEP mission.

NCEP Restricted Data Storage Locations

Restricted data can be found in the following locations:

- System networks [transitory]
- Long-term scratch file system in the path /tbd/tbd [transitory]
- Fast scratch file system in the path /tbd/tbd [stored]
- NCEP-Authorized user home file systems [stored]
- Backup media holding NCEP files [stored]

NCEP Restricted Data Protection

Restricted data stored is protected by setting each file containing restricted data as readable only by users in the RSTPROD group.

Authorized Users

NCEP explicitly grants access to restricted data to NCEP staff and associates whose work utilizes these data. This access is granted through each system’s account approval process.

Privileged Users

Privileged users include staff that supports the systems, storage, and networks utilized to accomplish NCEP work. Privileged access includes access to a systems administrator or root account on a system, privileged access to network devices, and other than general user access to system storage devices, including data archiving or backup equipment. A privileged user has access to restricted data as a result of their privileged access to these systems.

Limitations on Privileged Users

Privileged users are notified that any of the following actions may be taken only with NCEP Management and Site Manager approval:

- Copying or moving restricted data to a location not identified as an NCEP Restricted Data Storage Location
- Making restricted data available by any means to a user that is not identified by NCEP Management as authorized to access restricted data
- Making restricted data available by any means to the public such as through an internet-connected server or public portal

In accordance with applicable security controls, users of the R&D HPCS must first request an account prior to access approvals. Those users who would like an account must supply the requested/required data on a web-based form. Those requests and associated data supplied by the user are stored in a database and only accessible by authorized privileged account administrators. The user-supplied data is used only for identification and creation of unique accounts as well as for contact purposes if there should be a problem with the account. The user base consists of Federal employees, contractors, foreign nationals and casual collaborators.

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

<input checked="" type="checkbox"/>	The PII/BII in the system will not be shared.
-------------------------------------	-----------------------------------------------

- 6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input checked="" type="checkbox"/>	Yes, this IT system connects with or receives information from another IT system(s) authorized to process BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NCEP. AC-1, 3, 4, 5, 6, 14, 21, 22; AU-2, 6; IA-4, 5, 8; and SC-4, 7, 8
<input type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

- 6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
Other (specify):			

Section 7: Notice and Consent

- 7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

<input checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
-------------------------------------	------------------------------------------------------------------------------------------------------------------------------

X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The <u>Privacy Act statement</u> and/or privacy policy can be found at: NCEP: (located above Clear Form button) http://www.nco.ncep.noaa.gov/sib/restricted_data/restricted_data_sib/register/ and R&D HPCS AIM: (located at bottom right / top line) https://aim.rdhpcs.noaa.gov/	
X	Yes, notice is provided by other means.	Specify how: Notification and use is provided by NCEP on their rstprod web site: http://www.nco.ncep.noaa.gov/sib/restricted_data/restricted_data_sib/ Proprietary data is shared through NCEP agreements.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Proprietary data collected is provided through organizations with which NCEP has agreements for the use and dissemination of the data etc. Account users may decline to provide PII, by not providing it, but this will affect their ability to establish an account.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Proprietary data is provided through agreements, for research purposes as agreed on. Account users: By providing information to establish an account, the user consents to its uses – access to the data and trouble-shooting any problems with the account.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

x	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Account users may update their information at any time, and we ask them to update at least annually, using instructions on the Web site
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: This is NA for the proprietary data.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement. All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Users who would like an account must supply the requested/required data on a web-based form. Those requests and associated data supplied by the user are stored in a database and only accessible by authorized privileged account administrators. The user-supplied data is used only for identification and creation of unique accounts as well as for contact purposes if there should be a problem with the account.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>3/15/2017</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

The WCCOS data stored within the R&D HPCS and is only accessible to NCEP, which approves and provides access. Network accessibility to the storage and archive system is via internal connection (private circuits) and does not traverse the internet. Both NCEP and R&D HPCS users are required to login utilizing either 2-factor authentication and or CAC authentication.

R&D HPCS has 24hr network and system monitoring and security logs weekly for suspicious activities, attempted logins etc. Data residing within the R&D HPCS system boundary remains within a data center which is also monitored 24x7, has CCTV, and armed guards. Access to the data center where the Storage and Archive resides is accessible via CAC/Badge reader to authorized and vetted NOAA personnel and contractors. Maintenance, and other personnel not previously vetted by NOAA are escorted and observed at all times within the data center.

In accordance with applicable security controls, users of the R&D HPCS must first request an account prior to access approvals. Those users who would like an account must supply the

requested/required data on a web-based form. Those requests and associated data supplied by the user are stored in a database and only accessible by authorized privileged account administrators. The user-supplied data is used only for identification and creation of unique accounts as well as for contact purposes if there should be a problem with the account. The user base consists of Federal employees, contractors, foreign nationals and casual collaborators.

Section 9: Privacy Act

- 9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i> : DEPT-18, Employees Personnel Files not Covered by other Notices; COMMERCE/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

Section 10: Retention of Information

- 10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA 1200-02, Research Notebooks and NOAA1200-6, Data Requests.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.

	No, retention is not monitored for compliance to the schedule. Provide explanation:
--	-------------------------------------------------------------------------------------

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal		
Shredding		Overwriting
Degaussing	X	Deleting
Other (specify): The referenced data has a very long/perpetual life. Storage media that has potentially been used for this referenced data is degaussed once retired and prior to being removed from the system boundary.		

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: An individual may be identified from information in the accounts database.
x	Quantity of PII	Provide explanation: The only PII is account contact information,
X	Data Field Sensitivity	Provide explanation: There is no sensitive PII.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: AC-1, 3, 4, 5, 6, 14, 21, 22; AU-2, 6; IA-4, 5, 8; and SC-4, 7, 8
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: Addition of a Privacy Act Statement on account page
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: Addition of a Privacy Act Statement on account page
	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

<p>Information System Security Officer or System Owner Name: Justin May (ISSO) Office: NOAA/OCIO Phone: (303) 437-8155 Email: justin.may@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: MAY.JUSTIN.NATHANIEL.1039635980 <small>Digitally signed by MAY.JUSTIN.NATHANIEL.1039635980 Date: 2018.01.17 18:08:24 -07'00'</small></p> <p>Date signed:</p>	<p>Information Technology Security Officer Name: Jean Apedo Office: NOAA/OCIO Phone: (301) 628-5730 Email: jean.apedo@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: APEDO.JEAN.1188076064 <small>Digitally signed by APEDO.JEAN.1188076064 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn APEDO.JEAN.1188076064 Date: 2018.01.18 06:23:46 -05'00'</small></p> <p>Date signed: .1188076064</p>
<p>Authorizing Official Name: Zachary Goldstein Office: NOAA/OCIO Phone: (301) 713-9600 Email: zachary.goldstein@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: GOLDSTEIN.ZACHARY.G.1228698985 <small>Digitally signed by GOLDSTEIN.ZACHARY.G.1228698985 Date: 2018.01.23 09:27:19 -05'00'</small></p> <p>Date signed:</p>	<p>Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>Signature: GRAFF.MARK.HYRUM.151447892 <small>Digitally signed by GRAFF.MARK.HYRUM.151447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.151447892 Date: 2018.01.24 09:25:46 -05'00'</small></p> <p>Date signed: 47892</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NOAA Research & Development High Performance Computing System (R&D HPCS)

FISMA Name/ID (if different): R&D HPCS - NOAA0500

Name of IT System/ Program Owner: Frank Indiviglio

Name of Information System Security Officer: Justin May

Name of Authorizing Official(s): Zachary Goldstein

Date of Last PIA Compliance Review Board (CRB): 14 Mar 17

(This date must be within three (3) years.)

Date of PIA Review: 14 Dec 17

Name of Reviewer: Justin May

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer (SO or ISSO): MAY.JUSTIN.NATHANIEL.1039635980

Digitally signed by MAY JUSTIN NATHANIEL 1039635980
DN: cn=MAY JUSTIN NATHANIEL 1039635980, c=US, o=U.S. Government,
ou=CONTRACTOR
Reason: I am the author of this document
Date: 2017.12.14 22:29:20 -07:00

Date of BCPO Review: 1/24/18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: 7892

GRAFF.MARK.HYRUM.151444
Digitally signed by GRAFF MARK HYRUM 1514447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=OTHER, cn=GRAFF MARK HYRUM 1514447892
Date: 2018.01.24 09:18:14 -05:00

U.S. Department of Commerce
NOAA



Privacy Threshold Analysis
For the
NOAA Research & Development High Performance Computing
System (R&D HPCS) – NOAA0500

U.S. Department of Commerce Privacy Threshold Analysis NOAA Research and Development High Performance Computer

Unique Project Identifier: NOAA0500

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: NOAA0500 system is considered to be a General Support System which provides research and development weather models in support of NOAA's operational mission. The R&D HPCS operates large scale, extreme computing environments that encompass multiple geographic sites, and heterogeneous supercomputing architectures. This system supports NOAA's mission by providing cutting edge technology for weather and climate model developers. These models eventually form the basis for NOAA's daily weather forecasts, storm warnings, and climate change forecasts. System users include scientists from multiple NOAA Line Offices, and their research collaborators, including some foreign nationals.

NOAA's R&D HPC system (R&D HPCS) provides four fundamental HPC functions:

1. Large scale computing provides computing for development, testing, and production integrations of NOAA environmental models. The workload that runs on this subsystem is characterized by compute intensive codes with I/O characterized by regular snapshots of diagnostic fields.
2. Analysis and interactive computing provides computing for the post processing of data from production runs and the analysis of post processed data, code development, and debugging. The workload that runs on this subsystem is characterized by data intensive codes requiring high I/O bandwidth.
3. Data archiving provides long term storage of post processed model runs and analyses.
4. Networking links these subsystems together.

The users of the system are primarily, but not exclusively, NOAA employees who represent the following offices:

1. NOAA/ESRL Global Systems Division, Boulder, Colorado
2. NOAA National Weather Service (NWS), National Centers for Environmental Prediction (NCEP), Environmental Modeling Center (EMC), Camp Springs, Maryland
3. NOAA Geophysical Fluid Dynamics Laboratory (GFDL), Princeton, New Jersey

These users access the system and submit weather or climate modeling application program runs via job scheduling software. These models contain parallelized code to take advantage of the

large scale, highly parallelized environment offered by the HPCS. This is necessary to support the science. Modeling jobs can be extremely large (e.g., 1200 processors required), because they incorporate different local, regional, or global atmospheric and ocean models to create an ensemble model program. The scheduling software automatically identifies and collects the necessary processors to run the job, and controls its execution. Therefore, the user never has any direct interaction with the compute nodes of the system.

Weather and climate data is collected from a variety of sources and fed into the system by the user community. All of this data is vetted by the NOAA scientific community through processes outside of this system, to guarantee its authenticity and integrity. Once entered into the R&D HPCS, the system security controls are designed to guarantee the integrity of this data.

The current configuration of the R&D HPCS is architected along organizational lines. Large scale computing, analysis computing, and storage are located at the following locations:

1. NOAA Earth System Research Laboratory (ESRL), David Skaggs Research Center (DSRC325 N. Broadway Street, Boulder, Colorado 80305,
2. NOAA Geophysical Fluid Dynamics Laboratory (GFDL), Princeton University Forrestal Campus, 201 Forrestal Road, Princeton, New Jersey 08450,
3. NOAA Environmental, Security Computing Center (NESCC), 1000 Galliher Drive, Fairmont, WV 26554,
4. NOAA Center for Weather and Climate Predication (NCWCP), 5830 University Research Court, College Park, MD 20740.

The R&D HPCS system boundary encompasses these locations. Interconnection Security Agreements with ORNL, N-Wave, NCEP, GFDL, and ESRL provide general support and services such a LAN/WAN connectivity, authentication and identification controls, DNS, WEB and other IT infrastructure support.

Questionnaire:

1. What is the status of this information system?

- This is a new information system. *(Continue to answer questions and complete certification.)*
- This is an existing information system with changes that create new privacy risks. *(Complete chart below, continue to answer questions, and complete certification)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

This is an existing information system in which changes do not create new privacy risks. *(Skip questions and complete certification)*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *(Please describe the activities which may raise privacy concerns.)*

No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)"

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4.a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

- Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.
- No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

I certify the criteria implied by one or more of the questions above **apply** to the NOAA0500 IS and as a consequence of this applicability, I will perform and document a PIA for this IT system.

I certify the criteria implied by the questions above **do not apply** to the NOAA0500 IS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Frank Indiviglio

Signature of ISSO or SO: 0787 HART.LESLIE.B.136587 Digitally signed by HART.LESLIE.B.1365870787 Date: 2018.01.16 11:09:13 -07'00' Date: _____

Leslie Hart (acting for Frank Indiviglio)

Name of Information Technology Security Officer (ITSO): Jean Apedo

Signature of ITSO: .1188076064 APEDO.JEAN.1188076064 Digitally signed by APEDO.JEAN.1188076064 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=APEDO.JEAN.1188076064 Date: 2018.01.17 06:32:12 -05'00' Date: _____

Name of Authorizing Official (AO): Zachary Goldstein

Signature of AO: GOLDSTEIN.ZACHARY.G.1228698985 GOLDSTEIN.ZACHARY.G.1228698985 Digitally signed by GOLDSTEIN.ZACHARY.G.1228698985 Date: 2018.01.23 09:24:25 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.24 09:19:48 -05'00' Date: _____

Mark Graff - NOAA Federal

From: Mark Graff NOAA Federal
Sent: Wednesday, January 24, 2018 10:58 AM
To: Sarah Brabson NOAA Federal
Subject: Re: NOAA8884 PIA and PTA for your signature
Attachments: NOAA8884 PIA 011618 Final_SO ITSO Signature mhg.pdf; NOAA8884 PTA 01162018 Final_SO ITSO Signed mhg.pdf

Both signed and attached thanks!

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Tue, Jan 23, 2018 at 1:03 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

Mark, please sign when you have time. The ATO is 4 30 18. thx

Forwarded message

From: **Sarah Brabson - NOAA Federal** <sarah.brabson@noaa.gov>

Date: Tue, Jan 23, 2018 at 10:23 AM

Subject: NOAA8884 PIA and PTA for your signature

To: Mark Graff NOAA Federal <mark.graff@noaa.gov>

Cc: Gary Petroski NOAA Federal <gary.petroski@noaa.gov>

Revised per your comments, and okay'd for signatures by you. Despite the file names, the AO did sign as well.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division

Office [301 628 5751](tel:3016285751)

Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division

Office [301 628 5751](tel:3016285751)

Ce (b)(6)

**U.S. Department of Commerce
NOAA**



**Privacy Impact Assessment
for the
Southern Region General Support System (GSS) (NOAA8884)**

Reviewed by: Mark Graff, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment NOAA / Southern Region General Support System (GSS) (NOAA8884)

Unique Project Identifier: 006-000351100 00-48-02-00-01-00

Introduction: System Description

The National Weather Service (NWS) Southern Region provides weather, hydrologic, and climate forecasts and warnings for the United States, its territories, adjacent waters and ocean areas, for the protection of life and property and the enhancement of the national economy. NWS data and products form a national information database and infrastructure, which can be used by our partners, the public, and the global community. Issuance of products including forecasts and warning is dependent on a complex interaction of many information resources and systems. The GSS is designed and used to support the collection, processing, and dissemination of data that supports the mission of the organization. It also supports the administrative functions and the scientific and technical research and innovations activities of employees within the organization.

Although there are a variety of hardware and operating systems, all the activities are interconnected. The system provides direct or indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems, client-server and web-based server systems. The system supports a variety of users, functions, and applications, including word processing, financial data, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training, research and development, and collaboration.

All administrative functions relating to people and PII are conducted on-line with these systems: MARS, CBS and NFC. The system does not keep any information local, since all information can be accessed via the on line databases.

Personally Identifiable Information (PII) maintained in the system is:

1. Located in a local database at the local Weather Forecast Office/River Forecast Center that maintains information on volunteers who provide weather reports to them.
2. Located in an encrypted Folder located on the Regional HQ NAS device, under the user of the Regional ISSO. This information is required for locally stationed contractors that require CAC authorization. This data is compiled by the Trusted Agent (TA) for submittal to the OSY for background checks and input to the TASS system.

No information is shared except with OSY, for the Trusted Agent information and in the case of security or privacy breach (see Section 6.1)

The statutory authority covering the collection of this data is 5 U.S.C 301, Departmental Regulations and 15 USC 1512 - Sec. 1512, Powers and Duties of Department [of Commerce].

Authorities from DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.

Authorities from DEPT-25: 5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075.

This is a moderate level system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

This is a new information system.

This is an existing information system with no new privacy risks.

This is an existing information system with changes that create new privacy risks.

(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	

b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	X*
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

**NOAA8205 was incorporated into this collection.*

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: See authorities from DEPT-18 in the system description.					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	Version Number: 01-2015
b. Maiden Name		h. Place of Birth	X	n. Financial Information	
c. Alias	X	i. Home Address	X	o. Medical Information	
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): General description of volunteer's home location.					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address		f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X	d. Photographs	X	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

--

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. (Check all that apply.)

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify)					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify): Cooperative observers.					

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	X	Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	X
Other (specify):			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
--	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.
----------	--------------------------------------------------------------------------------------

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify): Information on weather volunteers.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

There are local databases at the local WFO/RFC that maintain information on volunteers who provide weather reports to them. The databases hold contact information on these volunteers, in order to contact them when needed and as a record of who provides the information.

All of this information is voluntary and the Co-Op Observer has the right to opt-out of the program at any time. This information is entered into a NOAA database called the Cooperative Station Service Accountability (CSSA), located and maintained by NWS Office of Climate Weather and Water Services (OCWWS).

A locally assigned NWS staff person is responsible for entry of this information into the CSSA database. A limited amount of this data is retained in the local office for quick access to contact the Co-Op in case of equipment outages.

This information is collected from members of the public.

The Regional ISSO has been assigned the Trusted Agent (TA) duties for multiple contractors. All badging paperwork and OSY Security/Investigative coversheets for the contractors are being saved to the ISSO's system. All transmission of PII data flows to other organizational entities (OSY) via secured Acellion SFTP server. All PII data residing on the NOAA8884 system is encrypted at rest with the use of McAfee Endpoint Security protection. This is an encrypted Directory only assessable from the user with CAC authentication.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X*		
DOC bureaus	X*		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*In case of breach. For DOC bureaus, also for submission of CAC documents to OSY.

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	-----------------------------------------------

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input type="checkbox"/>	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors*	X		
Other (specify):			

*Contractors log in to review their information before the TA approves.

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and
---	------------------------------------------------------------------------------------------------------

	discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and privacy policy can be found at: http://www.nws.noaa.gov/om/coop/index.htm .	
X	Yes, notice is provided by other means.	Specify how: There are privacy act statements on the federal-wise forms used by the TA. Notice to volunteers is provided when information is collected,
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: All of this information is voluntary, as part of the cooperative agreement to work with the NWS on providing observations. The only means of providing the PII is by completing and signing the cooperative agreement form. Prospective contractors may decline, but their employment would be affected.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: The only use of the information is for contact purposes, which is given as part of the signed agreement. No other uses are suggested or specified. For the clearance, there is only one use for the information.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: The local manager visits each volunteer twice monthly to monitor equipment and answer questions. Updates can be made then, or emailed, as explained by the manager during orientation. Contractors can log into the TA system to review their information but cannot make changes.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. (Check all that apply.)

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Any access to the local Database is logged and saved. AD maintains logging of all access to file system
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>4/19/2017</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher. MODERATE
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Access to the system maintaining the PII is controlled by access via Active Directory and the use of CAC (PIV) cards. Only employees with authority to maintain this database are allowed access to the information.

Trusted Agent data is located in an encrypted Folder located on the Regional HQ NAS device, under the user of the Regional ISSO. Can only be decrypted by use of CAC card using McAfee Files and Folders encryption for the ISO only.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (A new system of records notice (SORN) is required if the system is not covered by an existing SORN).

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

X	Yes, this system is covered by an existing system of records notice (SORN).
---	-----------------------------------------------------------------------------

	COMMERCE/NOAA-11 , Contact information for members of the public requesting or providing information related to NOAA's mission; COMMERCE/DEPT-13 , Investigative and Security Records. COMMERCE/DEPT-25 , Access Control and Identity Management
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule: Chapter 1300- Weather, 1307-05
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	<input checked="" type="checkbox"/>	Overwriting	
Degaussing	<input checked="" type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input checked="" type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Individual's PII are in the system.
X	Quantity of PII	Provide explanation: Only name and contact information for volunteers, and names of employees, are in the system.
X	Data Field Sensitivity	Application data has many sensitive fields filled out.
X	Context of Use	Voluntary submission of PII for internal use only
	Obligation to Protect Confidentiality	
X	Access to and Location of PII	Secured local database managed by limited Federal employees
	Other:	Provide explanation:

Section 12: Analysis





12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

<p>System Owner or Information System Security Officer</p> <p>Name: John Duxbury Office: NWS/SR Phone: 682-703-3703 Email: john.duxbury@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p>  <p>DUXBURY.JOHN.C.1365877730 2018.01.17 11:58:34 -06'00'</p>	<p>Information Technology Security Officer</p> <p>Name: Andrew Browne Office: NOAA NWS Office of the CIO Phone: 301-427-9033 Email: beckie.koonge@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>BROWNE.ANDREW.PATRICK.1472149349</p>  <p>Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2018.01.22 15:39:20 -05'00'</p>
<p>Authorizing Official</p> <p>Name: Steven Cooper Office: NWS/SR Phone: 682-703-3700 Email: steven.cooper@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>COOPER.STEVE.N.G.1365850930</p>  <p>Digitally signed by COOPER.STEVEN.G.1365850930 Date: 2018.01.22 14:11:48 -06'00'</p>	<p>Bureau Chief Privacy Officer</p> <p>Name: Mark Graff Office: NOAA Privacy Office Phone: 301-628-5658 Email: mark.graff@noaa.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>Signature: GRAFF.MARK.HYRUM.1514447892</p>  <p>Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.24 10:56:25 -05'00'</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

**U.S. Department of Commerce
NOAA**



**Privacy Threshold Analysis
for the
Southern Region GSS (NOAA8884)**

U.S. Department of Commerce Privacy Threshold Analysis

Southern Region GSS (NOAA8884)

Unique Project Identifier: 006-000351100 00-48-02-00-01-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

The National Weather Service (NWS) Southern Region provides weather, hydrologic, and climate forecasts and warnings for the United States, its territories, adjacent waters and ocean areas, for the protection of life and property and the enhancement of the national economy. NWS data and products form a national information database and infrastructure, which can be used by our partners, the public, and the global community. Issuance of products including forecasts and warning is dependent on a complex interaction of many information resources and systems. This system is designed and used to support the collection, processing, and dissemination of data that supports the mission of the origination. It also supports the administrative functions and the scientific & technical research and innovations activities of employees within the organization.

Although there are a variety of hardware and operating systems, all the activities are interconnected. The system provides direct or indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems; client-server and web-based server systems. The system supports a variety of users, functions, and applications; including word processing, financial data, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training, research and development and collaboration.

Questionnaire:

1. What is the status of this information system?

_____ This is a new information system. *Continue to answer questions and complete certification.*

This is an existing information system with changes that create new privacy risks.
 Complete chart below, continue to answer questions, and complete certification.

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					
*NOAA8205 was incorporated into this collection.					

This is an existing information system in which changes do not create new privacy risks. Skip questions and complete certification.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. Please describe the activities which may raise privacy concerns.

The Regional ISSO has been assigned the Trusted Agent (TA) duties for multiple contractors. All badging paperwork and OSY Security/Investigative coversheets for the contractors are being saved to the ISSO’s system.
 All transmission of PII data flows to other organizational entities (OSY) via secured Acellion SFTP server.
 All PII data residing on the NOAA8884 system is encrypted at rest with the use of McAfee Endpoint Security protection. This is an encrypted Directory only assessable from the user with CAC authentication.

No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the submitter has a commercial interest” and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.).”

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the Southern Region GSS (NOAA8884) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

John Duxbury (SO)

Signature of ISSO or SO:  Digitally signed by DUXBURY.JOHN.C.1365877730
2018.01.18 07:50:53 -06'00' Date: _____

Name of Information Technology Security Officer (ITSO):

Andrew Browne (ITSO)

Signature of ITSO: BROWNE.ANDREW.PA
TRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349
Date: 2018.01.22 15:38:35 -05'00' Date: _____

Name of Authorizing Official (AO):

Steven Cooper

Signature of AO: COOPER.STEVEN.G.136
5850930 Digitally signed by COOPER.STEVEN.G.1365850930
Date: 2018.01.22 14:10:31 -06'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1
514447892 Digitally signed by GRAFF MARK HYRUM 1514447892
DN: c=US, o=U S Government, ou=DoD, ou=PKG,
ou=OTHER, cn=GRAFF MARK HYRUM 1514447892
Date: 2018 01 24 10 52 07 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Wednesday, January 24, 2018 11:25 AM
To: Gioffre, Kathy (Federal); CPO
Cc: Mark Graff NOAA Federal; Gary Petroski NOAA Federal
Subject: NOAA8884 PIA and PTA for DOC review
Attachments: NOAA8884 PIA 011618 Final_SO ITSO Signature mhg.pdf; NOAA8884 PTA 01162018 Final_SO ITSO Signed mhg.pdf

Kathy, NOAA8884 is the system for which we withdrew our PIA a few months ago because the ISSO had just become a trusted agent and updates needed to be made.

The ATO is April 30, 2018. I am hoping that the CRB can be fit in in place of one of the NOAA systems for which we are providing certifications.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751

Ce (b)(6)

**U.S. Department of Commerce
NOAA**



**Privacy Impact Assessment
for the
Southern Region General Support System (GSS) (NOAA8884)**

Reviewed by: Mark Graff, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment NOAA / Southern Region General Support System (GSS) (NOAA8884)

Unique Project Identifier: 006-000351100 00-48-02-00-01-00

Introduction: System Description

The National Weather Service (NWS) Southern Region provides weather, hydrologic, and climate forecasts and warnings for the United States, its territories, adjacent waters and ocean areas, for the protection of life and property and the enhancement of the national economy. NWS data and products form a national information database and infrastructure, which can be used by our partners, the public, and the global community. Issuance of products including forecasts and warning is dependent on a complex interaction of many information resources and systems. The GSS is designed and used to support the collection, processing, and dissemination of data that supports the mission of the organization. It also supports the administrative functions and the scientific and technical research and innovations activities of employees within the organization.

Although there are a variety of hardware and operating systems, all the activities are interconnected. The system provides direct or indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems, client-server and web-based server systems. The system supports a variety of users, functions, and applications, including word processing, financial data, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training, research and development, and collaboration.

All administrative functions relating to people and PII are conducted on-line with these systems: MARS, CBS and NFC. The system does not keep any information local, since all information can be accessed via the on line databases.

Personally Identifiable Information (PII) maintained in the system is:

1. Located in a local database at the local Weather Forecast Office/River Forecast Center that maintains information on volunteers who provide weather reports to them.
2. Located in an encrypted Folder located on the Regional HQ NAS device, under the user of the Regional ISSO. This information is required for locally stationed contractors that require CAC authorization. This data is compiled by the Trusted Agent (TA) for submittal to the OSY for background checks and input to the TASS system.

No information is shared except with OSY, for the Trusted Agent information and in the case of security or privacy breach (see Section 6.1)

The statutory authority covering the collection of this data is 5 U.S.C 301, Departmental Regulations and 15 USC 1512 - Sec. 1512, Powers and Duties of Department [of Commerce].

Authorities from DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.

Authorities from DEPT-25: 5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075.

This is a moderate level system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

This is a new information system.

This is an existing information system with no new privacy risks.

This is an existing information system with changes that create new privacy risks.

(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	X*
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

**NOAA8205 was incorporated into this collection.*

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: See authorities from DEPT-18 in the system description.					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	Version Number: 01-2015
b. Maiden Name		h. Place of Birth	X	n. Financial Information	
c. Alias	X	i. Home Address	X	o. Medical Information	
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): General description of volunteer's home location.					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address		f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X	d. Photographs	X	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

--

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. (Check all that apply.)

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify)					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify): Cooperative observers.					

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	X	Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	X
Other (specify):			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
--	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.
----------	--------------------------------------------------------------------------------------

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify): Information on weather volunteers.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

There are local databases at the local WFO/RFC that maintain information on volunteers who provide weather reports to them. The databases hold contact information on these volunteers, in order to contact them when needed and as a record of who provides the information.

All of this information is voluntary and the Co-Op Observer has the right to opt-out of the program at any time. This information is entered into a NOAA database called the Cooperative Station Service Accountability (CSSA), located and maintained by NWS Office of Climate Weather and Water Services (OCWWS).

A locally assigned NWS staff person is responsible for entry of this information into the CSSA database. A limited amount of this data is retained in the local office for quick access to contact the Co-Op in case of equipment outages.

This information is collected from members of the public.

The Regional ISSO has been assigned the Trusted Agent (TA) duties for multiple contractors. All badging paperwork and OSY Security/Investigative coversheets for the contractors are being saved to the ISSO's system. All transmission of PII data flows to other organizational entities (OSY) via secured Acellion SFTP server. All PII data residing on the NOAA8884 system is encrypted at rest with the use of McAfee Endpoint Security protection. This is an encrypted Directory only assessable from the user with CAC authentication.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X*		
DOC bureaus	X*		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*In case of breach. For DOC bureaus, also for submission of CAC documents to OSY.

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	-----------------------------------------------

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input type="checkbox"/>	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors*	X		
Other (specify):			

*Contractors log in to review their information before the TA approves.

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and
---	------------------------------------------------------------------------------------------------------

	discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and privacy policy can be found at: http://www.nws.noaa.gov/om/coop/index.htm .	
X	Yes, notice is provided by other means.	Specify how: There are privacy act statements on the federal-wise forms used by the TA. Notice to volunteers is provided when information is collected,
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: All of this information is voluntary, as part of the cooperative agreement to work with the NWS on providing observations. The only means of providing the PII is by completing and signing the cooperative agreement form. Prospective contractors may decline, but their employment would be affected.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: The only use of the information is for contact purposes, which is given as part of the signed agreement. No other uses are suggested or specified. For the clearance, there is only one use for the information.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: The local manager visits each volunteer twice monthly to monitor equipment and answer questions. Updates can be made then, or emailed, as explained by the manager during orientation. Contractors can log into the TA system to review their information but cannot make changes.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. (Check all that apply.)

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Any access to the local Database is logged and saved. AD maintains logging of all access to file system
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>4/19/2017</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher. MODERATE
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

<p>Access to the system maintaining the PII is controlled by access via Active Directory and the use of CAC (PIV) cards. Only employees with authority to maintain this database are allowed access to the information.</p> <p>Trusted Agent data is located in an encrypted Folder located on the Regional HQ NAS device, under the user of the Regional ISSO. Can only be decrypted by use of CAC card using McAfee Files and Folders encryption for the ISO only.</p>

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (A new system of records notice (SORN) is required if the system is not covered by an existing SORN).

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN).
---	-----------------------------------------------------------------------------

	COMMERCE/NOAA-11 , Contact information for members of the public requesting or providing information related to NOAA’s mission; COMMERCE/DEPT-13 , Investigative and Security Records. COMMERCE/DEPT-25 , Access Control and Identity Management
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule: Chapter 1300- Weather, 1307-05
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	<input checked="" type="checkbox"/>	Overwriting	
Degaussing	<input checked="" type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input checked="" type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Individual's PII are in the system.
X	Quantity of PII	Provide explanation: Only name and contact information for volunteers, and names of employees, are in the system.
X	Data Field Sensitivity	Application data has many sensitive fields filled out.
X	Context of Use	Voluntary submission of PII for internal use only
	Obligation to Protect Confidentiality	
X	Access to and Location of PII	Secured local database managed by limited Federal employees
	Other:	Provide explanation:

Section 12: Analysis





12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

<p>System Owner or Information System Security Officer</p> <p>Name: John Duxbury Office: NWS/SR Phone: 682-703-3703 Email: john.duxbury@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p>  <p>DUXBURY.JOHN.C.1365877730 2018.01.17 11:58:34 -06'00'</p>	<p>Information Technology Security Officer</p> <p>Name: Andrew Browne Office: NOAA NWS Office of the CIO Phone: 301-427-9033 Email: beckie.koonge@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>BROWNE.ANDREW.PATRICK.1472149349</p>  <p>Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2018.01.22 15:39:20 -05'00'</p>
<p>Authorizing Official</p> <p>Name: Steven Cooper Office: NWS/SR Phone: 682-703-3700 Email: steven.cooper@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>COOPER.STEVEN.N.G.1365850930</p>  <p>Digitally signed by COOPER.STEVEN.N.G.1365850930 Date: 2018.01.22 14:11:48 -06'00'</p>	<p>Bureau Chief Privacy Officer</p> <p>Name: Mark Graff Office: NOAA Privacy Office Phone: 301-628-5658 Email: mark.graff@noaa.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>Signature: GRAFF.MARK.HYRUM.1514447892</p>  <p>Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.24 10:56:25 -05'00'</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

**U.S. Department of Commerce
NOAA**



**Privacy Threshold Analysis
for the
Southern Region GSS (NOAA8884)**

U.S. Department of Commerce Privacy Threshold Analysis

Southern Region GSS (NOAA8884)

Unique Project Identifier: 006-000351100 00-48-02-00-01-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

The National Weather Service (NWS) Southern Region provides weather, hydrologic, and climate forecasts and warnings for the United States, its territories, adjacent waters and ocean areas, for the protection of life and property and the enhancement of the national economy. NWS data and products form a national information database and infrastructure, which can be used by our partners, the public, and the global community. Issuance of products including forecasts and warning is dependent on a complex interaction of many information resources and systems. This system is designed and used to support the collection, processing, and dissemination of data that supports the mission of the origination. It also supports the administrative functions and the scientific & technical research and innovations activities of employees within the organization.

Although there are a variety of hardware and operating systems, all the activities are interconnected. The system provides direct or indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems; client-server and web-based server systems. The system supports a variety of users, functions, and applications; including word processing, financial data, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training, research and development and collaboration.

Questionnaire:

1. What is the status of this information system?

_____ This is a new information system. *Continue to answer questions and complete certification.*

This is an existing information system with changes that create new privacy risks.
 Complete chart below, continue to answer questions, and complete certification.

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): *NOAA8205 was incorporated into this collection.					

This is an existing information system in which changes do not create new privacy risks. Skip questions and complete certification.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. Please describe the activities which may raise privacy concerns.

The Regional ISSO has been assigned the Trusted Agent (TA) duties for multiple contractors. All badging paperwork and OSY Security/Investigative coversheets for the contractors are being saved to the ISSO’s system.
 All transmission of PII data flows to other organizational entities (OSY) via secured Acellion SFTP server.
 All PII data residing on the NOAA8884 system is encrypted at rest with the use of McAfee Endpoint Security protection. This is an encrypted Directory only assessable from the user with CAC authentication.

No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the submitter has a commercial interest” and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.).”

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: “The term ‘personally identifiable information’ refers to information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc...”

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is “yes” to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the Southern Region GSS (NOAA8884) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.


Name of Information System Security Officer (ISSO) or System Owner (SO):

John Duxbury (SO)

Signature of ISSO or SO:  DUXBURY.JOHN.C.1365877730
2018.01.18 07:50:53 06'00' Date: _____

Name of Information Technology Security Officer (ITSO):

Andrew Browne (ITSO)

Signature of ITSO: BROWNE.ANDREW.PA
TRICK.1472149349  Digitally signed by
BROWNE.ANDREW.PATRICK.1472149349
Date: 2018.01.22 15:38:35 -05'00' Date: _____

Name of Authorizing Official (AO):

Steven Cooper

Signature of AO: COOPER.STEVEN.G.136
5850930  Digitally signed by
COOPER.STEVEN.G.1365850930
Date: 2018.01.22 14:10:31 06'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1
514447892  Digitally signed by GRAFF MARK HYRUM 1514447892
DN c US, o U S Government, ou DoD, ou PKI,
ou OTHER, cn GRAFF MARK HYRUM 1514447892
Date 2018 01 24 10 52 07 05'00' Date: _____

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Wednesday, January 24, 2018 3:18 PM
To: Gioffre, Kathy (Federal); CPO
Cc: Mark Graff NOAA Federal
Subject: NOAA0500 certification documents minor changes to PIA detailed below
Attachments: NOAA0500 PIA_012418 for certification_012418.pdf; NOAA0500 PIA_Annual_Review_Certification_Form 14Dec17_ISSO Signed mhg.pdf; NOAA0500_PTA_Updated_14Dec17 LBH (2) mhg.pdf

Hi, Kathy on the PIA, in addition to updating the ATO date in Section 8.1, I added in the system description that employee PII would be shared in case of a breach.

In Section 4.1, I checked civil and criminal enforcement activities and also administrative matters. I also checked DOC Bureaus and Federal Agencies in 6.1, asterisking with breach explanation.

I added DEPT 13 to Section 9 to be consistent with those changes.

None of these is actually a change, but an update to reflect our recognition of the need to share in a breach, which we started including in PIAs several months ago.

thx Sarah

(the NOAA6101 certification is still in process, after a delay in LO level review)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

U.S. Department of Commerce
NOAA



Privacy Impact Assessment
for the
NOAA Research & Development High Performance Computing
System (R&D HPCS) – NOAA0500

Reviewed by: _____, Bureau Chief Privacy Officer
Mark Graff

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment NOAA Research & Development High Performance Computing System (R&D HPCS) – NOAA0500

Unique Project Identifier: NOAA0500

Introduction: System Description

NOAA0500 system provides research and development weather models in support of NOAA's operational mission. The R&D HPCS operates large scale, extreme computing environments that encompass multiple geographic sites, and heterogeneous supercomputing architectures. This system supports NOAA's mission by providing cutting edge technology for weather and climate model developers. These models eventually form the basis for NOAA's daily weather forecasts, storm warnings, and climate change forecasts. System users include scientists from multiple NOAA Line Offices, and their research collaborators, including some foreign nationals.

NOAA's R&D HPC system (R&D HPCS) provides four fundamental HPC functions:

1. Large scale computing provides computing for development, testing, and production integrations of NOAA environmental models. The workload that runs on this subsystem is characterized by computer intensive codes with I/O characterized by regular snapshots of diagnostic fields.
2. Analysis and interactive computing provides computing for the post processing of data from production runs and the analysis of post processed data, code development, and debugging. The workload that runs on this subsystem is characterized by data intensive codes requiring high I/O bandwidth.
3. Data archiving provides long term storage of post processed model runs and analyses.
4. Networking links these subsystems together.

The users of the system are primarily, but not exclusively, NOAA employees who represent the following offices:

1. NOAA/ESRL Global Systems Division, Boulder, Colorado
2. NOAA National Weather Service (NWS), National Centers for Environmental Prediction (NCEP), Environmental Modeling Center (EMC), Camp Springs, Maryland
3. NOAA Geophysical Fluid Dynamics Laboratory (GFDL), Princeton, New Jersey

These users access the system and submit weather or climate modeling application program runs via job scheduling software. These models contain parallelized code to take advantage of the large scale, highly parallelized environment offered by the HPCS. This is necessary to support the science. Modeling jobs can be extremely large (e.g., 1200 processors required), because they incorporate different local, regional, or global atmospheric and ocean models to create an ensemble model program. The scheduling software automatically identifies and collects the necessary processors to run the job, and controls its execution. Therefore, the user never has any direct interaction with the compute nodes of the system.

In accordance with applicable security controls, users of the R&D HPCS must first request an account prior to access approvals. Those users who would like an account must supply the requested/required data on a web-based form. Those requests and associated data supplied by the user are stored in a database and only accessible by authorized privileged account administrators. The user-supplied data is used only for identification and creation of unique accounts as well as for contact purposes if there should be a problem with the account. The user base consists of Federal employees, contractors, foreign nationals and casual collaborators.

Weather and climate data is collected from a variety of sources and fed into the system by the user community. All of this data is vetted by the NOAA scientific community through processes outside of this system, to guarantee its authenticity and integrity. Once entered into the R&D HPCS, the system security controls are designed to guarantee the integrity of this data.

The current configuration of the R&D HPCS is architected along organizational lines. Large scale computing, analysis computing, and storage, at the following locations, are within the boundaries of NOAA0500. The other functions at these locations are not within the NOAA0500 boundaries.

1. NOAA Earth System Research Laboratory (ESRL), David Skaggs Research Center (DSRC325 N. Broadway Street, Boulder, Colorado 80305,
2. NOAA Geophysical Fluid Dynamics Laboratory (GFDL), Princeton University Forrestal Campus, 201 Forrestal Road, Princeton, New Jersey 08450,
3. NOAA Environmental, Security Computing Center (NESCC), 1000 Galliher Drive, Fairmont, WV 26554.

The R&D HPCS has Interconnection Security Agreements with ORNL, N-Wave, NCEP, GFDL, and ESRL. These organizations provide general support and services such as LAN/WAN connectivity, authentication and identification controls, DNS, WEB and other IT infrastructure support.

The National Centers for Environmental Prediction (NCEP) utilize data acquired from commercial, other U.S Government and International sources to execute NCEP mission. A subset of this data, referred to as "restricted data" is made available to NCEP with restrictions on further dissemination.* As a direct or indirect party to the agreements governing the use of this Restricted Data, NCEP is charged with protecting restricted data during use and identifying restricted data to managers, users, staff and partners supporting NCEP mission.

Authority for collection of information: 5 U.S.C. 301 5 U.S.C. 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

*NOAA has agreements with ships and planes, which collect local weather data while at sea/in the air and share with NOAA. The data includes the positions of those ships and planes, because the two types of information cannot be separated. The location data is considered proprietary.

Information sharing: The PII in the system will not be shared outside of the bureau except in case of a breach. The BII (restricted data). NCEP receives and shares with RDHPC.

R&D HPCS FIPS 199 Impact Level: MODERATE

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- This is a new information system.
- This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

- This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (Check all that apply.)

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	

e. Age		k. Email Address		q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	
b. Job Title		e. Email Address	X	h. Work History	
c. Work Address		f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)					
WCOSS proprietary and restricted data (locations of ships and planes providing weather data).					

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	X
Telephone		Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify: NWS NCEP program owns the data and is responsible for its distribution.					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

- 2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

<input checked="" type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
-------------------------------------	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

- 3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

<input checked="" type="checkbox"/>	There are not any IT system supported activities which raise privacy risks/concerns.
-------------------------------------	--------------------------------------------------------------------------------------

Section 4: Purpose of the System

- 4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Archive and Storage only –no dissemination or processing within the R&D HPCS environment			

Section 5: Use of the Information

5.1 The National Centers for Environmental Prediction (NCEP) utilize data acquired from commercial, other U.S Government and International sources to execute NCEP mission. A subset of this data, referred to as “restricted data” is made available to NCEP with restrictions on further dissemination. As a direct or indirect party to the agreements governing the use of this Restricted Data, NCEP is charged with protecting restricted data during use and identifying restricted data to managers, users, staff and partners supporting NCEP mission.

NCEP Restricted Data Storage Locations

Restricted data can be found in the following locations:

- System networks [transitory]
- Long-term scratch file system in the path /tbd/tbd [transitory]
- Fast scratch file system in the path /tbd/tbd [stored]
- NCEP-Authorized user home file systems [stored]
- Backup media holding NCEP files [stored]

NCEP Restricted Data Protection

Restricted data stored is protected by setting each file containing restricted data as readable only by users in the RSTPROD group.

Authorized Users

NCEP explicitly grants access to restricted data to NCEP staff and associates whose work utilizes these data. This access is granted through each system’s account approval process.

Privileged Users

Privileged users include staff that supports the systems, storage, and networks utilized to accomplish NCEP work. Privileged access includes access to a systems administrator or root account on a system, privileged access to network devices, and other than general user access to system storage devices, including data archiving or backup equipment. A privileged user has access to restricted data as a result of their privileged access to these systems.

Limitations on Privileged Users

Privileged users are notified that any of the following actions may be taken only with NCEP Management and Site Manager approval:

- Copying or moving restricted data to a location not identified as an NCEP Restricted Data Storage Location
- Making restricted data available by any means to a user that is not identified by NCEP Management as authorized to access restricted data
- Making restricted data available by any means to the public such as through an internet-connected server or public portal

In accordance with applicable security controls, users of the R&D HPCS must first request an account prior to access approvals. Those users who would like an account must supply the requested/required data on a web-based form. Those requests and associated data supplied by the user are stored in a database and only accessible by authorized privileged account administrators. The user-supplied data is used only for identification and creation of unique accounts as well as for contact purposes if there should be a problem with the account. The user base consists of Federal employees, contractors, foreign nationals and casual collaborators.

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X*		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*In case of breach

	The PII/BII in the system will not be shared.
--	-----------------------------------------------

- 6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NCEP. AC-1, 3, 4, 5, 6, 14, 21, 22; AU-2, 6; IA-4, 5, 8; and SC-4, 7, 8
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

- 6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

- 7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
---	------------------------------------------------------------------------------------------------------------------------------

X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The <u>Privacy Act statement</u> and/or privacy policy can be found at: NCEP: (located above Clear Form button) http://www.nco.ncep.noaa.gov/sib/restricted_data/restricted_data_sib/register/ and R&D HPCS AIM: (located at bottom right / top line) https://aim.rdhpcs.noaa.gov/	
X	Yes, notice is provided by other means.	Specify how: Notification and use is provided by NCEP on their rstprod web site: http://www.nco.ncep.noaa.gov/sib/restricted_data/restricted_data_sib/ Proprietary data is shared through NCEP agreements.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Proprietary data collected is provided through organizations with which NCEP has agreements for the use and dissemination of the data etc. Account users may decline to provide PII, by not providing it, but this will affect their ability to establish an account.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Proprietary data is provided through agreements, for research purposes as agreed on. Account users: By providing information to establish an account, the user consents to its uses – access to the data and trouble-shooting any problems with the account.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

x	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Account users may update their information at any time, and we ask them to update at least annually, using instructions on the Web site. This is NA for the proprietary data.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Users who would like an account must supply the requested/required data on a web-based form. Those requests and associated data supplied by the user are stored in a database and only accessible by authorized privileged account administrators. The user-supplied data is used only for identification and creation of unique accounts as well as for contact purposes if there should be a problem with the account.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>3/15/2017</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

The WCCOS data stored within the R&D HPCS and is only accessible to NCEP, which approves and provides access. Network accessibility to the storage and archive system is via internal connection (private circuits) and does not traverse the internet. Both NCEP and R&D HPCS users are required to login utilizing either 2-factor authentication and or CAC authentication.

R&D HPCS has 24hr network and system monitoring and security logs weekly for suspicious activities, attempted logins etc. Data residing within the R&D HPCS system boundary remains within a data center which is also monitored 24x7, has CCTV, and armed guards. Access to the data center where the Storage and Archive resides is accessible via CAC/Badge reader to authorized and vetted NOAA personnel and contractors. Maintenance, and other personnel not previously vetted by NOAA are escorted and observed at all times within the data center.

In accordance with applicable security controls, users of the R&D HPCS must first request an account prior to access approvals. Those users who would like an account must supply the requested/required data on a web-based form. Those requests and associated data supplied by the user are stored in a database and only accessible by authorized privileged account administrators. The user-supplied data is used only for identification and creation of unique accounts as well as for contact purposes if there should be a problem with the account. The user base consists of Federal employees, contractors, foreign nationals and casual collaborators.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i> : DEPT-18, Employees Personnel Files not Covered by other Notices; COMMERCE/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA’s Mission. DEPT-13, Investigative and Security Files.
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA 1200-02, Research Notebooks and NOAA1200-6, Data Requests.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:

X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. (*Check all that apply.*)

Disposal			
Shredding		Overwriting	
Degaussing	X	Deleting	
Other (specify): The referenced data has a very long/perpetual life. Storage media that has potentially been used for this referenced data is degaussed once retired and prior to being removed from the system boundary.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. (*Check all that apply.*)

X	Identifiability	Provide explanation: An individual may be identified from information in the accounts database.
x	Quantity of PII	Provide explanation: The only PII is account contact information,
X	Data Field Sensitivity	Provide explanation: There is no sensitive PII.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: AC-1, 3, 4, 5, 6, 14, 21, 22; AU-2, 6; IA-4, 5, 8; and SC-4, 7, 8
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: Addition of a Privacy Act Statement on account page
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: Addition of a Privacy Act Statement on account page
	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

<p>Information System Security Officer or System Owner Name: Justin May (ISSO) Office: NOAA/OCIO Phone: (303) 437-8155 Email: justin.may@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: right;">Digitally signed by MAY.JUSTIN.NATHANIEL.1039635980 Date: 2018.01.17 18:08:24 -07'00'</p> <p>Signature: MAY.JUSTIN.NATHANIEL.1039635980</p> <p>Date signed:</p>	<p>Information Technology Security Officer Name: Jean Apedo Office: NOAA/OCIO Phone: (301) 628-5730 Email: jean.apedo@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: right;">Digitally signed by APEDO.JEAN.1188076064 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn APEDO.JEAN.1188076064 Date: 2018.01.18 06:23:46 -05'00'</p> <p>Signature: APEDO.JEAN.1188076064</p> <p>Date signed: .1188076064</p>
<p>Authorizing Official Name: Zachary Goldstein Office: NOAA/OCIO Phone: (301) 713-9600 Email: zachary.goldstein@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: right;">Digitally signed by GOLDSTEIN.ZACHARY.G.1228698985 Date: 2018.01.23 09:27:19 -05'00'</p> <p>Signature: GOLDSTEIN.ZACHARY.G.1228698985</p> <p>Date signed:</p>	<p>Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p style="text-align: right;">Digitally signed by GRAFF.MARK.HYRUM.151447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.151447892 Date: 2018.01.24 09:25:46 -05'00'</p> <p>Signature: GRAFF.MARK.HYRUM.151447892</p> <p>Date signed: 47892</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NOAA Research & Development High Performance Computing System (R&D HPCS)

FISMA Name/ID (if different): R&D HPCS - NOAA0500

Name of IT System/ Program Owner: Frank Indiviglio

Name of Information System Security Officer: Justin May

Name of Authorizing Official(s): Zachary Goldstein

Date of Last PIA Compliance Review Board (CRB): 14 Mar 17

(This date must be within three (3) years.)

Date of PIA Review: 14 Dec 17

Name of Reviewer: Justin May

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer (SO or ISSO): MAY.JUSTIN.NATHANIEL.1039635980

Digitally signed by MAY JUSTIN NATHANIEL 1039635980
DN: cn=MAY JUSTIN NATHANIEL 1039635980, c=US, o=U.S. Government,
ou=CONTRACTOR
Reason: I am the author of this document
Date: 2017.12.14 22:29:20 -07'00'

Date of BCPO Review: 1/24/18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: 7892

GRAFF.MARK.HYRUM.151444
Digitally signed by GRAFF MARK HYRUM 1514447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=OTHER, cn=GRAFF MARK HYRUM 1514447892
Date: 2018.01.24 09:18:14 -05'00'

U.S. Department of Commerce
NOAA



Privacy Threshold Analysis
For the
NOAA Research & Development High Performance Computing
System (R&D HPCS) – NOAA0500

U.S. Department of Commerce Privacy Threshold Analysis

NOAA Research and Development High Performance Computer

Unique Project Identifier: NOAA0500

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: NOAA0500 system is a considered to be a General Support System which provides research and development weather models in support of NOAA's operational mission. The R&D HPCS operates large scale, extreme computing environments that encompass multiple geographic sites, and heterogeneous supercomputing architectures. This system supports NOAA's mission by providing cutting edge technology for weather and climate model developers. These models eventually form the basis for NOAA's daily weather forecasts, storm warnings, and climate change forecasts. System users include scientists from multiple NOAA Line Offices, and their research collaborators, including some foreign nationals.

NOAA's R&D HPC system (R&D HPCS) provides four fundamental HPC functions:

1. Large scale computing provides computing for development, testing, and production integrations of NOAA environmental models. The workload that runs on this subsystem is characterized by compute intensive codes with I/O characterized by regular snapshots of diagnostic fields.
2. Analysis and interactive computing provides computing for the post processing of data from production runs and the analysis of post processed data, code development, and debugging. The workload that runs on this subsystem is characterized by data intensive codes requiring high I/O bandwidth.
3. Data archiving provides long term storage of post processed model runs and analyses.
4. Networking links these subsystems together.

The users of the system are primarily, but not exclusively, NOAA employees who represent the following offices:

1. NOAA/ESRL Global Systems Division, Boulder, Colorado
2. NOAA National Weather Service (NWS), National Centers for Environmental Prediction (NCEP), Environmental Modeling Center (EMC), Camp Springs, Maryland
3. NOAA Geophysical Fluid Dynamics Laboratory (GFDL), Princeton, New Jersey

These users access the system and submit weather or climate modeling application program runs via job scheduling software. These models contain parallelized code to take advantage of the

large scale, highly parallelized environment offered by the HPCS. This is necessary to support the science. Modeling jobs can be extremely large (e.g., 1200 processors required), because they incorporate different local, regional, or global atmospheric and ocean models to create an ensemble model program. The scheduling software automatically identifies and collects the necessary processors to run the job, and controls its execution. Therefore, the user never has any direct interaction with the compute nodes of the system.

Weather and climate data is collected from a variety of sources and fed into the system by the user community. All of this data is vetted by the NOAA scientific community through processes outside of this system, to guarantee its authenticity and integrity. Once entered into the R&D HPCS, the system security controls are designed to guarantee the integrity of this data.

The current configuration of the R&D HPCS is architected along organizational lines. Large scale computing, analysis computing, and storage are located at the following locations:

1. NOAA Earth System Research Laboratory (ESRL), David Skaggs Research Center (DSRC325 N. Broadway Street, Boulder, Colorado 80305,
2. NOAA Geophysical Fluid Dynamics Laboratory (GFDL), Princeton University Forrestal Campus, 201 Forrestal Road, Princeton, New Jersey 08450,
3. NOAA Environmental, Security Computing Center (NESCC), 1000 Galliher Drive, Fairmont, WV 26554,
4. NOAA Center for Weather and Climate Predication (NCWCP), 5830 University Research Court, College Park, MD 20740.

The R&D HPCS system boundary encompasses these locations. Interconnection Security Agreements with ORNL, N-Wave, NCEP, GFDL, and ESRL provide general support and services such a LAN/WAN connectivity, authentication and identification controls, DNS, WEB and other IT infrastructure support.

Questionnaire:

1. What is the status of this information system?

- This is a new information system. *(Continue to answer questions and complete certification.)*
- This is an existing information system with changes that create new privacy risks. *(Complete chart below, continue to answer questions, and complete certification)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

- This is an existing information system in which changes do not create new privacy risks. *(Skip questions and complete certification)*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

- Yes. *(Please describe the activities which may raise privacy concerns.)*

- No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

- Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

- Companies
- Other business entities

- No, this IT system does not collect any BII.

4. Personally Identifiable Information

4.a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

- Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- DOC employees
- Contractors working on behalf of DOC
- Members of the public

- No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

- Yes, the IT system collects, maintains, or disseminates PII other than user ID.

- No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

- Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.
- No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

I certify the criteria implied by one or more of the questions above **apply** to the NOAA0500 IS and as a consequence of this applicability, I will perform and document a PIA for this IT system.

I certify the criteria implied by the questions above **do not apply** to the NOAA0500 IS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Frank Indiviglio

Signature of ISSO or SO: 0787 HART.LESLIE.B.136587 Digitally signed by HART.LESLIE.B.1365870787 Date: 2018.01.16 11:09:13 -07'00' Date: _____

Leslie Hart (acting for Frank Indiviglio)

Name of Information Technology Security Officer (ITSO): Jean Apedo

Signature of ITSO: .1188076064 APEDO.JEAN.1188076064 Digitally signed by APEDO.JEAN.1188076064 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn APEDO.JEAN.1188076064 Date: 2018.01.17 06:32:12 -05'00' Date: _____

Name of Authorizing Official (AO): Zachary Goldstein

Signature of AO: GOLDSTEIN.ZACHARY.G.1228698985 GOLDSTEIN.ZACHARY.G.1228698985 Digitally signed by GOLDSTEIN.ZACHARY.G.1228698985 Date: 2018.01.23 09:24:25 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.24 09:19:48 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Thursday, January 25, 2018 1:31 PM
To: Tommy Thompson; John Soule NOAA Affiliate
Cc: Mark Graff NOAA Federal
Subject: Re: Minutes from the NOAA8850 CRB
Attachments: PIA Template 01 2017.docx; PTA Template 01 2017.docx

Also, here are the new PIA and PTA templates. We would have gotten by with the old ones, since this was started a while ago, but now that we have do a major revision . .

In the new PIA template (and in the PTA template), the system description is itemized; most of this was in the previous template of the PIA, but please ensure that all areas are addressed.

There are three new questions: 2.3, 2.4 (for this one the answer is NO) and 5.2 (this one would be a subset of what you now have in 8.2)

But please answer the questions I sent earlier before you dive into this. I do need the backbone wording for NOAA1200 as its CRB is scheduled for February 8.

thx again, Sarah

On Thu, Jan 25, 2018 at 1:11 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
Tommy and John, please see the attached, items 3, 4 and 6.

Should we check the financial info in Section 2.1

Other than the answer to 6.2, do we need any text to explain TA vs NOAA8850?

And please send language to describe that NOAA1200 uses NOAA8850 as the backbone for transmission (6.2).

I wish we could have avoided the confusion this am.

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751

Ce (b)(6)

U.S. Department of Commerce
[Bureau Name]



Privacy Impact Assessment
for the
[IT System Name]

Reviewed by: _____, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment
[Name of Bureau/Name of IT System]

Unique Project Identifier: [Number]

Introduction: System Description

*Provide a description of the system that addresses the following elements:
 The response must be written in plain language and be as comprehensive as necessary to describe the system.*

- (a) Whether it is a general support system, major application, or other type of system*
- (b) System location*
- (c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
- (d) The way the system operates to achieve the purpose(s) identified in Section 4*
- (e) How information in the system is retrieved by the user*
- (f) How information is transmitted to and from the system*
- (g) Any information sharing conducted by the system*
- (h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*
- (i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system*

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- _____ This is a new information system.
- _____ This is an existing information system with changes that create new privacy risks.
 (Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify):			

_____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

- 2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (*Check all that apply.*)

Identifying Numbers (IN)			
a. Social Security*		e. File/Case ID	i. Credit Card
b. Taxpayer ID		f. Driver's License	j. Financial Account
c. Employer ID		g. Passport	k. Financial Transaction
d. Employee ID		h. Alien Registration	l. Vehicle Identifier
m. Other identifying numbers (specify):			
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:			

General Personal Data (GPD)			
a. Name		g. Date of Birth	m. Religion
b. Maiden Name		h. Place of Birth	n. Financial Information
c. Alias		i. Home Address	o. Medical Information
d. Gender		j. Telephone Number	p. Military Service
e. Age		k. Email Address	q. Physical Characteristics
f. Race/Ethnicity		l. Education	r. Mother's Maiden Name
s. Other general personal data (specify):			

Work-Related Data (WRD)			
a. Occupation		d. Telephone Number	g. Salary
b. Job Title		e. Email Address	h. Work History
c. Work Address		f. Business Associates	
i. Other work-related data (specify):			

Distinguishing Features/Biometrics (DFB)			
a. Fingerprints		d. Photographs	g. DNA Profiles
b. Palm Prints		e. Scars, Marks, Tattoos	h. Retina/Iris Scans
c. Voice Recording/Signatures		f. Vascular Scan	i. Dental Profile
j. Other distinguishing features/biometrics (specify):			

System Administration/Audit Data (SAAD)			
a. User ID		c. Date/Time of Access	e. ID Files Accessed
b. IP Address		d. Queries Run	f. Contents of Files
g. Other system administration/audit data (specify):			

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		<input type="checkbox"/>
Other (specify):					

Government Sources					
Within the Bureau	<input type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		<input type="checkbox"/>
Other (specify):					

Non-government Sources					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input type="checkbox"/>		<input type="checkbox"/>
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

<input type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
--------------------------	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

<input type="checkbox"/>	There are not any IT system supported activities which raise privacy risks/concerns.
--------------------------	--------------------------------------------------------------------------------------

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated

will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

- 5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	-----------------------------------------------

- 6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input type="checkbox"/>	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
<input type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

- 6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input type="checkbox"/>		<input type="checkbox"/>
Other (specify):			

Section 7: Notice and Consent

- 7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

<input type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
<input type="checkbox"/>	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement

	and/or privacy policy can be found at:	.
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a

	moderate or higher.
	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i>
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

	There is an approved record control schedule. Provide the name of the record control schedule:
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	<input type="checkbox"/>	Overwriting	<input type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input type="checkbox"/>
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

	Identifiability	Provide explanation:
	Quantity of PII	Provide explanation:
	Data Field Sensitivity	Provide explanation:
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:

	Other:	Provide explanation:
--	--------	----------------------

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

--	--

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

<p>Information System Security Officer or System Owner</p> <p>Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>Date signed:</p>	<p>Information Technology Security Officer</p> <p>Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>Date signed:</p>
<p>Authorizing Official</p> <p>Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>Date signed:</p>	<p>Bureau Chief Privacy Officer</p> <p>Name: Office: Phone: Email:</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>Signature:</p> <p>Date signed:</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

U.S. Department of Commerce
[Bureau Name]



Privacy Threshold Analysis
for the
[IT System Name]

U.S. Department of Commerce Privacy Threshold Analysis

[Name of Bureau/Name of IT System]

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

- a) *Whether it is a general support system, major application, or other type of system*
- b) *System location*
- c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
- d) *The purpose that the system is designed to serve*
- e) *The way the system operates to achieve the purpose*
- f) *A general description of the type of information collected, maintained, use, or disseminated by the system*
- g) *Identify individuals who have access to information on the system*
- h) *How information in the system is retrieved by the user*
- i) *How information is transmitted to and from the system*

Questionnaire:

1. What is the status of this information system?

_____ This is a new information system. *Continue to answer questions and complete certification.*

_____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify):			

_____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

_____ Yes. *Please describe the activities which may raise privacy concerns.*

_____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the submitter has a commercial interest” and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)”

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

- Companies
- Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- DOC employees
- Contractors working on behalf of DOC
- Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

_____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

_____ I certify the criteria implied by one or more of the questions above **apply** to the [IT SYSTEM NAME] and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Signature of ISSO or SO: _____ Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: _____ Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: _____ Date: _____

Name of Bureau Chief Privacy Officer (BCPO): _____

Signature of BCPO: _____ Date: _____

Gioffre, Kathy (Federal)

From: Gioffre, Kathy (Federal)
Sent: Thursday, January 25, 2018 12:13 PM
To: Graff, Mark (Federal); Brabson, Sarah (Federal)
Cc: CPO; Ferguson, Dorrie (Federal); Toland, Michael (Federal); Gitelman, Steve (Contractor)
Subject: NOAA8850 NWS Enterprise Mission Enabling System CRB Minutes
Attachments: NOAA 8850 Minutes (20180125)Final.docx; PIA Template 01 2017.docx; PTA Template 01 2017.docx; PIA Annual Review Certification Form with PA Officer (20171101).docx

Good afternoon,

Attached are the CRB minutes for the NOAA8850 NWS Enterprise Mission Enabling System.

Also attached are the revised PIA, PTA and Certification forms in Word Format.

Kathy

Privacy Impact Assessment (PIA) Compliance Review Board (CRB) Meeting Minutes
NOAA NWS Enterprise Mission Enabling System (EMES; NOAA8850)
January 25, 2018

Attendees:

Privacy Team

Catrina Purvis
Kathy Gioffre
Steve Gitelman

NOAA

Sarah Brabson
Mark Graff
John Soule
Andrew Browne
Tommy Thompson

OCIO

Eunice Golloh
Maria Dumas
Eric Cline

Results/Conclusion:

Upon review of NOAA NWS Enterprise Mission Enabling System (EMES; NOAA8850), SAOP concurrence for ATO renewal was withheld pending further action and SORN clarification. However, OCIO granted concurrence for the renewal of the ATO based upon a review of system controls.

(b) (5)

(b) (5)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: _____

FISMA Name/ID (if different):

Name of IT System/ Program Owner:

Name of Information System Security Officer: _____

Name of Authorizing Official(s): _____

Date of Last PIA Compliance Review Board (CRB): _____
(This date must be within three (3) years.)

Date of PIA Review: _____

Name of Reviewer: _____

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: _____

Date of Privacy Act (PA) Review: _____

Name of Reviewer: _____

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: _____

Date of BCPO Review: _____

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): _____

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer:

U.S. Department of Commerce
[Bureau Name]



Privacy Impact Assessment
for the
[IT System Name]

Reviewed by: _____, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment
[Name of Bureau/Name of IT System]

Unique Project Identifier: [Number]

Introduction: System Description

*Provide a description of the system that addresses the following elements:
 The response must be written in plain language and be as comprehensive as necessary to describe the system.*

- (a) Whether it is a general support system, major application, or other type of system*
- (b) System location*
- (c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
- (d) The way the system operates to achieve the purpose(s) identified in Section 4*
- (e) How information in the system is retrieved by the user*
- (f) How information is transmitted to and from the system*
- (g) Any information sharing conducted by the system*
- (h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*
- (i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system*

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- _____ This is a new information system.
- _____ This is an existing information system with changes that create new privacy risks.
 (Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify):			

- _____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

- 2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)			
a. Social Security*		e. File/Case ID	i. Credit Card
b. Taxpayer ID		f. Driver's License	j. Financial Account
c. Employer ID		g. Passport	k. Financial Transaction
d. Employee ID		h. Alien Registration	l. Vehicle Identifier
m. Other identifying numbers (specify):			
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:			

General Personal Data (GPD)			
a. Name		g. Date of Birth	m. Religion
b. Maiden Name		h. Place of Birth	n. Financial Information
c. Alias		i. Home Address	o. Medical Information
d. Gender		j. Telephone Number	p. Military Service
e. Age		k. Email Address	q. Physical Characteristics
f. Race/Ethnicity		l. Education	r. Mother's Maiden Name
s. Other general personal data (specify):			

Work-Related Data (WRD)			
a. Occupation		d. Telephone Number	g. Salary
b. Job Title		e. Email Address	h. Work History
c. Work Address		f. Business Associates	
i. Other work-related data (specify):			

Distinguishing Features/Biometrics (DFB)			
a. Fingerprints		d. Photographs	g. DNA Profiles
b. Palm Prints		e. Scars, Marks, Tattoos	h. Retina/Iris Scans
c. Voice Recording/Signatures		f. Vascular Scan	i. Dental Profile
j. Other distinguishing features/biometrics (specify):			

System Administration/Audit Data (SAAD)			
a. User ID		c. Date/Time of Access	e. ID Files Accessed
b. IP Address		d. Queries Run	f. Contents of Files
g. Other system administration/audit data (specify):			

Other Information (specify)			

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		<input type="checkbox"/>
Other (specify):					

Government Sources					
Within the Bureau	<input type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		<input type="checkbox"/>
Other (specify):					

Non-government Sources					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input type="checkbox"/>		<input type="checkbox"/>
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

<input type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
--------------------------	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

<input type="checkbox"/>	There are not any IT system supported activities which raise privacy risks/concerns.
--------------------------	--------------------------------------------------------------------------------------

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated

will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

- 5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	-----------------------------------------------

- 6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input type="checkbox"/>	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
<input type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

- 6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input type="checkbox"/>		<input type="checkbox"/>
Other (specify):			

Section 7: Notice and Consent

- 7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

<input type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
<input type="checkbox"/>	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement

	and/or privacy policy can be found at:	.
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a

	moderate or higher.
	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i>
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

	There is an approved record control schedule. Provide the name of the record control schedule:
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	<input type="checkbox"/>	Overwriting	<input type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input type="checkbox"/>
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

	Identifiability	Provide explanation:
	Quantity of PII	Provide explanation:
	Data Field Sensitivity	Provide explanation:
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:

	Other:	Provide explanation:
--	--------	----------------------

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

--	--

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

<p>Information System Security Officer or System Owner</p> <p>Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>Date signed:</p>	<p>Information Technology Security Officer</p> <p>Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>Date signed:</p>
<p>Authorizing Official</p> <p>Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>Date signed:</p>	<p>Bureau Chief Privacy Officer</p> <p>Name: Office: Phone: Email:</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>Signature:</p> <p>Date signed:</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

U.S. Department of Commerce
[Bureau Name]



Privacy Threshold Analysis
for the
[IT System Name]

U.S. Department of Commerce Privacy Threshold Analysis

[Name of Bureau/Name of IT System]

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

- a) *Whether it is a general support system, major application, or other type of system*
- b) *System location*
- c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
- d) *The purpose that the system is designed to serve*
- e) *The way the system operates to achieve the purpose*
- f) *A general description of the type of information collected, maintained, use, or disseminated by the system*
- g) *Identify individuals who have access to information on the system*
- h) *How information in the system is retrieved by the user*
- i) *How information is transmitted to and from the system*

Questionnaire:

1. What is the status of this information system?

_____ This is a new information system. *Continue to answer questions and complete certification.*

_____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify):			

_____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

_____ Yes. *Please describe the activities which may raise privacy concerns.*

_____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the submitter has a commercial interest” and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)”

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

- Companies
- Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- DOC employees
- Contractors working on behalf of DOC
- Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

_____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

_____ I certify the criteria implied by one or more of the questions above **apply** to the [IT SYSTEM NAME] and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Signature of ISSO or SO: _____ Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: _____ Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: _____ Date: _____

Name of Bureau Chief Privacy Officer (BCPO): _____

Signature of BCPO: _____ Date: _____

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Thursday, January 25, 2018 2:32 PM
To: Nancy Defrancesco; Beckie Koonge NOAA Federal; Andrew Browne NOAA Affiliate; Amores, Catherine (Federal); Tahir Ismail; _NMFS InfoSec; John D. Parker; James Jones NOAA Affiliate
Cc: Mark Graff NOAA Federal
Subject: Announcement of new DOC PIA and PTA templates
Attachments: PTA Template 01 2017.docx; PIA_Template 2017.pdf

New DOC PIA and PTA templates are attached, and also posted on the NOAA Privacy Page: http://www.cio.noaa.gov/services_programs/privacy.html.

The changes: there are a few more items included in both the PIA and PTA system descriptions (d, e and f), and there are three new questions in the PIA:

2.3: Describe how the accuracy of the information in the system is ensured.

2.4: Is the information covered by the Paperwork Reduction Act? (in most cases, other than Fisheries, this will be no, but please consult with me, as the PRA Clearance Officer, to make sure).

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately.

I have not yet updated the PIA guidance posted on the privacy page, but these questions should be fairly self-explanatory in the meantime.

Please let your ISSOs know of these new templates at your next regular meeting. I am letting each know as we prepare for the next PTA or PIA.

Sarah D. Brabson
IT Infrastructure Investment Program Manager

PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751

Ce (b)(6)

U.S. Department of Commerce
[Bureau Name]



Privacy Impact Assessment
for the
[IT System Name]

Reviewed by: _____, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment
[Name of Bureau/Name of IT System]

Unique Project Identifier: [Number]

Introduction: System Description

*Provide a description of the system that addresses the following elements:
 The response must be written in plain language and be as comprehensive as necessary to describe the system.*

- (a) Whether it is a general support system, major application, or other type of system*
- (b) System location*
- (c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
- (d) The way the system operates to achieve the purpose(s) identified in Section 4*
- (e) How information in the system is retrieved by the user*
- (f) How information is transmitted to and from the system*
- (g) Any information sharing conducted by the system*
- (h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*
- (i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system*

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- _____ This is a new information system.
- _____ This is an existing information system with changes that create new privacy risks.
 (Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify):			

- _____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

- 2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (*Check all that apply.*)

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name		g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	
e. Age		k. Email Address		q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number		g. Salary	
b. Job Title		e. Email Address		h. Work History	
c. Work Address		f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)					

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		<input type="checkbox"/>
Other (specify):					

Government Sources					
Within the Bureau	<input type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		<input type="checkbox"/>
Other (specify):					

Non-government Sources					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input type="checkbox"/>		<input type="checkbox"/>
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
	No, the information is not covered by the Paperwork Reduction Act.

- 2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

<input type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
--------------------------	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

- 3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

<input type="checkbox"/>	There are not any IT system supported activities which raise privacy risks/concerns.
--------------------------	--------------------------------------------------------------------------------------

Section 4: Purpose of the System

- 4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated

will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

- 5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	-----------------------------------------------

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input type="checkbox"/>	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
<input type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input type="checkbox"/>		<input type="checkbox"/>
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

<input type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
<input type="checkbox"/>	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement

	and/or privacy policy can be found at:	.
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a

	moderate or higher.
	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i>
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

	There is an approved record control schedule. Provide the name of the record control schedule:
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	<input type="checkbox"/>	Overwriting	<input type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input type="checkbox"/>
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

	Identifiability	Provide explanation:
	Quantity of PII	Provide explanation:
	Data Field Sensitivity	Provide explanation:
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:

	Other:	Provide explanation:
--	--------	----------------------

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

<p>Information System Security Officer or System Owner</p> <p>Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>Date signed:</p>	<p>Information Technology Security Officer</p> <p>Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>Date signed:</p>
<p>Authorizing Official</p> <p>Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>Date signed:</p>	<p>Bureau Chief Privacy Officer</p> <p>Name: Office: Phone: Email:</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>Signature:</p> <p>Date signed:</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

U.S. Department of Commerce
[Bureau Name]



Privacy Threshold Analysis
for the
[IT System Name]

U.S. Department of Commerce Privacy Threshold Analysis

[Name of Bureau/Name of IT System]

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

- a) *Whether it is a general support system, major application, or other type of system*
- b) *System location*
- c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
- d) *The purpose that the system is designed to serve*
- e) *The way the system operates to achieve the purpose*
- f) *A general description of the type of information collected, maintained, use, or disseminated by the system*
- g) *Identify individuals who have access to information on the system*
- h) *How information in the system is retrieved by the user*
- i) *How information is transmitted to and from the system*

Questionnaire:

1. What is the status of this information system?

_____ This is a new information system. *Continue to answer questions and complete certification.*

_____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify):			

_____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

_____ Yes. *Please describe the activities which may raise privacy concerns.*

_____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the submitter has a commercial interest” and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)”

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

- Companies
- Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- DOC employees
- Contractors working on behalf of DOC
- Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

_____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

_____ I certify the criteria implied by one or more of the questions above **apply** to the [IT SYSTEM NAME] and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Signature of ISSO or SO: _____ Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: _____ Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: _____ Date: _____

Name of Bureau Chief Privacy Officer (BCPO): _____

Signature of BCPO: _____ Date: _____

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Thursday, January 25, 2018 5:01 PM
To: Mark Graff NOAA Federal
Subject: NOAA6101 certification docs for signature
Attachments: NOAA6101_PIA_1102018 LaVoi Signed.pdf; NOAA6101 PTA 2018.pdf; NOAA6101 certification for MHG signature.pdf

Here you go, I think no corrections needed.

The SAR is in the PIA folder. But I just sent you a message from Chuck Baxley.

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751

Ce (b)(6)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NOAA6101_PIA

FISMA Name/ID (if different): NOAA6101

Name of IT System/ Program Owner: NOS Office for Coastal Management (OCM)

Name of Information System Security Officer: Chuck Baxley

Name of Authorizing Official(s): Jeffrey L. Payne

Date of Last PIA Compliance Review Board (CRB): 2-6-2017

(This date must be within three (3) years.)

Date of PIA Review: 1/10/2017

Name of Reviewer: Chuck Baxley

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BAXLEY.CHARLES.A.III.1058676264 Digitally signed by BAXLEY.CHARLES.A.III.1058676264
Date: 2018.01.10 10:39:53 -05'00'

Date of Privacy Act (PA) Review: _____

Name of Reviewer: _____

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: _____

Date of BCPO Review: _____

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): _____

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: _____

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Mark Graff - NOAA Federal

From: Mark Graff NOAA Federal
Sent: Thursday, January 25, 2018 5:26 PM
To: Sarah Brabson NOAA Federal
Subject: Re: NOAA6101 certification docs for signature
Attachments: NOAA6101 PTA 2018 mhg.pdf; NOAA6101_PIA_1102018 LaVoi Signed mhg.pdf; NOAA6101 certification for MHG signature mhg.pdf

Here are the docs signed just contingent on Chuck confirming the issues with the 14 low Privacy Control POA&Ms. If you could just wait on sending to DOC until he confirms.

Thanks

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Thu, Jan 25, 2018 at 5:00 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
Here you go, I think no corrections needed.

The SAR is in the PIA folder. But I just sent you a message from Chuck Baxley.

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NOAA6101_PIA

FISMA Name/ID (if different): NOAA6101

Name of IT System/ Program Owner: NOS Office for Coastal Management (OCM)

Name of Information System Security Officer: Chuck Baxley

Name of Authorizing Official(s): Jeffrey L. Payne

Date of Last PIA Compliance Review Board (CRB): 2-6-2017
(This date must be within three (3) years.)

Date of PIA Review: 1/10/2017

Name of Reviewer: Chuck Baxley

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BAXLEY.CHARLES.A.III.1058676264 Digitally signed by BAXLEY.CHARLES.A.III.1058676264
Date: 2018.01.10 10:39:53 -05'00'

Date of Privacy Act (PA) Review: _____

Name of Reviewer: _____

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: _____

Date of BCPO Review: 1/25/18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF MARK HYRUM 1514447892
DN c US, o U S Government, ou DoD, ou PKI,
ou OTHER, cn GRAFF MARK HYRUM 1514447892
Date 2018 01 25 17 21 18 -05'00'

U.S. Department of Commerce
[Bureau Name]



Privacy Threshold Analysis
for
NOAA6101

U.S. Department of Commerce Privacy Threshold Analysis

NOAA6101

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

System NOAA6101 is a general support system used to ensure that the Office for Coastal Management's (OCM's) scientific and internal administrative I operational needs are met. The system is an integrated collection of subsystems designed to provide general office automation, infrastructure, and connectivity services to the National Oceanic and Atmospheric Administration's (NOAA) Office for Coastal Management (OCM) located in Charleston, SC, Silver Spring, MD, Honolulu, HI, Stennis Space Center, MS, additional OCM field offices, and remote staff. The system enables OCM to achieve its mission, which is to support the environmental, social, and economic well-being of the coast by linking people, information, and technology. OCM assists the nation's coastal resource Management community by providing access to information, technology, and training, and by producing new tools and approaches that often can be applied nationwide.

Two of the component subsystems are the file servers and Web Application Subsystem (WAS). While the file servers store and serve up administrative and operational data, the WAS hosts and serves data-driven Web-based applications. Applications served from an internal Web server are accessible only to NOAA employees and contractors operating from within the NOAA network. These internal applications track information related to OCM's operations I administration. Applications served from public-facing Web servers may be intended for OCM and other subsets of OCM, NOAA, other federal agencies, customers, partners, and/or the public.

Questionnaire:

1. What is the status of this information system?

This is a new information system. *Continue to answer questions and complete certification.*

This is an existing information system with changes that create new privacy risks.
Complete chart below, continue to answer questions, and complete certification.

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify):			

This is an existing information system in which changes do not create new privacy risks. *Continue to answer questions, and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *Please describe the activities which may raise privacy concerns.*

Activities are focused on internal administrative efforts (employee information), web-based inquiries and information sharing, and business specific information (contracts, proposals, etc...). All are protected in ways detailed in the Privacy Impact Assessment (PIA) for NOAA 6101.

No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

- Companies
- Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- DOC employees
- Contractors working on behalf of DOC
- Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

 x I certify the criteria implied by one or more of the questions above **apply** to the NOS Office for Coastal Management (OCM) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Chuck Baxley (ISSO)

Signature of ISSO or SO: BAXLEY.CHARLES.A.III.105 Digitally signed by BAXLEY.CHARLES.A.III.1058676264
8676264 Date: 2018.01.10 11:08:07 05'00'

Name of Information Technology Security Officer (ITSO): John D. Parker (ITSO)

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914
PARKER.JOHN.D.1365835914 Date: 2018.01.24 08:14:59 05'00'

Name of Authorizing Official (AO): Jeffrey L. Payne (AO)

Signature of AO: PAYNE.JEFFREY.L.DR.1365833 Digitally signed by PAYNE.JEFFREY.L.DR.1365833881
881 Date: 2018.01.10 17:55:59 05'00'

Name of Bureau Chief Privacy Officer (BCPO): MARK GRAFF

Signature of BCPO: GRAFF.MARK.HYRUM.1514447 Digitally signed by GRAFF.MARK.HYRUM.1514447892
892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892
Date: 2018.01.25 17:12:54 -05'00'

**U.S. Department of Commerce
NOAA**



**Privacy Impact Assessment
For
NOAA 6101
Office for Coastal Management**

Reviewed by: _____ Mark Graff _____, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

**U.S. Department of Commerce Privacy Impact Assessment
NOAA 6101
Office for Coastal Management**

Unique Project Identifier: NOAA 6101

Introduction: System Description

The mission of the National Oceanic and Atmospheric Administration (NOAA)'s NOAA6101, Office for Coastal Management (OCM) is to catalyze and influence a broad base of leaders, citizens, and coastal practitioners to ensure healthy coastal ecosystems, resilient coastal communities, and vibrant and sustainable coastal economies. The coast and its residents are at the epicenter of the impacts of changes in weather, climate, demographics, and economies. OCM manages coastal resources and uses through strengthening governance and investments in the development and implementation of comprehensive policies, rules, and plans. OCM administers the Coastal Zone Management Act, the Coral Reef Conservation Act, the Deep Seabed Hard Mineral Resources Act of 1980, and the Ocean Thermal Energy Conversion Act of 1980.

NOAA6101 is a general support system used to ensure that the OCM's scientific and internal administrative / operational needs are met. The system is an integrated collection of subsystems designed to provide general office automation, infrastructure, and connectivity services to NOAA OCM staff located in Charleston, SC, Silver Spring, MD, Honolulu, HI, Stennis Space Center, MS, additional OCM field offices, and other remote locations. The system enables OCM to achieve its mission, which is to support the environmental, social, and economic well-being of the coast by linking people, information, and technology. OCM assists the nation's coastal resource management community by providing access to information, technology, and training, and by producing new tools and approaches that often can be applied nationwide.

The OCM Strategic Plan addresses three strategic outcomes for the coastal management community: healthy coastal ecosystems, resilient coastal communities, and vibrant and sustainable coastal economies.

OCM has both Personally Identifiable Information (PII) and Business Identifiable Information (BII) within its system boundary. This Privacy Impact Assessment (PIA) details the types of PII/BII found within the system boundary for NOAA 6101, and how that information is protected.

Two of the component subsystems are the internal networked file servers and web application servers. The file servers are restricted to OCM staff members and typically used for administrative and operational functions and/or storage such as:

- Administrative functions (replacing a manual process),
- Employee/Contractor information needed for personnel, security, performance evaluation, merit rewards, training, travel, etc.,
- Review of applicant information (e.g., information submitted in response to requests for proposals and/or in response to a solicitation),

- To track information, requests, tasks, actions, or processes related to the OCM / NOAA mission.

The OCM web servers host and serve web-based applications and sites. OCM’s web servers primarily serve publicly accessible information, which is intended for OCM and other subsets of OCM, NOAA, other federal agencies, customers, partners, and/or the general public. There are a few applications and sites that are intentionally restricted (authentication required) to NOAA employees and contractors operating from within the NOAA network. These internal applications track information related to OCM’s operations / administration (e.g., safety/emergency contacts).

A subset of web applications/sites served by OCM web servers is detailed in section 5.1 below.

Information sharing:

As stated in Sections 5.1 and 6.1, information is periodically shared within the bureau on a case-by-case basis. Additionally, non-sensitive POC information for certain subject matter experts is made available via the OCM web presence.

For verification of foreign visitor identity, information may be shared with NOAA Security and DHS FLETC.

5 U.S.C. § 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

15 U.S.C. § 1512 is an Organic Law which confers general powers and duties authority to executive agencies, vesting jurisdiction and control of departments, bureaus, offices and branches.

The Federal Information Processing Standard (FIPS) 199 security impact category for the system is Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.

_____ This is an existing information system with changes that create new privacy risks.

(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	
b. Anonymous to Non-Anonymous		e. New Public Access	
		g. New Interagency Uses	
		h. Internal Flow or Collection	

c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

- This is an existing information system in which changes do not create new privacy risks.

OCM made this choice in part because one FISMA system was absorbed into another during the Coastal Services Center (CSC) (NOAA6101) and Office for Ocean and Coastal Resource Management (OCRM) (NOAA6601) office integration, so there was no new system created. Additionally, OCM does not believe the types of information/data that were added to NOAA6101 were different from any of the already present information and data and imparted no new risks to 6101.

Section 2: Information in the System

- 2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (*Check all that apply.*)

Identifying Numbers (IN)					
a. Social Security*	x	e. File/Case ID		i. Credit Card	
b. Taxpayer ID	x	f. Driver's License		j. Financial Account	
c. Employer ID	x	g. Passport	x	k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: Social Security numbers are collected for new NOAA/NOS/OCM employees. <i>These are transmitted to the NOAA Security Office via secure electronic transmission and then destroyed.</i> OCM does <u>not</u> maintain them on the IT system or as hard copy files. Passport numbers are handled in the same way as SSNs. These procedures are detailed in the OCM Standard Operating Procedure-Personnel Security. This SOP will be included/referenced in the NOAA 6101 System Security Plan. Taxpayer or employer ID information is collected infrequently (see section 5.1 for more details), but is stored only temporarily on the system.					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	x	o. Medical Information	
d. Gender		j. Telephone Number	x	p. Military Service	
e. Age		k. Email Address	x	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): Employee information is collected for emergency/disaster/CoOP-related contact needs. General inquiries related to information sharing consist of collecting name and email address in order to respond to the information requests. Certain subject matter experts agree explicitly to share contact information (name, phone, email) on OCM's public web site.					

Work-Related Data (WRD)					
a. Occupation	x	d. Telephone Number	x	g. Salary	
b. Job Title	x	e. Email Address	x	h. Work History	
c. Work Address	x	f. Business Associates			
i. Other work-related data (specify): Work related data is collected and shared with employees for internal office communication purposes. Additionally, grant or contract proposal information often contains PII/BII, such as budgets or cost proposals; this information is only accessible to those involved in grant or contract-specific work activities, and only on a need-to-know basis. Additionally, all financial transactions take place outside of the OCM system (i.e., NOAA Finance, Grants Online handle financial transactions). See section 5.1 below for more details.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)					

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	x	Hard Copy: Mail/Fax	x	Online	x
Telephone	x	Email	x		
Other (specify):					

Government Sources					
Within the Bureau	x	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations	x	Private Sector	x	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify): OCM uses CAC cards like much of the federal government, but none of that data is stored on OCM's system.			

x	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
---	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	x
Video surveillance		Electronic purchase transactions	
Other (specify):			

Building entry readers recognize CAC cards used to gain entry, but do not store any of the data embedded on the card.

X	There are not any IT system supported activities which raise privacy risks/concerns.
---	--------------------------------------------------------------------------------------

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	x
For administrative matters	x	To promote information sharing initiatives	x
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	x	For web measurement and customization technologies (multi-session)	x
Other (specify):			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

PII is collected to communicate with OCM customers and stakeholders on topics where they have an explicitly expressed professional interest, or have made a specific request for data or information.

Other PII is collected for OCM staff employment and personnel records (federal/contractor) and OCM visitor access information (federal/contractor/member of the public/foreign national).

BII is collected and maintained for purposes such as contractual agreements and grants.

Details are found below.

NOAA's Office for Coastal Management Business Operations Division collects data containing personally identifiable and business identifiable information (BII) for internal government operations / administrative processes. The processes include:

- Employee / Contractor information needed for personnel, performance evaluation, merit rewards, training, travel, accident reporting, etc. This type of PII information is reviewed and updated annually by staff.
- Employee / Contractor / Visitors / Foreign National information required by DOC and/or OPM for security purposes and/or background checks. Passport numbers are collected for foreign visitors, sent as appropriate for security checks, and removed from the system. All information is required per DOC PII Policy and Foreign National Processing¹ guidance as well as the Federal Law Enforcement Training Center (FLETC) Foreign National Visitor Process.
- Employee / Contractor emergency contact information for use in call trees, Continuity of Operations Plan (COOP), etc. which includes names, phone numbers, and addresses
- Applicant information submitted in response to requests for proposals and/or in response to a solicitation

External grant applications/proposals are not typically collected by OCM. Per the NOAA Grants Management Office policy, proposals almost always run through the Grants.gov submission process and end up in the Grants Online system. In rare cases, applicants without access to the Internet [e.g., US

¹ [http://deemedexports.noaa.gov/Documents/Message on Electronic Transmission of PII.pdf](http://deemedexports.noaa.gov/Documents/Message_on_Electronic_Transmission_of_PII.pdf)

territories] are permitted to submit paper applications. When this happens, OCM scans the proposals and loads them into Grants Online. Any subsequent sharing of grant proposals via email for review must be done via a secure file transfer process (e.g., Grants Online, Accellion if emailing internally or externally to NOAA, a secure Google Drive or a network location for internal NOAA reviewers, or a password protected website for internal and external NOAA reviewers). Once reviews are complete and awards are made, proposals are removed from the OCM system and the Grants Online system is the official repository.

Typical personal or business identifiable information collected for grant applications includes:

- proposer's name
- email
- phone #
- organization name
- organization DUNS #
- employer identification number or taxpayer identification number

For acquisitions, the business identifiable information collected typically includes:

- proposer's name
- email
- phone #
- organization name
- organization DUNS #
- Cost proposal information is also collected, and would be considered sensitive BII, as it is often proprietary.
- Management and technical approaches found in vendor proposals is often considered BII.

Other PII that is being collected and/or made available via Internet / Web sites or applications include:

- PRiMO: Web site that publicly lists some partner organization POCs (name, organization, email, phone number), along with OCM POCs. POC information is entirely voluntary and can be removed at any time upon request.
- Coastal Storms Program: Web site that publicly lists some partner organization POCs (name, organization, email, phone number), along with OCM POCs. POC information is entirely voluntary and can be removed at any time upon request.
- OCM Intranet: Contains current information on staff, including phone numbers, names, email addresses, and emergency contacts. The system is used to maintain up

- to date records on staff contact information.
- Task Order Management Information System (TOMIS): Application that collects and maintains POC information (name, email, phone, company name) for use in administering various contractor tasks and deliverables.
 - National Estuarine Research Reserves: Web site that publicly lists some partner organization POCs (name, organization, email, phone number), along with OCM POCs. POC information is entirely voluntary and can be removed at any time upon request.
 - Estuaries Education: Web site that publicly lists some partner organization POCs (name, organization, email, phone number), along with OCM POCs. POC information is entirely voluntary and can be removed at any time upon request.
 - Digital Coast: Publishes contact information of trainers for some trainings listed on the Digital Coast Training page. Information includes (name, email, location). Permission is acquired (via a form) from each trainer before listing their information on the site.
 - Ocean Law Search: Web site related to underwater cultural heritage that makes various public laws, statutes, articles, and court case summaries via an online searchable interface. All of the information available is publicly accessible and has been assembled to focus on underwater cultural heritage. Some of the documents available contain names and addresses of legislators, attorneys, plaintiffs, or witnesses.
 - CAMMP: Application that assists in building grant proposals. Data collected from applicants includes (name, title, email, applicant personnel names and salaries for grant budgeting).
 - Coral DB: Application that collects internal NOAA staff proposals to the NOAA Corals matrix program.
 - Data in the Classroom: Web site that publicly lists some OCM POCs (one staff member name, with phone and email). POC information is entirely voluntary and can be removed at any time upon request. There is also a “contact us” page, which collects name, zip code, phone.
 - Data Access Viewer (DAV): Application that receives requests for data from the public. Email addresses are stored to provide a method of contacting the requester when the data is ready for pickup on the OCM FTP site.
 - Training Manager System: Web site that collects information on training courses, hosts and participants of OCM training programs. Information that is collected is not shared publicly. Fields collected include (name, organization, address, city, state, zip, email, phone).
 - OCM Point of Contact Management Database: Centralized contact management database used to maintain information from customers who have requested data or information, participated in conferences, requested products/materials, or attended meetings or trainings offered by OCM. This is a secure and centralized database.

Fields collected include (name, title, organization, address, city, state, zip, country, email, phone).

- National Estuarine Research Reserves (NERRs) Intranet is an authenticated application for NERRs and OCM staff to work collaboratively. Information collected includes name, organization, email, and phone number.
- NERRs and State Coastal Zone Management Performance Measures DBs are authenticated applications for NERRs and CZM partners to document grant performance measures in a standardized way, and to work collaboratively with OCM staff. Information collected includes name, organization, email, and phone number.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus			
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			x (only non-sensitive, point of contact information is shared, typically for subject matter experts who have agreed to share this information)
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

* DHS FLETC for verification of foreign visitor identity.

	The PII/BII in the system will not be shared.
--	-----------------------------------------------

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
x	No, this IT system does not connect with or receive information from another IT system(s) authorized to

process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. (*Check all that apply.*)

Class of Users			
General Public		Government Employees	x
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. (*Check all that apply.*)

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
x	<p>Yes, notice is provided by Privacy Act statements (five total) and/or privacy policy. The Privacy Act statements can all be found in the appendix below and also at:</p> <ul style="list-style-type: none"> • https://coast.noaa.gov/contactform/ (Contact Us) • OCM Intranet (access is restricted) (OCM Intranet) • Offline form (access is restricted) (Partner Contact Information) • Performance measure tracking system (access is restricted) (CZM Performance Measures) • NERRs Intranet and performance measure tracking system (access is restricted) (NERRs Intranet and Performance Measures) <p>The privacy policy can be found at: coast.noaa.gov/PrivacyPolicy/privacyPolicy.html .</p>	
x	Yes, notice is provided by other means.	<p>Specify how: Subject matter experts often provide contact information via the OCM public web site. Prior to making the POC information public, the subject matter experts are asked to fill out a form acknowledging that they will be providing this information on a public web site and that they agree to do so. A Privacy Act statement is also made available.</p> <p>Visitors to the OCM web presence can request information by providing minimal PII through an information request contact form. Individuals are under no obligation to provide this information, and the details of how this information is handled are readily available via the OCM Privacy Policy and a Privacy Act statement.</p> <p>OCM staff members (employees) are provided notice of how PII is used (i.e., emergency contact information in case of natural disasters) upon hire.</p> <p>Partners/grantees may provide contact information (PII) to participate in the NERRs Intranet site established for collaboration and to enter data into grantee performance measurement tracking systems.</p>

		Vendors and grantees are notified via solicitations and calls for proposals that BII will be collected as necessary to effectively evaluate proposals.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

x	Yes, individuals have an opportunity to decline to provide PII/BII.	<p>Specify how: Subject matter experts often provide contact information via the OCM public web site. Prior to making the POC information public, the subject matter experts are asked to fill out a form acknowledging that they will be providing this information on a public web site and that they agree to do so; all have the opportunity to decline to provide PII as it is an “opt in” scenario. A Privacy Act statement is also made available.</p> <p>Visitors to the OCM web presence can request information by providing minimal PII through an information request contact form. Individuals are under no obligation to provide this information, and the details of how this information is handled are readily available via the OCM Privacy Policy and a Privacy Act statement.</p> <p>Staff members provide PII upon hire as a condition of employment. A Privacy Act statement concerning usage of this information is made available to OCM staff members. They may decline to provide PII but this may affect their employment status.</p> <p>Partners/grantees may provide contact information (PII) to participate in the NERRs Intranet site established for collaboration and to enter data into grantee performance measurement tracking systems. Partners can decline to provide this information as it is an “opt in” scenario.</p> <p>Vendors and/or grantees provide BII when submitting proposals of various types. Proposers may decline to provide BII, by not including it in their proposals; however, that declination effectively removes them from consideration of contract or grant awards, as there are certain types of information that contain BII that are essential to a full and valid competition.</p>
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Subject matter experts who may be asked or offer to provide contact information are informed of exactly how and where on the OCM web site their contact information will be made available. A Privacy Act statement for this type of scenario is also available.
---	--------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>Visitors to the OCM web presence can learn how PII is used via the OCM Privacy Policy and make the choice to opt in to the particular stated uses. A Privacy Act statement for this type of scenario is also available.</p> <p>Staff members provide PII upon hire as a condition of employment. They may consent to only particular uses, but this may affect their employment. A Privacy Act statement for this type of scenario is also available.</p> <p>Partners/grantees who provide contact information (PII) to participate in the NERRs Intranet site established for collaboration or to enter data into grantee performance measurement tracking systems opt in to providing PII for the particular stated uses.</p> <p>For vendors and grantees, the only usage of the BII is during proposal review and subsequent consultation with vendors or grantees. The BII is not shared or disseminated beyond this scope.</p>
	<p>No, individuals do not have an opportunity to consent to particular uses of their PII/BII.</p>	<p>Specify why not:</p>

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

<p>x</p>	<p>Yes, individuals have an opportunity to review/update PII/BII pertaining to them.</p>	<p>Specify how: Subject matter experts who provide contact information on the OCM web site can review, update, or delete their PII upon request at any time.</p> <p>Web site visitors who provide PII via a request for information can request to review, update or delete the PII provided at any time.</p> <p>Staff members can update PII during performance reviews or via secure Intranet.</p> <p>Partners/grantees who provide contact information (PII) to participate in the NERRs Intranet site established for collaboration or to enter data into grantee performance measurement tracking systems can review, update, or delete their PII upon request at any time.</p> <p>Vendors or grantees can review/update BII at any time upon request to the NOS proposal contact.</p>
	<p>No, individuals do not have an opportunity to review/update PII/BII pertaining to them.</p>	<p>Specify why not:</p>

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. (*Check all that apply.*)

	All users signed a confidentiality agreement or non-disclosure agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access to PII is tracked via logging of network directory access; logging of secured database access; and logging of Intranet administrative access.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 5/3/2016 <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones. An independent A&A is scheduled for completion by March 2017. All findings will be analyzed and will undergo NOS POA&M Management Process that could result in risk acceptance or creation of a POA&M.
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

<p>Secured database</p> <ul style="list-style-type: none"> OCM secures PII data into a SQL Server database on a secured server. Databases are only accessible based on least privilege and job requirements. Access is limited to SQL Administrators and IT Staff that are authorized for administrative system access. The servers hosting the aforementioned databases exist in an access controlled internally hosted data center where physical access is monitored and granted exclusively based on position responsibilities. Non-privileged users are restricted to access via SQL Server accounts only. Information placed in the database is only accessed on a need-to-know basis by internal staff who are identified as needing access to this information. <p>Secured file/folder network directory</p> <ul style="list-style-type: none"> OCM enforces assigned authorizations for controlling access to the system through the use of logical access control policies. Access controls lists are configured to enforce access authorization and assign user and group privileges. These access

control policies are employed to control the access between users and objects (files, directories, servers, printers, etc.). Access enforcement mechanisms are in place at the network, system and application levels.

Plans for encryption at rest: OCM's SQL Server databases are SQL v 2012 Standard Edition. This version/edition does not allow for straightforward encryption and therefore the PII data stored in our secure database is not encrypted. We secure the database via access control and configuration management as stated above. OCM does intend to upgrade to SQL 2016 SP1 as soon as possible, and at latest, by 9/30/2017. This upgrade will provide a straightforward pathway to database encryption. In addition, we are actively engaged in moving applications and databases into Microsoft Azure which also provides automatic SQL DB encryption.

Section 9: Privacy Act

- 9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

x	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i> : Existing Privacy Act system of records notices (SORNs) for NOAA cover the personnel information in this system: COMMERCE/DEPT-18 - Employees Personnel Files Not Covered by Notices of Other Agencies and NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission. Also, DEPT-2, Accounts Receivable; DEPT-6, Visitor Logs and Permits for Facilities under Department Control; DEPT-13, Investigative and Security Records; DEPT-25, Access Control and Identity Management System; and GSA/Govt-7, Federal Personal Identity Verification Identity Management System.
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

Section 10: Retention of Information

- 10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

x	There is an approved record control schedule. Provide the name of the record control schedule: The retention period for these records is guided by the
---	-----------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the federal government. The underlying paper records relating to employees are covered by GRS 1, Civilian Personnel Records. In accordance with GRS 20, item 3, electronic versions of records scheduled for disposal under other records schedules may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. Guidance for these records in the NOAA Records Schedules refers disposition to GRS 20.</p> <p>NOAA Records Schedules Chapter 1600 – National Ocean Service (NOS) Functional Files describes records created and maintained in the National Ocean Service (NOS) on the ocean and coastal zone management services and information products that support national needs arising from increasing uses and opportunities of the oceans and estuaries.</p> <p>1610-01 - Coastal Zone Management Program Documents 1610-02 - Program Change Files 1610-03 - Coastal Non-point Pollution Control Program 1610-04 - Federal Consistency 1610-05 - Program Administrative Guidance 1610-06 - The Coastal and Marine Management Program Information System</p>
	<p>No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:</p>
x	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	x	Overwriting	x
Degaussing	x	Deleting	x
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
x	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

x	Identifiability	Provide explanation: OCM only collects non-sensitive PII such as phone numbers and e-mail addresses. No SSNs or other sensitive PII/BIA information is electronically stored.
x	Quantity of PII	Provide explanation: Information collected is limited to a small subset of specific applications and personnel files.
x	Data Field Sensitivity	Provide explanation: Phone numbers and e-mail addresses are the primary information collected, and are used for communication purposes.
x	Context of Use	Provide explanation: The vast majority of PII collected is used for emergency contact information for staff members, or for communicating back to information requesters.
	Obligation to Protect Confidentiality	Provide explanation:
x	Access to and Location of PII	Provide explanation: Concept of least privilege; secure network and database; encrypted storage and transmission
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process change. Explanation: Addition of Privacy Act Statements to several sites.
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

X	Yes, the conduct of this PIA results in required technology changes Explanation: addition of Privacy Act Statements to several sites.
	No, the conduct of this PIA does not result in any required technology changes.

Appendix – Privacy Act Statements

NOAA OCM Privacy Act Statement (Contact Us)

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: NOAA Office for Coastal Management (OCM) collects this information for the purpose of responding to “contact us” form requests and subscriptions to newsletters from NOAA OCM websites.

Routine Uses: NOAA will use this information to respond to requests submitted on the Contact Us page and for subscriptions to newsletters as selected on the contact us form. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice Commerce/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA’s Mission.

Disclosure: Furnishing this information is voluntary.

NOAA OCM Privacy Act Statement (OCM Intranet)

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: NOAA Office for Coastal Management (OCM) collects this intranet information for employee emergency and administrative contact purposes.

Routine Uses: NOAA will use this information for emergency or administrative contact purposes. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among NOAA staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice Commerce/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA’s Mission.

Disclosure: Furnishing this information is voluntary.

NOAA OCM Privacy Act Statement (Partner Contact Information)

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: NOAA Office for Coastal Management (OCM) collects this information for the purpose of publishing the contact information of partners who provide services or resources on NOAA OCM websites.

Routine Uses: NOAA will use this information on public websites to identify points of contact for various resources listed on the NOAA Office for Coastal Management websites. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice Commerce/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.

Disclosure: Furnishing this information is voluntary.

NOAA OCM Privacy Act Statement (CZM Performance Measures)

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: NOAA Office for Coastal Management (OCM) collects this intranet information for user authentication, performance measurement project tracking and administrative contact purposes.

Routine Uses: NOAA will use this information for authentication, performance measurement project tracking and administrative contact purposes. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among NOAA staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice Commerce/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.

Disclosure: Furnishing this information is voluntary.

NOAA OCM Privacy Act Statement (NERRs Intranet and Performance Measures)

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: NOAA Office for Coastal Management (OCM) collects this intranet information for user authentication, organizational directory, performance measurement tracking, and administrative contact purposes.

Routine Uses: NOAA will use this information for authentication, organizational directory, employee emergency, and administrative contact purposes. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among NOAA staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice Commerce/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.

Disclosure: Furnishing this information is voluntary.

Points of Contact and Signatures

<p>Information System Security Officer or System Owner Name: Anthony A. LaVoi Office: NOAA/NOS/OCM Phone: 843-740-1274 Email: Tony.LaVoi@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>LAVOI.ANTHONY.A.1365862580 <small>Digitally signed by LAVOI.ANTHONY.A.1365862580 Date: 2018.01.25 10:50:31 -05'00'</small></p>	<p>Information Technology Security Officer Name: John Parker Office: NOAA/NOS Phone: 240-533-0832 Email: John.D.Parker@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>PARKER.JOHN.D.1365835914 <small>Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.01.24 15:28:59 -05'00'</small></p>
<p>Authorizing Official Name: Jeffrey L. Payne Office: NOAA/NOS/OCM Phone: 843-740-1207 Email: Jeff.Payne@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>PAYNE.JEFFREY.L.DR.1365833881 <small>Digitally signed by PAYNE.JEFFREY.L.DR.1365833881 Date: 2018.01.10 17:57:46 -05'00'</small></p>	<p>Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA/OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>GRAFF.MARK.HYRUM.1514447892 <small>Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.25 17:15:31 -05'00'</small></p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Friday, January 26, 2018 10:00 AM
To: Troy Cole NOAA Federal
Cc: Brent MacAloney; Mark Graff NOAA Federal
Subject: Re: Account info in NOAA1300
Attachments: PTA Template 01 2017.docx; PIA_Template_01 2017.docx

Maybe I'm not clear on whose information this is. It's vendor information? For some reason, I thought it was employees and contractors. If vendor, then not duplicative.

As soon as you think you have enough information, please use, or have the applicable person use, the attached new PTA and PTA templates for your drafts. I'm not sure of Amin's role he is the one who sent me a PTA the other day with user ID only checked.

Yes, encryption is good, and in fact is now required for PII.

On Fri, Jan 26, 2018 at 9:54 AM, Troy Cole NOAA Federal <troy.cole@noaa.gov> wrote:

Hi Sarah... I'm confused by your statement about "needless duplication." Who are we advocating that position to - our Vendors? If so, that is not a realistic option as we have tens of thousands of vendors and they can easily ignore our request as opposed to customizing documents for our Agency.

In the end, we are looking to ensure that the encryption utilized within ServiceNow is sufficient in the event an attachment contains banking information, business TINs, or (rarely) SSNs. What do we need to do to make sure we are covered? My understanding is that Brent implemented the Agency's encryption standard within ServiceNow, so he did not go rogue there...

Thanks,
Troy

Troy Cole

Chief, Commercial Payments Branch
Accounting Operations Division
NOAA Finance Office
[\(301\) 444 2790](tel:(301)444-2790)

On Fri, Jan 26, 2018 at 9:15 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

You can't really do a privacy impact assessment for data that is not yet determined. There would have to be a clear plan for its collection. Is there anyone with whom you can advocate that this is needless duplication and and privacy risk?

Looping Mark back in here.

On Fri, Jan 26, 2018 at 7:46 AM, Brent MacAloney <brent.macaloney@noaa.gov> wrote:

That's what Troy and I figured. Funny how if someone sends us something we don't ask for, we are still

accountable for anticipating that the information may be sent and then subsequently safeguarding that information.

I guess the question I have for you is what are the next steps?

Thanks,
Brent

On Thu, Jan 25, 2018 at 5:01 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
Oh, yes, we would be held accountable. thx

On Thu, Jan 25, 2018 at 4:59 PM, Brent MacAloney <brent.macaloney@noaa.gov> wrote:
Hi Sarah,

Unfortunately, that's not my call. I have a tasking to transfer the Commercial Payments Branch processing over to ServiceNow. The thing is the Commercial Payments Branch is not requiring the collection of this information, nor do they want it. However, people do sometimes include it when they send invoices in. Troy is trying to do the right thing and make sure that in the event that information is unnecessarily sent, we are covered from a PII standpoint.

So with that said, would we be held accountable if that type of unsolicited information was included in an invoice attachment processed in ServiceNow platform and we did not document that in the NOAA1300 PIA?

Thanks,
Brent

On Thu, Jan 25, 2018 at 4:40 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
Hey, my recommendation is not to collect any of that. It's redundant for one thing. Encryption is good but would not prevent the need for a PIA for the system.

On Thu, Jan 25, 2018 at 4:32 PM, Brent MacAloney <brent.macaloney@noaa.gov> wrote:
Hi Sarah,

When you say NOAASafe, do you mean ServiceNow? If not, I'm not sure what NOAASafe is and we'd probably have to ask the folks at ActioNet for more clarification.

With ServiceNow, the only information we currently collect is information that is in the NOAA LDAP. If you are talking about what we'd like to start collecting for the Commercial Payments Branch, then I will need to involve Troy Cole in that discussion. It is my understanding that it could contain (most of the time it wouldn't) Bank Account Information, Social Security Numbers, Tax ID Numbers, and business points of contact and their addresses. Although what makes this unique is that all of this information would be contained in an encrypted file and not a searchable database field.

Not sure if this helps with your original question or not.

Brent

On Thu, Jan 25, 2018 at 12:30 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

Brent, can you tell me what PII other than user ID is in this NOAASafe? I got a PTA just now that says user ID only . . .

BII from businesses and/or companies?

PII from feds, contractors and/or members of the public?

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

Brent MacAloney

Enterprise Services Program Manager
Service Delivery Division
NOAA Office of the Chief Information Officer
U.S. Department of Commerce
Ofc: [\(301\) 628-5758](tel:3016285758)
Mob (b)(6)
Email: Brent.MacAloney@noaa.gov

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

Brent MacAloney

Enterprise Services Program Manager
Service Delivery Division
NOAA Office of the Chief Information Officer
U.S. Department of Commerce
Ofc: [\(301\) 628-5758](tel:3016285758)
Mob: (b)(6)
Email: Brent.MacAloney@noaa.gov

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

Brent MacAloney

Enterprise Services Program Manager
Service Delivery Division
NOAA Office of the Chief Information Officer
U.S. Department of Commerce
Ofc: [\(301\) 628-5758](tel:3016285758)
Mob: (b)(6)
Email: Brent.MacAloney@noaa.gov

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751

Ce (b)(6)

U.S. Department of Commerce
[Bureau Name]



Privacy Impact Assessment
for the
[IT System Name]

Reviewed by: _____, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment
[Name of Bureau/Name of IT System]

Unique Project Identifier: [Number]

Introduction: System Description

*Provide a description of the system that addresses the following elements:
 The response must be written in plain language and be as comprehensive as necessary to describe the system.*

- (a) Whether it is a general support system, major application, or other type of system*
- (b) System location*
- (c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
- (d) The way the system operates to achieve the purpose(s) identified in Section 4*
- (e) How information in the system is retrieved by the user*
- (f) How information is transmitted to and from the system*
- (g) Any information sharing conducted by the system*
- (h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*
- (i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system*

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- _____ This is a new information system.
- _____ This is an existing information system with changes that create new privacy risks.
 (Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify):			

- _____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

- 2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)			
a. Social Security*		e. File/Case ID	i. Credit Card
b. Taxpayer ID		f. Driver's License	j. Financial Account
c. Employer ID		g. Passport	k. Financial Transaction
d. Employee ID		h. Alien Registration	l. Vehicle Identifier
m. Other identifying numbers (specify):			
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:			

General Personal Data (GPD)			
a. Name		g. Date of Birth	m. Religion
b. Maiden Name		h. Place of Birth	n. Financial Information
c. Alias		i. Home Address	o. Medical Information
d. Gender		j. Telephone Number	p. Military Service
e. Age		k. Email Address	q. Physical Characteristics
f. Race/Ethnicity		l. Education	r. Mother's Maiden Name
s. Other general personal data (specify):			

Work-Related Data (WRD)			
a. Occupation		d. Telephone Number	g. Salary
b. Job Title		e. Email Address	h. Work History
c. Work Address		f. Business Associates	
i. Other work-related data (specify):			

Distinguishing Features/Biometrics (DFB)			
a. Fingerprints		d. Photographs	g. DNA Profiles
b. Palm Prints		e. Scars, Marks, Tattoos	h. Retina/Iris Scans
c. Voice Recording/Signatures		f. Vascular Scan	i. Dental Profile
j. Other distinguishing features/biometrics (specify):			

System Administration/Audit Data (SAAD)			
a. User ID		c. Date/Time of Access	e. ID Files Accessed
b. IP Address		d. Queries Run	f. Contents of Files
g. Other system administration/audit data (specify):			

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		
Other (specify):					

Government Sources					
Within the Bureau	<input type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		
Other (specify):					

Non-government Sources					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input type="checkbox"/>		
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
	No, the information is not covered by the Paperwork Reduction Act.

- 2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

<input type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
--------------------------	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

- 3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

<input type="checkbox"/>	There are not any IT system supported activities which raise privacy risks/concerns.
--------------------------	--------------------------------------------------------------------------------------

Section 4: Purpose of the System

- 4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated

will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

- 5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	-----------------------------------------------

- 6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input type="checkbox"/>	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
<input type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

- 6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input type="checkbox"/>		<input type="checkbox"/>
Other (specify):			

Section 7: Notice and Consent

- 7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

<input type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
<input type="checkbox"/>	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement

	and/or privacy policy can be found at:	.
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a

	moderate or higher.
	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i>
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

	There is an approved record control schedule. Provide the name of the record control schedule:
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	<input type="checkbox"/>	Overwriting	<input type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input type="checkbox"/>
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

	Identifiability	Provide explanation:
	Quantity of PII	Provide explanation:
	Data Field Sensitivity	Provide explanation:
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:

	Other:	Provide explanation:
--	--------	----------------------

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

--	--

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

<p>Information System Security Officer or System Owner</p> <p>Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>Date signed:</p>	<p>Information Technology Security Officer</p> <p>Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>Date signed:</p>
<p>Authorizing Official</p> <p>Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>Date signed:</p>	<p>Bureau Chief Privacy Officer</p> <p>Name: Office: Phone: Email:</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>Signature:</p> <p>Date signed:</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

U.S. Department of Commerce
[Bureau Name]



Privacy Threshold Analysis
for the
[IT System Name]

U.S. Department of Commerce Privacy Threshold Analysis

[Name of Bureau/Name of IT System]

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

- a) *Whether it is a general support system, major application, or other type of system*
- b) *System location*
- c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
- d) *The purpose that the system is designed to serve*
- e) *The way the system operates to achieve the purpose*
- f) *A general description of the type of information collected, maintained, use, or disseminated by the system*
- g) *Identify individuals who have access to information on the system*
- h) *How information in the system is retrieved by the user*
- i) *How information is transmitted to and from the system*

Questionnaire:

1. What is the status of this information system?

_____ This is a new information system. *Continue to answer questions and complete certification.*

_____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify):			

_____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

_____ Yes. *Please describe the activities which may raise privacy concerns.*

_____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the submitter has a commercial interest” and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)”

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

- Companies
- Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- DOC employees
- Contractors working on behalf of DOC
- Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

_____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

_____ I certify the criteria implied by one or more of the questions above **apply** to the [IT SYSTEM NAME] and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Signature of ISSO or SO: _____ Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: _____ Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: _____ Date: _____

Name of Bureau Chief Privacy Officer (BCPO): _____

Signature of BCPO: _____ Date: _____

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Friday, January 26, 2018 12:07 PM
To: Mark Graff NOAA Federal
Cc: Nancy Defrancesco; Brian.Little
Subject: NOAA5023 certification docs for your signature
Attachments: NOAA5023 SARSAT PIA_for NOAA CPO and DOC SAOP sigs.pdf; NOAA5023 PIA Annual Review Certification Form with PA Officer Final__JAN2018.pdf; NOAA5023 PTA 20170814.pdf

Mark, attached are the current PIA with most recent ATO signature, and Section 1.1 stating no new privacy risks.

Also the PTA from 8 14 17, also stating new privacy risks.

And finally, the certification, also stating no new privacy risks.

thx for signing! Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751

Ce (b)(6)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NOAA/Search and Rescue Satellite-Aided Tracking (SARSAT) (NOAA5023)

FISMA Name/ID (if different): Search and Rescue Satellite-Aided Tracking (SARSAT) / NOAA5023

Name of IT System/ Program Owner: Thomas Renkevans

Name of Information System Security Officer: Brian Little

Name of Authorizing Official(s): Mark Paese

Date of Last PIA Compliance Review Board (CRB): 06/08/2017
(This date must be within three (3) years.)

Date of PIA Review: 1/10/2018

Name of Reviewer: Brian Little

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: LITTLE.BRIAN.WILLIAM.1365841230 Digitally signed by LITTLE.BRIAN.WILLIAM.1365841230
Date: 2018.01.10 13:09:07 -05'00'

Date of Privacy Act (PA) Review: 1/10/2018

Name of Reviewer: Brian Little

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: LITTLE.BRIAN.WILLIAM.1365841230 Digitally signed by LITTLE.BRIAN.WILLIAM.1365841230
Date: 2018.01.10 13:09:43 -05'00'

Date of BCPO Review: _____

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): _____

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: _____

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Friday, January 26, 2018 3:13 PM
To: Nancy Defrancesco; Beckie Koonge NOAA Federal; Andrew Browne NOAA Affiliate; Amores, Catherine (Federal); Tahir Ismail; _NMFS InfoSec; John D. Parker; James Jones NOAA Affiliate
Cc: Mark Graff NOAA Federal
Subject: Re: Announcement of new DOC PIA and PTA templates
Attachments: PIA_Template_01 2017.docx; PTA Template 01 2017.docx

Just to let you know that on more careful examination of the templates, as the first person completed her PIA and PTA the last few items in the system descriptions differ slightly between the PIA and PTA.

And I'm resending both templates here since I had inadvertently sent the PIA pdf yesterday, and then sent the correct one by itself this am.

They are both of course on the NOAA privacy page.

That's it, thanks

thx Sarah

On Thu, Jan 25, 2018 at 2:31 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
New DOC PIA and PTA templates are attached, and also posted on the NOAA Privacy Page: http://www.cio.noaa.gov/services_programs/privacy.html.

The changes: there are a few more items included in both the PIA and PTA system descriptions (d, e and f), and there are three new questions in the PIA:

2.3: Describe how the accuracy of the information in the system is ensured.

2.4: Is the information covered by the Paperwork Reduction Act? (in most cases, other than Fisheries, this will be no, but please consult with me, as the PRA Clearance Officer, to make sure).

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately.

I have not yet updated the PIA guidance posted on the privacy page, but these questions should be fairly self-explanatory in the meantime.

Please let your ISSOs know of these new templates at your next regular meeting. I am letting each know as we prepare for the next PTA or PIA.

Sarah D. Brabson

IT Infrastructure Investment Program Manager

PRA Clearance Officer

Governance and Portfolio Division

Office [301 628 5751](tel:3016285751)

Ce (b)(6)

Sarah D. Brabson

IT Infrastructure Investment Program Manager

PRA Clearance Officer

Governance and Portfolio Division

Office 301 628 5751

Ce (b)(6)

U.S. Department of Commerce
[Bureau Name]



Privacy Impact Assessment
for the
[IT System Name]

Reviewed by: _____, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment
[Name of Bureau/Name of IT System]

Unique Project Identifier: [Number]

Introduction: System Description

*Provide a description of the system that addresses the following elements:
 The response must be written in plain language and be as comprehensive as necessary to describe the system.*

- (a) Whether it is a general support system, major application, or other type of system*
- (b) System location*
- (c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
- (d) The way the system operates to achieve the purpose(s) identified in Section 4*
- (e) How information in the system is retrieved by the user*
- (f) How information is transmitted to and from the system*
- (g) Any information sharing conducted by the system*
- (h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*
- (i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system*

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- _____ This is a new information system.
- _____ This is an existing information system with changes that create new privacy risks.
 (Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify):			

- _____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

- 2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)			
a. Social Security*		e. File/Case ID	i. Credit Card
b. Taxpayer ID		f. Driver's License	j. Financial Account
c. Employer ID		g. Passport	k. Financial Transaction
d. Employee ID		h. Alien Registration	l. Vehicle Identifier
m. Other identifying numbers (specify):			
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:			

General Personal Data (GPD)			
a. Name		g. Date of Birth	m. Religion
b. Maiden Name		h. Place of Birth	n. Financial Information
c. Alias		i. Home Address	o. Medical Information
d. Gender		j. Telephone Number	p. Military Service
e. Age		k. Email Address	q. Physical Characteristics
f. Race/Ethnicity		l. Education	r. Mother's Maiden Name
s. Other general personal data (specify):			

Work-Related Data (WRD)			
a. Occupation		d. Telephone Number	g. Salary
b. Job Title		e. Email Address	h. Work History
c. Work Address		f. Business Associates	
i. Other work-related data (specify):			

Distinguishing Features/Biometrics (DFB)			
a. Fingerprints		d. Photographs	g. DNA Profiles
b. Palm Prints		e. Scars, Marks, Tattoos	h. Retina/Iris Scans
c. Voice Recording/Signatures		f. Vascular Scan	i. Dental Profile
j. Other distinguishing features/biometrics (specify):			

System Administration/Audit Data (SAAD)			
a. User ID		c. Date/Time of Access	e. ID Files Accessed
b. IP Address		d. Queries Run	f. Contents of Files
g. Other system administration/audit data (specify):			

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		<input type="checkbox"/>
Other (specify):					

Government Sources					
Within the Bureau	<input type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		<input type="checkbox"/>
Other (specify):					

Non-government Sources					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input type="checkbox"/>		<input type="checkbox"/>
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
	No, the information is not covered by the Paperwork Reduction Act.

- 2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

<input type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
--------------------------	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

- 3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

<input type="checkbox"/>	There are not any IT system supported activities which raise privacy risks/concerns.
--------------------------	--------------------------------------------------------------------------------------

Section 4: Purpose of the System

- 4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated

will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

- 5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	-----------------------------------------------

- 6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input type="checkbox"/>	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
<input type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

- 6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input type="checkbox"/>		<input type="checkbox"/>
Other (specify):			

Section 7: Notice and Consent

- 7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

<input type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
<input type="checkbox"/>	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement

	and/or privacy policy can be found at:	.
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a

	moderate or higher.
	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i>
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

	There is an approved record control schedule. Provide the name of the record control schedule:
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	<input type="checkbox"/>	Overwriting	<input type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input type="checkbox"/>
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

	Identifiability	Provide explanation:
	Quantity of PII	Provide explanation:
	Data Field Sensitivity	Provide explanation:
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:

	Other:	Provide explanation:
--	--------	----------------------

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

--	--

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

<p>Information System Security Officer or System Owner</p> <p>Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>Date signed:</p>	<p>Information Technology Security Officer</p> <p>Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>Date signed:</p>
<p>Authorizing Official</p> <p>Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>Date signed:</p>	<p>Bureau Chief Privacy Officer</p> <p>Name: Office: Phone: Email:</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>Signature:</p> <p>Date signed:</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

U.S. Department of Commerce
[Bureau Name]



Privacy Threshold Analysis
for the
[IT System Name]

U.S. Department of Commerce Privacy Threshold Analysis

[Name of Bureau/Name of IT System]

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

- a) *Whether it is a general support system, major application, or other type of system*
- b) *System location*
- c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
- d) *The purpose that the system is designed to serve*
- e) *The way the system operates to achieve the purpose*
- f) *A general description of the type of information collected, maintained, use, or disseminated by the system*
- g) *Identify individuals who have access to information on the system*
- h) *How information in the system is retrieved by the user*
- i) *How information is transmitted to and from the system*

Questionnaire:

1. What is the status of this information system?

_____ This is a new information system. *Continue to answer questions and complete certification.*

_____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify):			

_____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

_____ Yes. *Please describe the activities which may raise privacy concerns.*

_____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the submitter has a commercial interest” and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)”

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

- Companies
- Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- DOC employees
- Contractors working on behalf of DOC
- Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

_____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

_____ I certify the criteria implied by one or more of the questions above **apply** to the [IT SYSTEM NAME] and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Signature of ISSO or SO: _____ Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: _____ Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: _____ Date: _____

Name of Bureau Chief Privacy Officer (BCPO): _____

Signature of BCPO: _____ Date: _____

Mark Graff - NOAA Federal

From: Mark Graff NOAA Federal
Sent: Monday, January 29, 2018 8:32 AM
To: Sarah Brabson NOAA Federal
Cc: Nancy Defrancesco; Brian.Little
Subject: Re: NOAA5023 certification docs for your signature
Attachments: NOAA5023 PTA 20170814 mhg.pdf; NOAA5023 SARSAT PIA_for NOAA CPO and DOC SAOP sigs mhg.pdf; NOAA5023 PIA Annual Review Certification Form with PA Officer Final__JAN2018 mhg.pdf

Looks good

A couple small things. The PTA needs signatures from the ITSO and AO. Also, I'd need to get a copy of the most recent SAR or at least the Privacy Control Assessment for SARSAT to review before this is sent off to DOC. I can see the assessment from 6/6/2017 and if that's the most recent version available, that should work, but just let me know if I should be reviewing a more recent assessment. Signed and attached contingent on those two things. Thanks again

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Fri, Jan 26, 2018 at 12:07 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

Mark, attached are the current PIA with most recent ATO signature, and Section 1.1 stating no new privacy risks.

Also the PTA from 8 14 17, also stating new privacy risks.

And finally, the certification, also stating no new privacy risks.

thx for signing! Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division

Office 301 628 5751

Ce (b)(6)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NOAA/Search and Rescue Satellite-Aided Tracking (SARSAT) (NOAA5023)

FISMA Name/ID (if different): Search and Rescue Satellite-Aided Tracking (SARSAT) / NOAA5023

Name of IT System/ Program Owner: Thomas Renkevans

Name of Information System Security Officer: Brian Little

Name of Authorizing Official(s): Mark Paese

Date of Last PIA Compliance Review Board (CRB): 06/08/2017
(This date must be within three (3) years.)

Date of PIA Review: 1/10/2018

Name of Reviewer: Brian Little

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: LITTLE.BRIAN.WILLIAM.1365841230 Digitally signed by LITTLE.BRIAN.WILLIAM.1365841230
Date: 2018.01.10 13:09:07 -05'00'

Date of Privacy Act (PA) Review: 1/10/2018

Name of Reviewer: Brian Little

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: LITTLE.BRIAN.WILLIAM.1365841230 Digitally signed by LITTLE.BRIAN.WILLIAM.1365841230
Date: 2018.01.10 13:09:43 -05'00'

Date of BCPO Review: 1.29.18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: GRAFF.MARK.HYRU M.1514447892

Digitally signed by GRAFF MARK HYRUM 1514447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=OTHER, cn=GRAFF MARK HYRUM 1514447892
Date: 2018.01.29 08:24:23 -0500

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

**U.S. Department of Commerce
National Oceanic and Atmospheric Administration
(NOAA)**



**Privacy Impact Assessment
For
NOAA / Search and Rescue Satellite-Aided Tracking (SARSAT)
NOAA5023**

Reviewed by: _____Mark Graff_____, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

**U.S. Department of Commerce Privacy Impact Assessment
NOAA / Search and Rescue Satellite-Aided Tracking (SARSAT)
NOAA5023**

Unique Project Identifier: 006-48-01-15-01-3208-00

Introduction: System Description

NOAA is the lead agency in the United States (U.S.) for the Search and Rescue Satellite-Aided Tracking (SARSAT) program and represents the United States to the international COSPAS-SARSAT program. SARSAT relays distress signals, via satellite, from emergency beacons carried by aviators, mariners and land based users to search and rescue authorities.

NOAA maintains a national registry of U.S.-coded 406 MHz emergency beacon registration information that is referred to as the “Registration Database,” or RGDB (physically stored on servers within the SARSAT boundary, in Suitland, Maryland). This registry allows 406 MHz emergency beacon users to comply with registration requirements in Title 47, Parts 80, 87 and 95, of the U.S. Code of Federal Regulations (47 CFR). The RGDB also allows beacon users to comply with the requirements of the International Civil Aviation Organization (ICAO), which focuses on aviation safety and security, in compatibility with the quality of the environment, and the International Maritime Organization (IMO), a specialized agency of the United Nations, which is responsible for measures to improve the safety and security of international shipping and to prevent marine pollution from ships. It also plays a role in legal liability and compensation issues and the facilitation of international maritime traffic.

U.S. beacon owners are required by 47 CFR to register all U.S.-coded 406 MHz beacons with NOAA before installation and/or use. Each individual 406 MHz emergency beacon contains a unique hexadecimal identification code/Unique Identification Number (UIN). We have internal software that connects to the database each time there is a new distress case to check if the associated beacon is registered. If the beacon is registered, the custom internal software attaches the registration data from the database to the alert that is sent to the appropriate rescue agency/agencies. When the beacon is activated within the U.S. areas of responsibility, the beacon UIN is transmitted digitally and relayed via satellite to the U.S. Mission Control Center (USMCC). The USMCC decodes the beacon UIN, links it to the RGDB, and then appends the registration information on the distress alert message relayed to the appropriate Rescue Coordination Center (RCC) or appropriate Mission Control Center (MCC).

The information contained in the RGDB provides the RCC and MCC with the identity of the individual(s) they are searching for; contact information so that the RCC can determine whether or not the beacon has been activated as the result of an actual emergency; and information about the vessel or aircraft. The registration information allows the RCC and MCC to resolve a distress case by telephone instead of wasting valuable resources responding to false alerts. Information may be provided to or received from international registration authorities to ensure registration information resides in the correct database based on the country code of the beacon

or the mailing address of the beacon owner. Failure to register, re-register (as required every two years), or notify NOAA of any changes to the status of one's 406 MHz beacon could result in penalties and/or fines being issued under federal law.

Authorities

The legal authorities are 5 U.S.C. 301, Departmental Regulations and 47 CFR parts 80, 87, and 95. The cited regulations reflect Communications Act of 1934, as amended—(Communications Act); Communications Satellite Act of 1962, as amended—(Communications Satellite Act); International Telecommunication Union Radio Regulations, in force for the United States—(Radio Regulations); Agreement Between the United States of America and Canada for the Promotion of Safety on the Great Lakes by Means of Radio, as amended, and the Technical Regulations annexed thereto—(Great Lakes Radio Agreement); International Convention for Safety of Life at Sea, 1974, as amended, and the Annex thereto—(Safety Convention); Vessel Bridge-to-Bridge Radiotelephone Act—(Bridge-to-Bridge Act).

Information Sharing

Information is shared with other federal agencies, foreign governments and foreign entities in order to ensure rescue coordination and to ensure registration information resides in the correct database based on the country code of the beacon or the mailing address of the beacon owner. Information is shared within the bureau only in case of a privacy incident.

An amended system of records notice, COMMERCE/NOAA-20, Search and Rescue Satellite Aided Tracking (SARSAT) 406 MHz Emergency Beacon Registration Database was published on January 12, 2017 (82 FR 3719).

This is a FIPS 199 high impact system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- This is a new information system.
- This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	
b. Anonymous to Non-Anonymous		e. New Public Access	
c. Significant System Management Changes		f. Commercial Sources	
		g. New Interagency Uses	
		h. Internal Flow or Collection	
		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):			

This is an existing information system with no changes that create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (Check all that apply.)

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	X
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					
Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	
b. Job Title		e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)
Names and telephone numbers of emergency contacts.

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal	X	Foreign	X		
Other (specify)					

Non-government Sources					
Public Organizations	X	Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. (Check all that apply.)

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. (Check all that apply.)

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Search and Rescue			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The information that is collected is used by Rescue Coordination Centers and Mission Control Centers to assist in carrying out their mission of rescue coordination and false alert abatement.

A secondary use of the information is to contact beacon owners every two years to remind them to update their registration information in the RGDB.

The intended use of the information is to provide emergency beacon owner contact information to Rescue Coordination Centers to validate the need for rescue team deployment, coordinate rescue efforts and provide early identification of false alerts.

Information may be provided to or received from international registration authorities to ensure registration information resides in the correct database based on the country code of the beacon or the mailing address of the beacon owner.

The information will be shared with Mission Control Centers and Rescue Coordination Centers in the U.S. that are operated by the U.S. Air Force and the U.S. Coast Guard. If the emergency beacon is activated overseas, the information would be shared with Rescue Coordination Centers and Mission Control Centers of other countries.

Beacon owners are required to provide this information under 47 CFR Parts 80, 87 and 95.

All information is provided by the beacon owner. Owners are able to update, change and remove data at any time via the password protected Web site or by sending hard copy notification to NOAA-SARSAT.

The PII/BII identified in Section 1.1 of this document is in reference to a member of the public.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. (Check all that apply.)

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X*		
DOC bureaus			
Federal agencies	X		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments	X		
Foreign entities	X		
Other (specify):			

*For privacy incidents

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	-----------------------------------------------

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NOAA5023 shares with the following entities via File Transfer Protocol (FTP) or Secure File Transfer Protocol (SFTP) over Virtual Private Network (VPN) tunnels and via fax to assist in carrying out their mission of rescue coordination and false alert abatement:</p> <p>France Mission Control Center Spain Mission Control Center Australia Mission Control Center Russia Mission Control Center Japan Mission Control Center Air Force Rescue Coordination Center Alaska Air Command Rescue Coordination Center Coast Guard District 1-Boston Rescue Coordination Center Coast Guard District 5-Portsmouth Rescue Coordination Center Coast Guard District 7-Miami Rescue Coordination Center Coast Guard District 8-New Orleans Rescue Coordination Center Coast Guard District 9-Cleveland Rescue Coordination Center Coast Guard District 10-Seattle Rescue Coordination Center Coast Guard District 14-Honolulu Rescue Coordination Center Coast Guard District 17-Juneau Rescue Coordination Center Coast Guard Sector Guam Rescue Coordination Center Coast Guard District 11-San Francisco Rescue Coordination Center Coast Guard Sector San Juan Rescue Coordination Center Coast Guard LANTAREA-Portsmouth Rescue Coordination Center Search and Rescue Point of Contact Bermuda Search and Rescue Point of Contact Honduras Search and Rescue Point of Contact Colombia Search and Rescue Point of Contact Dominican Republic</p>
---	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Search and Rescue Point of Contact Ecuador Search and Rescue Point of Contact Guyana Search and Rescue Point of Contact Mexico Search and Rescue Point of Contact Panama Search and Rescue Point of Contact Venezuela Brazil Mission Control Center Canada Mission Control Center Peru Mission Control Center Chile Mission Control Center Argentina Mission Control Center	The information contained in the RGDB provides the RCC and MCC with the identity of the individual(s) they are searching for; contact information so that the RCC and MCC can determine whether or not the beacon has been activated as the result of an actual emergency; and information about the vessel or aircraft. The registration information allows the RCC and MCC to resolve a distress case by telephone instead of wasting valuable resources responding to false alerts.
No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.	

- 6.3 Identify the class of users who will have access to the IT system and the PII/BII. (*Check all that apply.*)

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

- 7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. (*Check all that apply.*)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://beaconregistration.noaa.gov/RGDB/	
	Yes, notice is provided by other means.	Specify how: Notice is provided on the registration forms.
	No, notice is not provided.	Specify why not:

- 7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Beacon owners can decline to provide the information, but then they would not be in compliance with 47 CFR Parts 80, 87 and 95 and also would not receive search and rescue services.
	No, individuals do not have an	Specify why not:

	opportunity to decline to provide PII/BII.	
--	--------------------------------------------	--

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Owners might indicate on their registration forms that they do not consent to particular uses of the information; however, they would then not be in compliance with the referenced regulations or be able to receive Search and Rescue activities.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: All information is provided by the beacon owner. Owners are able to update, change and remove data at any time via the password protected Web site or by sending hard copy notification to NOAA-SARSAT.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Logging is in place to record each attempted access attempt to PII/BII.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>06/14/2017</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

--	--

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Detailed audit logging is captured and stored on all devices used to access or store PII/BII. Encryption and hashing are used to protect the confidentiality and integrity of PII/BII in storage and in transmission.

NOAA5023 has internal software that connects to the database each time there is a new distress case to check if the associated beacon is registered. If the beacon is registered, the custom internal software attaches the registration data from the database to the alert that is sent to the appropriate rescue agency/agencies.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i> : An amended system of records notice, COMMERCE/NOAA-20, Search and Rescue Satellite Aided Tracking (SARSAT) 406 MHz Emergency Beacon Registration Database was published on January 12, 2017 (82 FR 3719).
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: The records are scheduled in the NOAA Records Disposition Handbook, item 1404-02, which provides for a 50-year retention of the electronic registration records. The schedule was approved by the National Archives and Records Administration (NARA) under Job Number N1-370-03-10.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Only non-sensitive PII is collected
	Quantity of PII	Provide explanation:
	Data Field Sensitivity	Provide explanation: There are no sensitive data fields.
x	Context of Use	Provide explanation: Ability to search and rescue based on PII.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Physical and logical access controls are in place to restrict access to PII

	Other:	Provide explanation:
--	--------	----------------------

Section 12: Analysis


12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: A Privacy Act Statement is being added to the registration Web page.
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

<p>Information System Security Officer or System Owner Name: Thomas Renkevens (System Owner) Office: NESDIS Phone: 301-683-3257 Email: thomas.renkevens@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: right;"> <small>Digitally signed by RENKEVENS.THOMAS.M.136583067 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=RENKEVENS THOMAS.M.136583067 Date: 2018.01.19 12:10:45 -0500</small></p> <p>Signature: <u>RENKEVENS.THOMAS.M.136583067</u> <small>37</small></p> <p>Date signed: <u>January 19, 2018</u></p>	<p>Information Technology Security Officer Name: Nancy A. DeFrancesco Office: NESDIS Phone: 240-429-0285 Email: nancy.defrancesco@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: right;"> <small>Digitally signed by DEFRANCESCO.NANCY.A.1377370917 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=DEFRANCESCO NANCY.A.1377370917 Date: 2018.01.24 07:01:12 -0500</small></p> <p>Signature: <u>DEFRANCESCO.NANCY.A.1377370917</u></p> <p>Date signed: <u>01/23/2018</u></p>
<p>Authorizing Official Name: Mark S. Paese Office: NESDIS Phone: 301-713-2010 Email: mark.paese@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: right;"> <small>Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.29 08:26:12 -0500</small></p> <p>Signature: <u></u></p> <p>Date signed: <u>1/25/18</u></p>	<p>Bureau Chief Privacy Officer Name: Office: Phone: Email:</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p style="text-align: right;"> <small>Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.29 08:26:12 -0500</small></p> <p>Signature: <u>GRAFF.MARK.HYRUM.1514447892</u> <small>K.HYRUM.1</small></p> <p>Date signed: <u>514447892</u></p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Monday, January 29, 2018 8:34 AM
To: Gioffre, Kathy (Federal); CPO
Cc: Mark Graff NOAA Federal; Chuck Baxley NOAA Federal; John D. Parker
Subject: NOAA6101 certification documents for DOC OPOG review ONLY CHANGE IS TO ATO DATE
Attachments: NOAA6101 PTA 2018 mhg.pdf; NOAA6101_PIA_1102018 LaVoi Signed mhg.pdf; NOAA6101 certification for MHG signature mhg.pdf

Kathy, attached are the PIA with updated ATO date, PTA and certification. All should be in order!

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751

Ce (b)(6)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NOAA6101_PIA

FISMA Name/ID (if different): NOAA6101

Name of IT System/ Program Owner: NOS Office for Coastal Management (OCM)

Name of Information System Security Officer: Chuck Baxley

Name of Authorizing Official(s): Jeffrey L. Payne

Date of Last PIA Compliance Review Board (CRB): 2-6-2017
(This date must be within three (3) years.)

Date of PIA Review: 1/10/2017

Name of Reviewer: Chuck Baxley

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BAXLEY.CHARLES.A.III.1058676264 Digitally signed by BAXLEY.CHARLES.A.III.1058676264
Date: 2018.01.10 10:39:53 -05'00'

Date of Privacy Act (PA) Review: _____

Name of Reviewer: _____

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: _____

Date of BCPO Review: 1/25/18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF MARK HYRUM 1514447892
DN c US, o U S Government, ou DoD, ou PKI,
ou OTHER, cn GRAFF MARK HYRUM 1514447892
Date 2018 01 25 17 21 18 -05'00'

U.S. Department of Commerce
[Bureau Name]



Privacy Threshold Analysis
for
NOAA6101

U.S. Department of Commerce Privacy Threshold Analysis

NOAA6101

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

System NOAA6101 is a general support system used to ensure that the Office for Coastal Management's (OCM's) scientific and internal administrative I operational needs are met. The system is an integrated collection of subsystems designed to provide general office automation, infrastructure, and connectivity services to the National Oceanic and Atmospheric Administration's (NOAA) Office for Coastal Management (OCM) located in Charleston, SC, Silver Spring, MD, Honolulu, HI, Stennis Space Center, MS, additional OCM field offices, and remote staff. The system enables OCM to achieve its mission, which is to support the environmental, social, and economic well-being of the coast by linking people, information, and technology. OCM assists the nation's coastal resource Management community by providing access to information, technology, and training, and by producing new tools and approaches that often can be applied nationwide.

Two of the component subsystems are the file servers and Web Application Subsystem (WAS). While the file servers store and serve up administrative and operational data, the WAS hosts and serves data-driven Web-based applications. Applications served from an internal Web server are accessible only to NOAA employees and contractors operating from within the NOAA network. These internal applications track information related to OCM's operations I administration. Applications served from public-facing Web servers may be intended for OCM and other subsets of OCM, NOAA, other federal agencies, customers, partners, and/or the public.

Questionnaire:

1. What is the status of this information system?

- This is a new information system. *Continue to answer questions and complete certification.*
- This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify):			

- This is an existing information system in which changes do not create new privacy risks. *Continue to answer questions, and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

- Yes. *Please describe the activities which may raise privacy concerns.*

Activities are focused on internal administrative efforts (employee information), web-based inquiries and information sharing, and business specific information (contracts, proposals, etc...). All are protected in ways detailed in the Privacy Impact Assessment (PIA) for NOAA 6101.

- No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

- Companies
 Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- DOC employees
 Contractors working on behalf of DOC
 Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

I certify the criteria implied by one or more of the questions above **apply** to the NOS Office for Coastal Management (OCM) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Chuck Baxley (ISSO)

Signature of ISSO or SO: BAXLEY.CHARLES.A.III.1058676264 Digitally signed by BAXLEY.CHARLES.A.III.1058676264 Date: 2018.01.10 11:08:07 -05'00'

Name of Information Technology Security Officer (ITSO): John D. Parker (ITSO)

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.01.24 08:14:31 -05'00'

Name of Authorizing Official (AO): Jeffrey L. Payne (AO)

Signature of AO: PAYNE.JEFFREY.L.DR.1365833881881 Digitally signed by PAYNE.JEFFREY.L.DR.1365833881 Date: 2018.01.10 17:55:59 -05'00'

Name of Bureau Chief Privacy Officer (BCPO): MARK GRAFF

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.25 17:12:54 -05'00'

**U.S. Department of Commerce
NOAA**



**Privacy Impact Assessment
For
NOAA 6101
Office for Coastal Management**

Reviewed by: _____ Mark Graff _____, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

**U.S. Department of Commerce Privacy Impact Assessment
NOAA 6101
Office for Coastal Management**

Unique Project Identifier: NOAA 6101

Introduction: System Description

The mission of the National Oceanic and Atmospheric Administration (NOAA)'s NOAA6101, Office for Coastal Management (OCM) is to catalyze and influence a broad base of leaders, citizens, and coastal practitioners to ensure healthy coastal ecosystems, resilient coastal communities, and vibrant and sustainable coastal economies. The coast and its residents are at the epicenter of the impacts of changes in weather, climate, demographics, and economies. OCM manages coastal resources and uses through strengthening governance and investments in the development and implementation of comprehensive policies, rules, and plans. OCM administers the Coastal Zone Management Act, the Coral Reef Conservation Act, the Deep Seabed Hard Mineral Resources Act of 1980, and the Ocean Thermal Energy Conversion Act of 1980.

NOAA6101 is a general support system used to ensure that the OCM's scientific and internal administrative / operational needs are met. The system is an integrated collection of subsystems designed to provide general office automation, infrastructure, and connectivity services to NOAA OCM staff located in Charleston, SC, Silver Spring, MD, Honolulu, HI, Stennis Space Center, MS, additional OCM field offices, and other remote locations. The system enables OCM to achieve its mission, which is to support the environmental, social, and economic well-being of the coast by linking people, information, and technology. OCM assists the nation's coastal resource management community by providing access to information, technology, and training, and by producing new tools and approaches that often can be applied nationwide.

The OCM Strategic Plan addresses three strategic outcomes for the coastal management community: healthy coastal ecosystems, resilient coastal communities, and vibrant and sustainable coastal economies.

OCM has both Personally Identifiable Information (PII) and Business Identifiable Information (BII) within its system boundary. This Privacy Impact Assessment (PIA) details the types of PII/BII found within the system boundary for NOAA 6101, and how that information is protected.

Two of the component subsystems are the internal networked file servers and web application servers. The file servers are restricted to OCM staff members and typically used for administrative and operational functions and/or storage such as:

- Administrative functions (replacing a manual process),
- Employee/Contractor information needed for personnel, security, performance evaluation, merit rewards, training, travel, etc.,
- Review of applicant information (e.g., information submitted in response to requests for proposals and/or in response to a solicitation),

- To track information, requests, tasks, actions, or processes related to the OCM / NOAA mission.

The OCM web servers host and serve web-based applications and sites. OCM’s web servers primarily serve publicly accessible information, which is intended for OCM and other subsets of OCM, NOAA, other federal agencies, customers, partners, and/or the general public. There are a few applications and sites that are intentionally restricted (authentication required) to NOAA employees and contractors operating from within the NOAA network. These internal applications track information related to OCM’s operations / administration (e.g., safety/emergency contacts).

A subset of web applications/sites served by OCM web servers is detailed in section 5.1 below.

Information sharing:

As stated in Sections 5.1 and 6.1, information is periodically shared within the bureau on a case-by-case basis. Additionally, non-sensitive POC information for certain subject matter experts is made available via the OCM web presence.

For verification of foreign visitor identity, information may be shared with NOAA Security and DHS FLETC.

5 U.S.C. § 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

15 U.S.C. § 1512 is an Organic Law which confers general powers and duties authority to executive agencies, vesting jurisdiction and control of departments, bureaus, offices and branches.

The Federal Information Processing Standard (FIPS) 199 security impact category for the system is Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

This is a new information system.

This is an existing information system with changes that create new privacy risks.

(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	
b. Anonymous to Non-Anonymous		e. New Public Access	
		g. New Interagency Uses	
		h. Internal Flow or Collection	

c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

- This is an existing information system in which changes do not create new privacy risks.

OCM made this choice in part because one FISMA system was absorbed into another during the Coastal Services Center (CSC) (NOAA6101) and Office for Ocean and Coastal Resource Management (OCRM) (NOAA6601) office integration, so there was no new system created. Additionally, OCM does not believe the types of information/data that were added to NOAA6101 were different from any of the already present information and data and imparted no new risks to 6101.

Section 2: Information in the System

- 2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (*Check all that apply.*)

Identifying Numbers (IN)					
a. Social Security*	x	e. File/Case ID		i. Credit Card	
b. Taxpayer ID	x	f. Driver's License		j. Financial Account	
c. Employer ID	x	g. Passport	x	k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: Social Security numbers are collected for new NOAA/NOS/OCM employees. <i>These are transmitted to the NOAA Security Office via secure electronic transmission and then destroyed.</i> OCM does <u>not</u> maintain them on the IT system or as hard copy files. Passport numbers are handled in the same way as SSNs. These procedures are detailed in the OCM Standard Operating Procedure-Personnel Security. This SOP will be included/referenced in the NOAA 6101 System Security Plan. Taxpayer or employer ID information is collected infrequently (see section 5.1 for more details), but is stored only temporarily on the system.					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	x	o. Medical Information	
d. Gender		j. Telephone Number	x	p. Military Service	
e. Age		k. Email Address	x	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): Employee information is collected for emergency/disaster/CoOP-related contact needs. General inquiries related to information sharing consist of collecting name and email address in order to respond to the information requests. Certain subject matter experts agree explicitly to share contact information (name, phone, email) on OCM's public web site.					

Work-Related Data (WRD)					
a. Occupation	x	d. Telephone Number	x	g. Salary	
b. Job Title	x	e. Email Address	x	h. Work History	
c. Work Address	x	f. Business Associates			
i. Other work-related data (specify): Work related data is collected and shared with employees for internal office communication purposes. Additionally, grant or contract proposal information often contains PII/BII, such as budgets or cost proposals; this information is only accessible to those involved in grant or contract-specific work activities, and only on a need-to-know basis. Additionally, all financial transactions take place outside of the OCM system (i.e., NOAA Finance, Grants Online handle financial transactions). See section 5.1 below for more details.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)					

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	x	Hard Copy: Mail/Fax	x	Online	x
Telephone	x	Email	x		
Other (specify):					

Government Sources					
Within the Bureau	x	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations	x	Private Sector	x	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify): OCM uses CAC cards like much of the federal government, but none of that data is stored on OCM's system.			

x	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
---	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	x
Video surveillance		Electronic purchase transactions	
Other (specify):			

Building entry readers recognize CAC cards used to gain entry, but do not store any of the data embedded on the card.

X	There are not any IT system supported activities which raise privacy risks/concerns.
---	--------------------------------------------------------------------------------------

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	x
For administrative matters	x	To promote information sharing initiatives	x
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	x	For web measurement and customization technologies (multi-session)	x
Other (specify):			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

PII is collected to communicate with OCM customers and stakeholders on topics where they have an explicitly expressed professional interest, or have made a specific request for data or information.

Other PII is collected for OCM staff employment and personnel records (federal/contractor) and OCM visitor access information (federal/contractor/member of the public/foreign national).

BII is collected and maintained for purposes such as contractual agreements and grants.

Details are found below.

NOAA's Office for Coastal Management Business Operations Division collects data containing personally identifiable and business identifiable information (BII) for internal government operations / administrative processes. The processes include:

- Employee / Contractor information needed for personnel, performance evaluation, merit rewards, training, travel, accident reporting, etc. This type of PII information is reviewed and updated annually by staff.
- Employee / Contractor / Visitors / Foreign National information required by DOC and/or OPM for security purposes and/or background checks. Passport numbers are collected for foreign visitors, sent as appropriate for security checks, and removed from the system. All information is required per DOC PII Policy and Foreign National Processing¹ guidance as well as the Federal Law Enforcement Training Center (FLETC) Foreign National Visitor Process.
- Employee / Contractor emergency contact information for use in call trees, Continuity of Operations Plan (COOP), etc. which includes names, phone numbers, and addresses
- Applicant information submitted in response to requests for proposals and/or in response to a solicitation

External grant applications/proposals are not typically collected by OCM. Per the NOAA Grants Management Office policy, proposals almost always run through the Grants.gov submission process and end up in the Grants Online system. In rare cases, applicants without access to the Internet [e.g., US

¹ [http://deemedexports.noaa.gov/Documents/Message on Electronic Transmission of PII.pdf](http://deemedexports.noaa.gov/Documents/Message_on_Electronic_Transmission_of_PII.pdf)

territories] are permitted to submit paper applications. When this happens, OCM scans the proposals and loads them into Grants Online. Any subsequent sharing of grant proposals via email for review must be done via a secure file transfer process (e.g., Grants Online, Accellion if emailing internally or externally to NOAA, a secure Google Drive or a network location for internal NOAA reviewers, or a password protected website for internal and external NOAA reviewers). Once reviews are complete and awards are made, proposals are removed from the OCM system and the Grants Online system is the official repository.

Typical personal or business identifiable information collected for grant applications includes:

- proposer's name
- email
- phone #
- organization name
- organization DUNS #
- employer identification number or taxpayer identification number

For acquisitions, the business identifiable information collected typically includes:

- proposer's name
- email
- phone #
- organization name
- organization DUNS #
- Cost proposal information is also collected, and would be considered sensitive BII, as it is often proprietary.
- Management and technical approaches found in vendor proposals is often considered BII.

Other PII that is being collected and/or made available via Internet / Web sites or applications include:

- PRiMO: Web site that publicly lists some partner organization POCs (name, organization, email, phone number), along with OCM POCs. POC information is entirely voluntary and can be removed at any time upon request.
- Coastal Storms Program: Web site that publicly lists some partner organization POCs (name, organization, email, phone number), along with OCM POCs. POC information is entirely voluntary and can be removed at any time upon request.
- OCM Intranet: Contains current information on staff, including phone numbers, names, email addresses, and emergency contacts. The system is used to maintain up

- to date records on staff contact information.
- Task Order Management Information System (TOMIS): Application that collects and maintains POC information (name, email, phone, company name) for use in administering various contractor tasks and deliverables.
 - National Estuarine Research Reserves: Web site that publicly lists some partner organization POCs (name, organization, email, phone number), along with OCM POCs. POC information is entirely voluntary and can be removed at any time upon request.
 - Estuaries Education: Web site that publicly lists some partner organization POCs (name, organization, email, phone number), along with OCM POCs. POC information is entirely voluntary and can be removed at any time upon request.
 - Digital Coast: Publishes contact information of trainers for some trainings listed on the Digital Coast Training page. Information includes (name, email, location). Permission is acquired (via a form) from each trainer before listing their information on the site.
 - Ocean Law Search: Web site related to underwater cultural heritage that makes various public laws, statutes, articles, and court case summaries via an online searchable interface. All of the information available is publicly accessible and has been assembled to focus on underwater cultural heritage. Some of the documents available contain names and addresses of legislators, attorneys, plaintiffs, or witnesses.
 - CAMMP: Application that assists in building grant proposals. Data collected from applicants includes (name, title, email, applicant personnel names and salaries for grant budgeting).
 - Coral DB: Application that collects internal NOAA staff proposals to the NOAA Corals matrix program.
 - Data in the Classroom: Web site that publicly lists some OCM POCs (one staff member name, with phone and email). POC information is entirely voluntary and can be removed at any time upon request. There is also a “contact us” page, which collects name, zip code, phone.
 - Data Access Viewer (DAV): Application that receives requests for data from the public. Email addresses are stored to provide a method of contacting the requester when the data is ready for pickup on the OCM FTP site.
 - Training Manager System: Web site that collects information on training courses, hosts and participants of OCM training programs. Information that is collected is not shared publicly. Fields collected include (name, organization, address, city, state, zip, email, phone).
 - OCM Point of Contact Management Database: Centralized contact management database used to maintain information from customers who have requested data or information, participated in conferences, requested products/materials, or attended meetings or trainings offered by OCM. This is a secure and centralized database.

Fields collected include (name, title, organization, address, city, state, zip, country, email, phone).

- National Estuarine Research Reserves (NERRs) Intranet is an authenticated application for NERRs and OCM staff to work collaboratively. Information collected includes name, organization, email, and phone number.
- NERRs and State Coastal Zone Management Performance Measures DBs are authenticated applications for NERRs and CZM partners to document grant performance measures in a standardized way, and to work collaboratively with OCM staff. Information collected includes name, organization, email, and phone number.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. (Check all that apply.)

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus			
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			x (only non-sensitive, point of contact information is shared, typically for subject matter experts who have agreed to share this information)
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

* DHS FLETC for verification of foreign visitor identity.

	The PII/BII in the system will not be shared.
--	-----------------------------------------------

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
x	No, this IT system does not connect with or receive information from another IT system(s) authorized to

process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. (*Check all that apply.*)

Class of Users			
General Public		Government Employees	x
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. (*Check all that apply.*)

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
x	<p>Yes, notice is provided by Privacy Act statements (five total) and/or privacy policy. The Privacy Act statements can all be found in the appendix below and also at:</p> <ul style="list-style-type: none"> • https://coast.noaa.gov/contactform/ (Contact Us) • OCM Intranet (access is restricted) (OCM Intranet) • Offline form (access is restricted) (Partner Contact Information) • Performance measure tracking system (access is restricted) (CZM Performance Measures) • NERRs Intranet and performance measure tracking system (access is restricted) (NERRs Intranet and Performance Measures) <p>The privacy policy can be found at: coast.noaa.gov/PrivacyPolicy/privacyPolicy.html .</p>	
x	Yes, notice is provided by other means.	<p>Specify how: Subject matter experts often provide contact information via the OCM public web site. Prior to making the POC information public, the subject matter experts are asked to fill out a form acknowledging that they will be providing this information on a public web site and that they agree to do so. A Privacy Act statement is also made available.</p> <p>Visitors to the OCM web presence can request information by providing minimal PII through an information request contact form. Individuals are under no obligation to provide this information, and the details of how this information is handled are readily available via the OCM Privacy Policy and a Privacy Act statement.</p> <p>OCM staff members (employees) are provided notice of how PII is used (i.e., emergency contact information in case of natural disasters) upon hire.</p> <p>Partners/grantees may provide contact information (PII) to participate in the NERRs Intranet site established for collaboration and to enter data into grantee performance measurement tracking systems.</p>

		Vendors and grantees are notified via solicitations and calls for proposals that BII will be collected as necessary to effectively evaluate proposals.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

x	Yes, individuals have an opportunity to decline to provide PII/BII.	<p>Specify how: Subject matter experts often provide contact information via the OCM public web site. Prior to making the POC information public, the subject matter experts are asked to fill out a form acknowledging that they will be providing this information on a public web site and that they agree to do so; all have the opportunity to decline to provide PII as it is an “opt in” scenario. A Privacy Act statement is also made available.</p> <p>Visitors to the OCM web presence can request information by providing minimal PII through an information request contact form. Individuals are under no obligation to provide this information, and the details of how this information is handled are readily available via the OCM Privacy Policy and a Privacy Act statement.</p> <p>Staff members provide PII upon hire as a condition of employment. A Privacy Act statement concerning usage of this information is made available to OCM staff members. They may decline to provide PII but this may affect their employment status.</p> <p>Partners/grantees may provide contact information (PII) to participate in the NERRs Intranet site established for collaboration and to enter data into grantee performance measurement tracking systems. Partners can decline to provide this information as it is an “opt in” scenario.</p> <p>Vendors and/or grantees provide BII when submitting proposals of various types. Proposers may decline to provide BII, by not including it in their proposals; however, that declination effectively removes them from consideration of contract or grant awards, as there are certain types of information that contain BII that are essential to a full and valid competition.</p>
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Subject matter experts who may be asked or offer to provide contact information are informed of exactly how and where on the OCM web site their contact information will be made available. A Privacy Act statement for this type of scenario is also available.
---	--------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>Visitors to the OCM web presence can learn how PII is used via the OCM Privacy Policy and make the choice to opt in to the particular stated uses. A Privacy Act statement for this type of scenario is also available.</p> <p>Staff members provide PII upon hire as a condition of employment. They may consent to only particular uses, but this may affect their employment. A Privacy Act statement for this type of scenario is also available.</p> <p>Partners/grantees who provide contact information (PII) to participate in the NERRs Intranet site established for collaboration or to enter data into grantee performance measurement tracking systems opt in to providing PII for the particular stated uses.</p> <p>For vendors and grantees, the only usage of the BII is during proposal review and subsequent consultation with vendors or grantees. The BII is not shared or disseminated beyond this scope.</p>
	<p>No, individuals do not have an opportunity to consent to particular uses of their PII/BII.</p>	<p>Specify why not:</p>

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

<p>x</p>	<p>Yes, individuals have an opportunity to review/update PII/BII pertaining to them.</p>	<p>Specify how: Subject matter experts who provide contact information on the OCM web site can review, update, or delete their PII upon request at any time.</p> <p>Web site visitors who provide PII via a request for information can request to review, update or delete the PII provided at any time.</p> <p>Staff members can update PII during performance reviews or via secure Intranet.</p> <p>Partners/grantees who provide contact information (PII) to participate in the NERRs Intranet site established for collaboration or to enter data into grantee performance measurement tracking systems can review, update, or delete their PII upon request at any time.</p> <p>Vendors or grantees can review/update BII at any time upon request to the NOS proposal contact.</p>
	<p>No, individuals do not have an opportunity to review/update PII/BII pertaining to them.</p>	<p>Specify why not:</p>

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. (*Check all that apply.*)

	All users signed a confidentiality agreement or non-disclosure agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access to PII is tracked via logging of network directory access; logging of secured database access; and logging of Intranet administrative access.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 5/3/2016 <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones. An independent A&A is scheduled for completion by March 2017. All findings will be analyzed and will undergo NOS POA&M Management Process that could result in risk acceptance or creation of a POA&M.
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

<p>Secured database</p> <ul style="list-style-type: none"> OCM secures PII data into a SQL Server database on a secured server. Databases are only accessible based on least privilege and job requirements. Access is limited to SQL Administrators and IT Staff that are authorized for administrative system access. The servers hosting the aforementioned databases exist in an access controlled internally hosted data center where physical access is monitored and granted exclusively based on position responsibilities. Non-privileged users are restricted to access via SQL Server accounts only. Information placed in the database is only accessed on a need-to-know basis by internal staff who are identified as needing access to this information. <p>Secured file/folder network directory</p> <ul style="list-style-type: none"> OCM enforces assigned authorizations for controlling access to the system through the use of logical access control policies. Access controls lists are configured to enforce access authorization and assign user and group privileges. These access

control policies are employed to control the access between users and objects (files, directories, servers, printers, etc.). Access enforcement mechanisms are in place at the network, system and application levels.

Plans for encryption at rest: OCM's SQL Server databases are SQL v 2012 Standard Edition. This version/edition does not allow for straightforward encryption and therefore the PII data stored in our secure database is not encrypted. We secure the database via access control and configuration management as stated above. OCM does intend to upgrade to SQL 2016 SP1 as soon as possible, and at latest, by 9/30/2017. This upgrade will provide a straightforward pathway to database encryption. In addition, we are actively engaged in moving applications and databases into Microsoft Azure which also provides automatic SQL DB encryption.

Section 9: Privacy Act

- 9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (*A new system of records notice (SORN) is required if the system is not covered by an existing SORN*).

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

x	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number (<i>list all that apply</i>): Existing Privacy Act system of records notices (SORNs) for NOAA cover the personnel information in this system: COMMERCE/DEPT-18 - Employees Personnel Files Not Covered by Notices of Other Agencies and NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission. Also, DEPT-2, Accounts Receivable; DEPT-6, Visitor Logs and Permits for Facilities under Department Control; DEPT-13, Investigative and Security Records; DEPT-25, Access Control and Identity Management System; and GSA/Govt-7, Federal Personal Identity Verification Identity Management System.
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

Section 10: Retention of Information

- 10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. (*Check all that apply.*)

x	There is an approved record control schedule. Provide the name of the record control schedule: The retention period for these records is guided by the
---	-----------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the federal government. The underlying paper records relating to employees are covered by GRS 1, Civilian Personnel Records. In accordance with GRS 20, item 3, electronic versions of records scheduled for disposal under other records schedules may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. Guidance for these records in the NOAA Records Schedules refers disposition to GRS 20.</p> <p>NOAA Records Schedules Chapter 1600 – National Ocean Service (NOS) Functional Files describes records created and maintained in the National Ocean Service (NOS) on the ocean and coastal zone management services and information products that support national needs arising from increasing uses and opportunities of the oceans and estuaries.</p> <p>1610-01 - Coastal Zone Management Program Documents 1610-02 - Program Change Files 1610-03 - Coastal Non-point Pollution Control Program 1610-04 - Federal Consistency 1610-05 - Program Administrative Guidance 1610-06 - The Coastal and Marine Management Program Information System</p>
	<p>No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:</p>
x	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	x	Overwriting	x
Degaussing	x	Deleting	x
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
x	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

x	Identifiability	Provide explanation: OCM only collects non-sensitive PII such as phone numbers and e-mail addresses. No SSNs or other sensitive PII/BIA information is electronically stored.
x	Quantity of PII	Provide explanation: Information collected is limited to a small subset of specific applications and personnel files.
x	Data Field Sensitivity	Provide explanation: Phone numbers and e-mail addresses are the primary information collected, and are used for communication purposes.
x	Context of Use	Provide explanation: The vast majority of PII collected is used for emergency contact information for staff members, or for communicating back to information requesters.
	Obligation to Protect Confidentiality	Provide explanation:
x	Access to and Location of PII	Provide explanation: Concept of least privilege; secure network and database; encrypted storage and transmission
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process change. Explanation: Addition of Privacy Act Statements to several sites.
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

X	Yes, the conduct of this PIA results in required technology changes Explanation: addition of Privacy Act Statements to several sites.
	No, the conduct of this PIA does not result in any required technology changes.

Appendix – Privacy Act Statements

NOAA OCM Privacy Act Statement (Contact Us)

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: NOAA Office for Coastal Management (OCM) collects this information for the purpose of responding to “contact us” form requests and subscriptions to newsletters from NOAA OCM websites.

Routine Uses: NOAA will use this information to respond to requests submitted on the Contact Us page and for subscriptions to newsletters as selected on the contact us form. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice Commerce/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA’s Mission.

Disclosure: Furnishing this information is voluntary.

NOAA OCM Privacy Act Statement (OCM Intranet)

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: NOAA Office for Coastal Management (OCM) collects this intranet information for employee emergency and administrative contact purposes.

Routine Uses: NOAA will use this information for emergency or administrative contact purposes. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among NOAA staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice Commerce/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA’s Mission.

Disclosure: Furnishing this information is voluntary.

NOAA OCM Privacy Act Statement (Partner Contact Information)

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: NOAA Office for Coastal Management (OCM) collects this information for the purpose of publishing the contact information of partners who provide services or resources on NOAA OCM websites.

Routine Uses: NOAA will use this information on public websites to identify points of contact for various resources listed on the NOAA Office for Coastal Management websites. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice Commerce/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.

Disclosure: Furnishing this information is voluntary.

NOAA OCM Privacy Act Statement (CZM Performance Measures)

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: NOAA Office for Coastal Management (OCM) collects this intranet information for user authentication, performance measurement project tracking and administrative contact purposes.

Routine Uses: NOAA will use this information for authentication, performance measurement project tracking and administrative contact purposes. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among NOAA staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice Commerce/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.

Disclosure: Furnishing this information is voluntary.

NOAA OCM Privacy Act Statement (NERRs Intranet and Performance Measures)

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: NOAA Office for Coastal Management (OCM) collects this intranet information for user authentication, organizational directory, performance measurement tracking, and administrative contact purposes.

Routine Uses: NOAA will use this information for authentication, organizational directory, employee emergency, and administrative contact purposes. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among NOAA staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice Commerce/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.

Disclosure: Furnishing this information is voluntary.

Points of Contact and Signatures

<p>Information System Security Officer or System Owner Name: Anthony A. LaVoi Office: NOAA/NOS/OCM Phone: 843-740-1274 Email: Tony.LaVoi@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>LAVOI.ANTHONY.A.1365862580 <small>Digitally signed by LAVOI.ANTHONY.A.1365862580 Date: 2018.01.25 10:50:31 -05'00'</small></p>	<p>Information Technology Security Officer Name: John Parker Office: NOAA/NOS Phone: 240-533-0832 Email: John.D.Parker@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>PARKER.JOHN.D.1365835914 <small>Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.01.24 15:28:59 -05'00'</small></p>
<p>Authorizing Official Name: Jeffrey L. Payne Office: NOAA/NOS/OCM Phone: 843-740-1207 Email: Jeff.Payne@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>PAYNE.JEFFREY.L.DR.1365833881 <small>Digitally signed by PAYNE.JEFFREY.L.DR.1365833881 Date: 2018.01.10 17:57:46 -05'00'</small></p>	<p>Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA/OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>GRAFF.MARK.HYRUM.1514447892 <small>Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.25 17:15:31 -05'00'</small></p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Tuesday, January 30, 2018 12:11 PM
To: Mark Graff NOAA Federal
Subject: Fwd: NOAA6001 Signed PTA
Attachments: NOAA6001 FY18 PTA 2018 1 30.pdf

NOAA6001 PTA for your signature (note in new template)

Thanks, Sarah

Forwarded message

From: Barbara Von mettenheim - NOAA Affiliate <barbara.vonmettenheim@noaa.gov>
Date: Tue, Jan 30, 2018 at 12:06 PM
Subject: NOAA6001 Signed PTA
To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>
Cc: "John D. Parker NOAA Federal" <john.d.parker@noaa.gov>, Jason MacMaster NOAA Federal <Jason.macmaster@noaa.gov>

Hi Sarah

All of the folks over here have signed. JParker, JMacMaster, Paul Scholz. Please forward the word version to me.

Thank you,
Barbara

Barbara von Mettenheim, PhD, CISSP
ERT contractor
NOAA
Alternate ISSO NOAA6001
(b)(6) cell
[240 533 0860](tel:2405330860), desk

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division

Office 301 628 5751

Ce (b)(6)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Mark Graff - NOAA Federal

From: Mark Graff NOAA Federal
Sent: Tuesday, January 30, 2018 12:37 PM
To: Sarah Brabson NOAA Federal
Subject: Re: NOAA6001 Signed PTA
Attachments: NOAA6001 FY18 PTA 2018 1 30 mhg.pdf

Signed and approved great.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Tue, Jan 30, 2018 at 12:10 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
NOAA6001 PTA for your signature (note in new template)

Thanks, Sarah

Forwarded message

From: **Barbara Von mettenheim - NOAA Affiliate** <barbara.vonmettenheim@noaa.gov>
Date: Tue, Jan 30, 2018 at 12:06 PM
Subject: NOAA6001 Signed PTA
To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>
Cc: "John D. Parker NOAA Federal" <john.d.parker@noaa.gov>, Jason MacMaster NOAA Federal <Jason.macmaster@noaa.gov>

Hi Sarah

All of the folks over here have signed. JParker, JMacMaster, Paul Scholz. Please forward the word version to me.

Thank you,
Barbara

Barbara von Mettenheim, PhD, CISSP
ERT contractor
NOAA

Alternate ISSO NOAA6001

(b)(6) cell
[240 533 0860](tel:2405330860), desk

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

**U.S. Department of Commerce
NOAA**



**Privacy Threshold Analysis
for the
NOS Enterprise Information System
(NOAA6001)**

U.S. Department of Commerce Privacy Threshold Analysis
NOS Enterprise Information System
(NOAA6001)

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction:

(a) *Whether it is a general support system, major application, or other type of system*

The National Ocean Service (NOS) Enterprise Information System (EIS) is an integrated collection of components designed to provide general office automation, infrastructure and connectivity services to NOS Headquarters and component program and staff offices either resident in Silver Spring, MD, or logically connected to the system through WAN links. NOAA6001 is the general support system for NOS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking. Other than this information, there are no applications or databases that collect or store employee PII.

(b) *System location* - Silver Spring, MD.

(c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)* This is a standalone system.

(d) *The purpose that the system is designed to serve* In addition to general purpose office automation support (file/printer sharing, application hosting, collaboration, etc.) provided by NOAA6001, the system provides help desk services and supports a number of internal web sites and a minor application which collects, stores and/or disseminates PII. NOAA6001 also stores BII information on file shares.

- **Constituents Database** PII, no BII The business owner, Policy and Constituent Affairs Division (PCAD), upgraded the Constituents Database to a newer version of .NET and encrypted the fields that house privacy data. This version addresses issues identified in the 2014 SCA assessment. This upgrade reduces the risk over the former version of the application.
- **GovDelivery** This is an online communications tool that delivers public information of interest by email to customers of NOS.
- **FedSelect** – This is a tool that stores proprietary/source selection information, used in the ProTech Oceans Domain Source Selection. This includes, but is not limited to, industry’s technical proposals, management schemes, price breakdowns, etc., as well as the Government’s evaluation of this data. Its purpose is to record and store data.

Source selection team members use FedSelect to review and record their evaluations of the proposals. It is also be used by the team as a whole to generate consensus evaluations of proposals. FedSelect derives its legal authority to collect PII and BII from the FAR Subpart 15.2 Solicitation and Receipt of Proposals and Information. FedSelect does not share any data in this system outside of NOAA. This application is going to be in production only for FY18. The data will be retained within the NOAA6001 boundary for up to five years post-award. The expected award date is 3-4th qtr. FY18. The fields that include PII are encrypted at rest.

- In NOS, the Local Registration Authority (LRA) is responsible for identity verification of NOS administrators that need to request public key infrastructure (PKI) certificates from DOD. This verification process uses form DD-2841 that requires the LRA to enter PII. This form is stored on the NOS network in a password protected zip file. The PII collected consists of the unique identification number from a federal government-issued identification credential with a picture, for example Military ID card or Passport card; the unique identification number from a non-federal government-issued identification card (for example, Driver License card). The form also contains common access card (CAC) card electronic data interchange personal identifier (EDIP), full name, work email, work phone number. Only the numbers are collected from the artifacts and stored in the system. The employee provides the information in person directly to the LRA who returns the artifacts to the user and does not store images of them on the system.

(e) *The way the system operates to achieve the purpose* - NOAA6001 groups elements of the system into three areas, each of which serves a distinct and specific function:

- Network Devices -- NOS SSMC (Silver Spring Metro Center) campus backbone and NOS Wide Area Network (WAN)
- NOS Domain Servers -- The NOS domain infrastructure components and Headquarters Local Area Network (File, Print, Application) services
- Web Application Servers -- NOS application and database hosting services

NOAA6001 has four websites using Tier 2 multi-session cookies that are not collecting PII. They are used for analytics and for improving the customer experience. The four sites are: [http:// oceanservice.noaa.gov](http://oceanservice.noaa.gov), [http:// oceantoday.noaa.gov](http://oceantoday.noaa.gov), <http://celebrating200years.noaa.gov> and <http://estuarinebathymetry.noaa.gov>.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO ([https:// policy.cio.gov/web-policy/analytics](https://policy.cio.gov/web-policy/analytics)), which states:

"A. All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

"C. Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

- (f) *A general description of the type of information collected, maintained, use, or disseminated by the system* - NOAA6001 systems collect non-sensitive PII and BII such as names, email addresses of individuals and businesses, financial information, and information related to hiring.
- (g) *Identify individuals who have access to information on the system* The users of the NOAA6001 systems that collect non-sensitive PII and BII are authorized government and contractor workers within the program office. These systems are not accessible to the general public
- (h) *How information in the system is retrieved by the user* - The information is retrieved through an application user interface, except for the data that is kept on the shared drives.
- (i) *How information is transmitted to and from the system* the information is manually input into the system by the administrator or through a bulk upload from a spreadsheet.

Questionnaire:

1. What is the status of this information system?

- This is a new information system. *Continue to answer questions and complete certification.*
- This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): The FedSelect application introduces a level of BII we have not had before. This temporary system will be disabled this fiscal year. The data will be retained within the NOAA6001 boundary for up to five years post award. The expected award date is 3-4 th qtr. FY18.					

- This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*
- This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *Please describe the activities which may raise privacy concerns.*

No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities - AAMB collects and stores limited BII from businesses or other entities that are providing proprietary information in support of a grant application or federal acquisition actions. Occasionally this is financial information included with the acquisition package.

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is “yes” to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

FedSelect Is an application that enables contracting evaluators to document their strength, weakness, and deficiency comments and their ratings and rationale electronically in one data file. Allows contracting officers and specialists to monitor the progress of an evaluation and move directly from individual evaluations to consensus. This system may contain

GovDelivery is used to send newsletters and information about NOS to stakeholders. The system collects email addresses of recipients, but not names or addresses.

The Constituents’ database collects limited PII from stakeholders involved with or interested in information provided by the National Ocean Service.

NOAA6001 collects and stores information related to the Office of the Assistant Administrator, Management and Budget (AAMB), which includes limited PII, specifically, names, telephone numbers and email addresses (voluntarily submitted by data providers and customers) to facilitate external coordination with data providers.

NOAA6001 stores PII on an ad-hoc basis as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

NOS has a Local Registration Authority (LRA) who is responsible for identity verification of NOS administrators that need to request public key infrastructure (PKI) certificates from DOD. This verification process uses form DD-2841 that requires the LRA to enter PII. This form is stored on the NOS network in a password protected zip file. The PII collected consists of the unique identification number from a federal government-issued identification credential with a picture, for example Military ID card or Passport card; the unique identification number from a non-federal government-issued identification card, for example Driver License card. The form also contains common access card (CAC) card electronic data interchange personal identifier (EDIP), full name, work email, work phone number. Only the numbers are collected from the artifacts and stored in the system. The LRA returns the artifacts to the user and does not store images of them on NOAA6001 systems.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the NOS Enterprise Information System and as a consequence of this applicability, I will perform and document a PIA for this IT system.

Name of Information System Security Officer (ISSO): Jason MacMaster

Signature of ISSO: MACMASTER.JASON.RICHARD.1096271197 Digitally signed by MACMASTER.JASON.RICHARD.1096271
Date: 2018.01.30 12:01:33 05'00' Date: _____

Name of Information Technology Security Officer (ITSO): John D. Parker

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914
Date: 2018.01.30 07:43:35 05'00' Date: _____

Name of Authorizing Official (AO): Paul Scholz

Signature of AO: SCHOLZ.PAUL.M.1365867239 Digitally signed by SCHOLZ.PAUL.M.1365867239
Date: 2018.01.30 08:22:55 05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892
DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892
Date: 2018.01.30 12:36:23 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Friday, February 2, 2018 3:07 PM
To: Ericka EvansSterling NOAA Affiliate
Cc: Nancy Defrancesco; Mark Graff NOAA Federal
Subject: Re NOAA5006 PIA
Attachments: PTA Template 01 2017_instructions corrected.docx; NOAA5006_051617.docx; PIA_Template_01 2017.docx

Hi, Ericka, you received NSOF system information this past year, correct?

If there had been no major changes, or as DOC says, 'no changes creating new privacy risks", we could have done a short certification, so hopefully we can do that next year.

But I see that you did say in your Sept PTA that it's not clear if there are new privacy risks. Is it clearer now?

If it can be argued that there are new privacy risks, we have a new PIA template on the Privacy Site, which mainly has a more detailed list of questions in the system description, and 3 4 additional free form questions.

Because the PTA was inconclusive, we should probably amend it to be in line with the PIA. New template for this also, attached and on the site. Similar laundry list of questions in the system description.

If you have determined no new risks, I can explain the certification process.

Here also is the Word version of the previously approved PIA. .

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751

Ce (b)(6)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

U.S. Department of Commerce
[Bureau Name]



Privacy Impact Assessment
for the
[IT System Name]

Reviewed by: _____, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment
[Name of Bureau/Name of IT System]

Unique Project Identifier: [Number]

Introduction: System Description

*Provide a description of the system that addresses the following elements:
 The response must be written in plain language and be as comprehensive as necessary to describe the system.*

- (a) Whether it is a general support system, major application, or other type of system*
- (b) System location*
- (c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
- (d) The way the system operates to achieve the purpose(s) identified in Section 4*
- (e) How information in the system is retrieved by the user*
- (f) How information is transmitted to and from the system*
- (g) Any information sharing conducted by the system*
- (h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*
- (i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system*

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- _____ This is a new information system.
- _____ This is an existing information system with changes that create new privacy risks.
 (Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify):			

- _____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

- 2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (*Check all that apply.*)

Identifying Numbers (IN)			
a. Social Security*		e. File/Case ID	i. Credit Card
b. Taxpayer ID		f. Driver's License	j. Financial Account
c. Employer ID		g. Passport	k. Financial Transaction
d. Employee ID		h. Alien Registration	l. Vehicle Identifier
m. Other identifying numbers (specify):			
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:			

General Personal Data (GPD)			
a. Name		g. Date of Birth	m. Religion
b. Maiden Name		h. Place of Birth	n. Financial Information
c. Alias		i. Home Address	o. Medical Information
d. Gender		j. Telephone Number	p. Military Service
e. Age		k. Email Address	q. Physical Characteristics
f. Race/Ethnicity		l. Education	r. Mother's Maiden Name
s. Other general personal data (specify):			

Work-Related Data (WRD)			
a. Occupation		d. Telephone Number	g. Salary
b. Job Title		e. Email Address	h. Work History
c. Work Address		f. Business Associates	
i. Other work-related data (specify):			

Distinguishing Features/Biometrics (DFB)			
a. Fingerprints		d. Photographs	g. DNA Profiles
b. Palm Prints		e. Scars, Marks, Tattoos	h. Retina/Iris Scans
c. Voice Recording/Signatures		f. Vascular Scan	i. Dental Profile
j. Other distinguishing features/biometrics (specify):			

System Administration/Audit Data (SAAD)			
a. User ID		c. Date/Time of Access	e. ID Files Accessed
b. IP Address		d. Queries Run	f. Contents of Files
g. Other system administration/audit data (specify):			

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		
Other (specify):					

Government Sources					
Within the Bureau	<input type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		
Other (specify):					

Non-government Sources					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input type="checkbox"/>		
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
	No, the information is not covered by the Paperwork Reduction Act.

- 2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

<input type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
--------------------------	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

- 3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

<input type="checkbox"/>	There are not any IT system supported activities which raise privacy risks/concerns.
--------------------------	--------------------------------------------------------------------------------------

Section 4: Purpose of the System

- 4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated

will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

- 5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	-----------------------------------------------

- 6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input type="checkbox"/>	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
<input type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

- 6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input type="checkbox"/>		<input type="checkbox"/>
Other (specify):			

Section 7: Notice and Consent

- 7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

<input type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
<input type="checkbox"/>	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement

	and/or privacy policy can be found at:	.
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a

	moderate or higher.
	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i>
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

	There is an approved record control schedule. Provide the name of the record control schedule:
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	<input type="checkbox"/>	Overwriting	<input type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input type="checkbox"/>
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

	Identifiability	Provide explanation:
	Quantity of PII	Provide explanation:
	Data Field Sensitivity	Provide explanation:
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:

	Other:	Provide explanation:
--	--------	----------------------

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

--	--

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

<p>Information System Security Officer or System Owner</p> <p>Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>Date signed:</p>	<p>Information Technology Security Officer</p> <p>Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>Date signed:</p>
<p>Authorizing Official</p> <p>Name: Office: Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature:</p> <p>Date signed:</p>	<p>Bureau Chief Privacy Officer</p> <p>Name: Office: Phone: Email:</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p>Signature:</p> <p>Date signed:</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

U.S. Department of Commerce
[Bureau Name]



Privacy Threshold Analysis
for the
[IT System Name]

U.S. Department of Commerce Privacy Threshold Analysis

[Name of Bureau/Name of IT System]

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

- a) *Whether it is a general support system, major application, or other type of system*
- b) *System location*
- c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
- d) *The purpose that the system is designed to serve*
- e) *The way the system operates to achieve the purpose*
- f) *A general description of the type of information collected, maintained, use, or disseminated by the system*
- g) *Identify individuals who have access to information on the system*
- h) *How information in the system is retrieved by the user*
- i) *How information is transmitted to and from the system*

Questionnaire:

1. What is the status of this information system?

_____ This is a new information system. *Continue to answer questions and complete certification.*

_____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

_____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Continue to answer questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

_____ Yes. *Please describe the activities which may raise privacy concerns.*

_____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the submitter has a commercial interest” and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.).”

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

- Companies
- Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- DOC employees
- Contractors working on behalf of DOC
- Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

_____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

_____ I certify the criteria implied by one or more of the questions above **apply** to the [IT SYSTEM NAME] and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Signature of ISSO or SO: _____ Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: _____ Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: _____ Date: _____

Name of Bureau Chief Privacy Officer (BCPO): _____

Signature of BCPO: _____ Date: _____

Purvis, Catrina (Federal)

Subject: NOAA6001 and NOAA6401
Location: Open Office 52017 (SMC) Md Conf Rm Good morning,
dial in information i (b)(6)
[REDACTED]

Start: Thursday, February 8, 2018 9:30 AM
End: Thursday, February 8, 2018 10:00 AM

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Purvis, Catrina (Federal)

Attachments: NOAA6001 FY18 PTA 2018 1 30 mhg.pdf; NOAA6001 PIA
final_for BCPO signature.pdf; NOAA6401 Privacy Threshold
Analysis (PTA) mhg.pdf; NOAA6401 Privacy Threshold
Analysis (PTA) mhg.pdf

Mark/Sarah,

Please ensure all required attendees are present at this telecom (dial in information i (b)(6)
[REDACTED] meeting, such as the ITSO, System Owner, etc., and other attendees who are
able to respond to questions related to the systems identified above.

*Also, if any of the systems are classified, please provide a hard copy of the SARs and POA&Ms for each system
identified above to Catrina Purvis 2 days prior to the meeting date.*

Warm Regards,

*Dorrie Ferguson,
Management and Program Analyst
Office of Privacy & Open Government
Error! Hyperlink reference not valid.
Office: (202) 482-8157*

—
—

**U.S. Department of Commerce
NOAA**



**Privacy Threshold Analysis
for the
NOS Enterprise Information System
(NOAA6001)**

U.S. Department of Commerce Privacy Threshold Analysis
NOS Enterprise Information System
(NOAA6001)

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction:

(a) *Whether it is a general support system, major application, or other type of system*

The National Ocean Service (NOS) Enterprise Information System (EIS) is an integrated collection of components designed to provide general office automation, infrastructure and connectivity services to NOS Headquarters and component program and staff offices either resident in Silver Spring, MD, or logically connected to the system through WAN links. NOAA6001 is the general support system for NOS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking. Other than this information, there are no applications or databases that collect or store employee PII.

(b) *System location* - Silver Spring, MD.

(c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)* This is a standalone system.

(d) *The purpose that the system is designed to serve* In addition to general purpose office automation support (file/printer sharing, application hosting, collaboration, etc.) provided by NOAA6001, the system provides help desk services and supports a number of internal web sites and a minor application which collects, stores and/or disseminates PII. NOAA6001 also stores BII information on file shares.

- **Constituents Database** PII, no BII The business owner, Policy and Constituent Affairs Division (PCAD), upgraded the Constituents Database to a newer version of .NET and encrypted the fields that house privacy data. This version addresses issues identified in the 2014 SCA assessment. This upgrade reduces the risk over the former version of the application.
- **GovDelivery** This is an online communications tool that delivers public information of interest by email to customers of NOS.
- **FedSelect** – This is a tool that stores proprietary/source selection information, used in the ProTech Oceans Domain Source Selection. This includes, but is not limited to, industry’s technical proposals, management schemes, price breakdowns, etc., as well as the Government’s evaluation of this data. Its purpose is to record and store data.

Source selection team members use FedSelect to review and record their evaluations of the proposals. It is also be used by the team as a whole to generate consensus evaluations of proposals. FedSelect derives its legal authority to collect PII and BII from the FAR Subpart 15.2 Solicitation and Receipt of Proposals and Information. FedSelect does not share any data in this system outside of NOAA. This application is going to be in production only for FY18. The data will be retained within the NOAA6001 boundary for up to five years post-award. The expected award date is 3-4th qtr. FY18. The fields that include PII are encrypted at rest.

- In NOS, the Local Registration Authority (LRA) is responsible for identity verification of NOS administrators that need to request public key infrastructure (PKI) certificates from DOD. This verification process uses form DD-2841 that requires the LRA to enter PII. This form is stored on the NOS network in a password protected zip file. The PII collected consists of the unique identification number from a federal government-issued identification credential with a picture, for example Military ID card or Passport card; the unique identification number from a non-federal government-issued identification card (for example, Driver License card). The form also contains common access card (CAC) card electronic data interchange personal identifier (EDIP), full name, work email, work phone number. Only the numbers are collected from the artifacts and stored in the system. The employee provides the information in person directly to the LRA who returns the artifacts to the user and does not store images of them on the system.

(e) *The way the system operates to achieve the purpose* - NOAA6001 groups elements of the system into three areas, each of which serves a distinct and specific function:

- Network Devices -- NOS SSMC (Silver Spring Metro Center) campus backbone and NOS Wide Area Network (WAN)
- NOS Domain Servers -- The NOS domain infrastructure components and Headquarters Local Area Network (File, Print, Application) services
- Web Application Servers -- NOS application and database hosting services

NOAA6001 has four websites using Tier 2 multi-session cookies that are not collecting PII. They are used for analytics and for improving the customer experience. The four sites are: [http:// oceanservice.noaa.gov](http://oceanservice.noaa.gov), [http:// oceantoday.noaa.gov](http://oceantoday.noaa.gov), <http://celebrating200years.noaa.gov> and <http://estuarinebathymetry.noaa.gov>.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO ([https:// policy.cio.gov/web-policy/analytics](https://policy.cio.gov/web-policy/analytics)), which states:

"A. All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

"C. Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

- (f) *A general description of the type of information collected, maintained, use, or disseminated by the system* - NOAA6001 systems collect non-sensitive PII and BII such as names, email addresses of individuals and businesses, financial information, and information related to hiring.
- (g) *Identify individuals who have access to information on the system* The users of the NOAA6001 systems that collect non-sensitive PII and BII are authorized government and contractor workers within the program office. These systems are not accessible to the general public
- (h) *How information in the system is retrieved by the user* - The information is retrieved through an application user interface, except for the data that is kept on the shared drives.
- (i) *How information is transmitted to and from the system* the information is manually input into the system by the administrator or through a bulk upload from a spreadsheet.

Questionnaire:

1. What is the status of this information system?

- This is a new information system. *Continue to answer questions and complete certification.*
- This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): The FedSelect application introduces a level of BII we have not had before. This temporary system will be disabled this fiscal year. The data will be retained within the NOAA6001 boundary for up to five years post award. The expected award date is 3-4 th qtr. FY18.					

- This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*
- This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *Please describe the activities which may raise privacy concerns.*

No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities - AAMB collects and stores limited BII from businesses or other entities that are providing proprietary information in support of a grant application or federal acquisition actions. Occasionally this is financial information included with the acquisition package.

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is “yes” to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

FedSelect Is an application that enables contracting evaluators to document their strength, weakness, and deficiency comments and their ratings and rationale electronically in one data file. Allows contracting officers and specialists to monitor the progress of an evaluation and move directly from individual evaluations to consensus. This system may contain

GovDelivery is used to send newsletters and information about NOS to stakeholders. The system collects email addresses of recipients, but not names or addresses.

The Constituents’ database collects limited PII from stakeholders involved with or interested in information provided by the National Ocean Service.

NOAA6001 collects and stores information related to the Office of the Assistant Administrator, Management and Budget (AAMB), which includes limited PII, specifically, names, telephone numbers and email addresses (voluntarily submitted by data providers and customers) to facilitate external coordination with data providers.

NOAA6001 stores PII on an ad-hoc basis as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

NOS has a Local Registration Authority (LRA) who is responsible for identity verification of NOS administrators that need to request public key infrastructure (PKI) certificates from DOD. This verification process uses form DD-2841 that requires the LRA to enter PII. This form is stored on the NOS network in a password protected zip file. The PII collected consists of the unique identification number from a federal government-issued identification credential with a picture, for example Military ID card or Passport card; the unique identification number from a non-federal government-issued identification card, for example Driver License card. The form also contains common access card (CAC) card electronic data interchange personal identifier (EDIP), full name, work email, work phone number. Only the numbers are collected from the artifacts and stored in the system. The LRA returns the artifacts to the user and does not store images of them on NOAA6001 systems.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the NOS Enterprise Information System and as a consequence of this applicability, I will perform and document a PIA for this IT system.

Name of Information System Security Officer (ISSO): Jason MacMaster

Signature of ISSO: MACMASTER.JASON.RICHARD.1096271197 Digitally signed by MACMASTER.JASON.RICHARD.1096271
Date: 2018.01.30 12:01:33 05'00' Date: _____

Name of Information Technology Security Officer (ITSO): John D. Parker

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914
Date: 2018.01.30 07:43:35 05'00' Date: _____

Name of Authorizing Official (AO): Paul Scholz

Signature of AO: SCHOLZ.PAUL.M.1365867239 Digitally signed by SCHOLZ.PAUL.M.1365867239
Date: 2018.01.30 08:22:55 05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892
DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892
Date: 2018.01.30 12:36:23 -05'00' Date: _____

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

U.S. Department of Commerce
NOAA
National Geodetic Survey



Privacy Threshold Analysis
for
National Geodetic Survey General Support System
(NOAA6401)

Template version 2015-001

U.S. Department of Commerce Privacy Threshold Analysis
NOAA/National Geodetic Survey General Support System
(NOAA6401)

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: The mission of the National Geodetic Survey (NGS) is to define, maintain and provide access to the National Spatial Reference System (NSRS) to meet our nation's economic, social, and environmental needs.

NGS provides the framework for all positioning activities in the Nation. The foundational elements - latitude, longitude, elevation and shoreline information - contribute to informed decision making and impact a wide range of important activities including mapping and charting, flood risk determination, transportation, land use and ecosystem management. NGS' authoritative spatial data, models and tools are vital for the protection and management of natural and manmade resources and support the economic prosperity and environmental health of the Nation.

The major NGS projects and services are Continuously Operating Reference Stations (CORS), Height Modernization, Gravity for the Redefinition of the American Vertical Datum (GRAV-D), Airport Surveys, Online Positioning User Service (OPUS), Vertical Datum Transformation (VDatum), Global Positioning System (GPS) Satellites Orbits, Shoreline Mapping, State Advisor Program, and Emergency Response Imagery (ERI). NOAA6401 also provides general office automation, geosciences research, and training workshops.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

_____ This is a new information system. *Continue to answer questions and complete certification.*

This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify): We now have expanded our collection of aerial data to include UAS. Although not a change, we now recognize that we do store BII data related to acquisitions. We also have video surveillance at one facility. See details in Question 2.			

_____ This is an existing information system in which changes do not create new privacy risks. *Continue to answer questions, and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *Please describe the activities which may raise privacy concerns.*

NGS has for many years collected aerial imagery to support its mission, in the last year this has expanded to include UAS collected data. We now have video surveillance system for physical security purposes at our Norfolk, VA facility.

_____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities. *NOAA6401 collects and stores limited BII from businesses or other entities that are providing proprietary information in support of a grant application or federal acquisition actions. Occasionally this is financial information included with the acquisition package*

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID. *NOAA6401 stores PII on an ad-hoc basis as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes*

and hiring ranking are stored temporarily during the hiring phase; in addition, the system stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking. External data providers and/or customers may voluntarily share one or more of the following information types: name, telephone number and/or email address to facilitate coordination with them.

_____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

_____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

I certify the criteria implied by one or more of the questions above **apply** to the **National Geodetic Survey General Support System** and as a consequence of this applicability, I will perform and document a PIA for this IT system.

____ I certify the criteria implied by the questions above **do not apply** to the **National Geodetic Survey General Support System** and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Giovanni Sella (ISSO)

Signature of ISSO or SO: SELLA.GIOVANNI.FEDERICO.1365835140 Digitally signed by SELLA.GIOVANNI.FEDERICO.1365835140 Date: 2017.11.09 08:43:56 -05'00'

Name of Information Technology Security Officer (ITSO): John D. Parker (ITSO)

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2017.11.09 09:11:48 -05'00'

Name of Authorizing Official (AO):Juliana Blackwell (AO)

Signature of AO: Juliana P. Blackwell Digitally signed by BLACKWELLJULIANAP.1043590622 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=BLACKWELLJULIANAP.1043590622 Date: 2017.11.13 07:55:02 05'00'

Name of Bureau Chief Privacy Officer (BCPO): MARK GRAFF (BCPO)

Signature of BCPO: GRAFF.MARK.HYRUM.151447892 Digitally signed by GRAFF.MARK.HYRUM.151447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.151447892 Date: 2017.11.13 14:37:53 05'00'

U.S. Department of Commerce
NOAA
National Geodetic Survey



Privacy Threshold Analysis
for
National Geodetic Survey General Support System
(NOAA6401)

Template version 2015-001

U.S. Department of Commerce Privacy Threshold Analysis
NOAA/National Geodetic Survey General Support System
(NOAA6401)

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: The mission of the National Geodetic Survey (NGS) is to define, maintain and provide access to the National Spatial Reference System (NSRS) to meet our nation's economic, social, and environmental needs.

NGS provides the framework for all positioning activities in the Nation. The foundational elements - latitude, longitude, elevation and shoreline information - contribute to informed decision making and impact a wide range of important activities including mapping and charting, flood risk determination, transportation, land use and ecosystem management. NGS' authoritative spatial data, models and tools are vital for the protection and management of natural and manmade resources and support the economic prosperity and environmental health of the Nation.

The major NGS projects and services are Continuously Operating Reference Stations (CORS), Height Modernization, Gravity for the Redefinition of the American Vertical Datum (GRAV-D), Airport Surveys, Online Positioning User Service (OPUS), Vertical Datum Transformation (VDatum), Global Positioning System (GPS) Satellites Orbits, Shoreline Mapping, State Advisor Program, and Emergency Response Imagery (ERI). NOAA6401 also provides general office automation, geosciences research, and training workshops.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

_____ This is a new information system. *Continue to answer questions and complete certification.*

This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify): We now have expanded our collection of aerial data to include UAS. Although not a change, we now recognize that we do store BII data related to acquisitions. We also have video surveillance at one facility. See details in Question 2.			

_____ This is an existing information system in which changes do not create new privacy risks. *Continue to answer questions, and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *Please describe the activities which may raise privacy concerns.*

NGS has for many years collected aerial imagery to support its mission, in the last year this has expanded to include UAS collected data. We now have video surveillance system for physical security purposes at our Norfolk, VA facility.

_____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities. *NOAA6401 collects and stores limited BII from businesses or other entities that are providing proprietary information in support of a grant application or federal acquisition actions. Occasionally this is financial information included with the acquisition package*

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID. *NOAA6401 stores PII on an ad-hoc basis as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes*

and hiring ranking are stored temporarily during the hiring phase; in addition, the system stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking. External data providers and/or customers may voluntarily share one or more of the following information types: name, telephone number and/or email address to facilitate coordination with them.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

I certify the criteria implied by one or more of the questions above **apply** to the **National Geodetic Survey General Support System** and as a consequence of this applicability, I will perform and document a PIA for this IT system.

____ I certify the criteria implied by the questions above **do not apply** to the **National Geodetic Survey General Support System** and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Giovanni Sella (ISSO)

Signature of ISSO or SO: SELLA.GIOVANNI.FEDERICO.1365835140
Digitally signed by SELLA.GIOVANNI.FEDERICO.1365835140
Date: 2017.11.09 08:43:56 -05'00'

Name of Information Technology Security Officer (ITSO): John D. Parker (ITSO)

Signature of ITSO: PARKER.JOHN.D.1365835914
Digitally signed by PARKER.JOHN.D.1365835914
Date: 2017.11.09 09:11:48 -05'00'

Name of Authorizing Official (AO):Juliana Blackwell (AO)

Signature of AO: Juliana P. Blackwell
Digitally signed by BLACKWELLJULIANAP.1043590622
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=BLACKWELLJULIANAP.1043590622
Date: 2017.11.13 07:55:02 05'00'

Name of Bureau Chief Privacy Officer (BCPO): MARK GRAFF (BCPO)

Signature of BCPO: GRAFF.MARK.HYRUM.151447892
Digitally signed by GRAFF.MARK.HYRUM.151447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.151447892
Date: 2017.11.13 14:37:53 05'00'

Purvis, Catrina (Federal)

Subject: NOAA6001 and NOAA6401
Location: Open Office 52017 (SMC) Md Conf Rm Good morning,
dial in information i (b)(6)
[REDACTED]

Start: Thursday, February 8, 2018 9:30 AM
End: Thursday, February 8, 2018 10:30 AM

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Purvis, Catrina (Federal)

Attachments: NOAA6001 FY18 PTA 2018 1 30 mhg.pdf; NOAA6001 PIA
final_for BCPO signature.pdf; NOAA6401 Privacy Threshold
Analysis (PTA) mhg.pdf; NOAA6401 Privacy Threshold
Analysis (PTA) mhg.pdf

Mark/Sarah,

Please ensure all required attendees are present at this telecom (dial in information i (b)(6)
[REDACTED] meeting, such as the ITSO, System Owner, etc., and other attendees who are
able to respond to questions related to the systems identified above.

*Also, if any of the systems are classified, please provide a hard copy of the SARs and POA&Ms for each system
identified above to Catrina Purvis 2 days prior to the meeting date.*

Warm Regards,

*Dorrie Ferguson,
Management and Program Analyst
Office of Privacy & Open Government
Error! Hyperlink reference not valid.
Office: (202) 482-8157*

—
—

**U.S. Department of Commerce
NOAA**



**Privacy Threshold Analysis
for the
NOS Enterprise Information System
(NOAA6001)**

U.S. Department of Commerce Privacy Threshold Analysis
NOS Enterprise Information System
(NOAA6001)

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction:

(a) *Whether it is a general support system, major application, or other type of system*

The National Ocean Service (NOS) Enterprise Information System (EIS) is an integrated collection of components designed to provide general office automation, infrastructure and connectivity services to NOS Headquarters and component program and staff offices either resident in Silver Spring, MD, or logically connected to the system through WAN links. NOAA6001 is the general support system for NOS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking. Other than this information, there are no applications or databases that collect or store employee PII.

(b) *System location* - Silver Spring, MD.

(c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)* This is a standalone system.

(d) *The purpose that the system is designed to serve* In addition to general purpose office automation support (file/printer sharing, application hosting, collaboration, etc.) provided by NOAA6001, the system provides help desk services and supports a number of internal web sites and a minor application which collects, stores and/or disseminates PII. NOAA6001 also stores BII information on file shares.

- **Constituents Database** PII, no BII The business owner, Policy and Constituent Affairs Division (PCAD), upgraded the Constituents Database to a newer version of .NET and encrypted the fields that house privacy data. This version addresses issues identified in the 2014 SCA assessment. This upgrade reduces the risk over the former version of the application.
- **GovDelivery** This is an online communications tool that delivers public information of interest by email to customers of NOS.
- **FedSelect** – This is a tool that stores proprietary/source selection information, used in the ProTech Oceans Domain Source Selection. This includes, but is not limited to, industry’s technical proposals, management schemes, price breakdowns, etc., as well as the Government’s evaluation of this data. Its purpose is to record and store data.

Source selection team members use FedSelect to review and record their evaluations of the proposals. It is also be used by the team as a whole to generate consensus evaluations of proposals. FedSelect derives its legal authority to collect PII and BII from the FAR Subpart 15.2 Solicitation and Receipt of Proposals and Information. FedSelect does not share any data in this system outside of NOAA. This application is going to be in production only for FY18. The data will be retained within the NOAA6001 boundary for up to five years post-award. The expected award date is 3-4th qtr. FY18. The fields that include PII are encrypted at rest.

- In NOS, the Local Registration Authority (LRA) is responsible for identity verification of NOS administrators that need to request public key infrastructure (PKI) certificates from DOD. This verification process uses form DD-2841 that requires the LRA to enter PII. This form is stored on the NOS network in a password protected zip file. The PII collected consists of the unique identification number from a federal government-issued identification credential with a picture, for example Military ID card or Passport card; the unique identification number from a non-federal government-issued identification card (for example, Driver License card). The form also contains common access card (CAC) card electronic data interchange personal identifier (EDIP), full name, work email, work phone number. Only the numbers are collected from the artifacts and stored in the system. The employee provides the information in person directly to the LRA who returns the artifacts to the user and does not store images of them on the system.

(e) *The way the system operates to achieve the purpose* - NOAA6001 groups elements of the system into three areas, each of which serves a distinct and specific function:

- Network Devices -- NOS SSMC (Silver Spring Metro Center) campus backbone and NOS Wide Area Network (WAN)
- NOS Domain Servers -- The NOS domain infrastructure components and Headquarters Local Area Network (File, Print, Application) services
- Web Application Servers -- NOS application and database hosting services

NOAA6001 has four websites using Tier 2 multi-session cookies that are not collecting PII. They are used for analytics and for improving the customer experience. The four sites are: [http:// oceanservice.noaa.gov](http://oceanservice.noaa.gov), [http:// oceantoday.noaa.gov](http://oceantoday.noaa.gov), <http://celebrating200years.noaa.gov> and <http://estuarinebathymetry.noaa.gov>.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO ([https:// policy.cio.gov/web-policy/analytics](https://policy.cio.gov/web-policy/analytics)), which states:

"A. All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

"C. Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

- (f) *A general description of the type of information collected, maintained, use, or disseminated by the system* - NOAA6001 systems collect non-sensitive PII and BII such as names, email addresses of individuals and businesses, financial information, and information related to hiring.
- (g) *Identify individuals who have access to information on the system* The users of the NOAA6001 systems that collect non-sensitive PII and BII are authorized government and contractor workers within the program office. These systems are not accessible to the general public
- (h) *How information in the system is retrieved by the user* - The information is retrieved through an application user interface, except for the data that is kept on the shared drives.
- (i) *How information is transmitted to and from the system* the information is manually input into the system by the administrator or through a bulk upload from a spreadsheet.

Questionnaire:

1. What is the status of this information system?

- This is a new information system. *Continue to answer questions and complete certification.*
- This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): The FedSelect application introduces a level of BII we have not had before. This temporary system will be disabled this fiscal year. The data will be retained within the NOAA6001 boundary for up to five years post award. The expected award date is 3-4 th qtr. FY18.					

- This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*
- This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *Please describe the activities which may raise privacy concerns.*

No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities - AAMB collects and stores limited BII from businesses or other entities that are providing proprietary information in support of a grant application or federal acquisition actions. Occasionally this is financial information included with the acquisition package.

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

_____ No, this IT system does not collect any PII.

If the answer is “yes” to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

FedSelect Is an application that enables contracting evaluators to document their strength, weakness, and deficiency comments and their ratings and rationale electronically in one data file. Allows contracting officers and specialists to monitor the progress of an evaluation and move directly from individual evaluations to consensus. This system may contain

GovDelivery is used to send newsletters and information about NOS to stakeholders. The system collects email addresses of recipients, but not names or addresses.

The Constituents’ database collects limited PII from stakeholders involved with or interested in information provided by the National Ocean Service.

NOAA6001 collects and stores information related to the Office of the Assistant Administrator, Management and Budget (AAMB), which includes limited PII, specifically, names, telephone numbers and email addresses (voluntarily submitted by data providers and customers) to facilitate external coordination with data providers.

NOAA6001 stores PII on an ad-hoc basis as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

NOS has a Local Registration Authority (LRA) who is responsible for identity verification of NOS administrators that need to request public key infrastructure (PKI) certificates from DOD. This verification process uses form DD-2841 that requires the LRA to enter PII. This form is stored on the NOS network in a password protected zip file. The PII collected consists of the unique identification number from a federal government-issued identification credential with a picture, for example Military ID card or Passport card; the unique identification number from a non-federal government-issued identification card, for example Driver License card. The form also contains common access card (CAC) card electronic data interchange personal identifier (EDIP), full name, work email, work phone number. Only the numbers are collected from the artifacts and stored in the system. The LRA returns the artifacts to the user and does not store images of them on NOAA6001 systems.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the NOS Enterprise Information System and as a consequence of this applicability, I will perform and document a PIA for this IT system.

Name of Information System Security Officer (ISSO): Jason MacMaster

Signature of ISSO: MACMASTER.JASON.RICHARD.1096271197 Digitally signed by MACMASTER.JASON.RICHARD.1096271
Date: 2018.01.30 12:01:33 05'00' Date: _____

Name of Information Technology Security Officer (ITSO): John D. Parker

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914
Date: 2018.01.30 07:43:35 05'00' Date: _____

Name of Authorizing Official (AO): Paul Scholz

Signature of AO: SCHOLZ.PAUL.M.1365867239 Digitally signed by SCHOLZ.PAUL.M.1365867239
Date: 2018.01.30 08:22:55 05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892
DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892
Date: 2018.01.30 12:36:23 -05'00' Date: _____

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

U.S. Department of Commerce
NOAA
National Geodetic Survey



Privacy Threshold Analysis
for
National Geodetic Survey General Support System
(NOAA6401)

Template version 2015-001

U.S. Department of Commerce Privacy Threshold Analysis
NOAA/National Geodetic Survey General Support System
(NOAA6401)

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: The mission of the National Geodetic Survey (NGS) is to define, maintain and provide access to the National Spatial Reference System (NSRS) to meet our nation's economic, social, and environmental needs.

NGS provides the framework for all positioning activities in the Nation. The foundational elements - latitude, longitude, elevation and shoreline information - contribute to informed decision making and impact a wide range of important activities including mapping and charting, flood risk determination, transportation, land use and ecosystem management. NGS' authoritative spatial data, models and tools are vital for the protection and management of natural and manmade resources and support the economic prosperity and environmental health of the Nation.

The major NGS projects and services are Continuously Operating Reference Stations (CORS), Height Modernization, Gravity for the Redefinition of the American Vertical Datum (GRAV-D), Airport Surveys, Online Positioning User Service (OPUS), Vertical Datum Transformation (VDatum), Global Positioning System (GPS) Satellites Orbits, Shoreline Mapping, State Advisor Program, and Emergency Response Imagery (ERI). NOAA6401 also provides general office automation, geosciences research, and training workshops.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

_____ This is a new information system. *Continue to answer questions and complete certification.*

This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify): We now have expanded our collection of aerial data to include UAS. Although not a change, we now recognize that we do store BII data related to acquisitions. We also have video surveillance at one facility. See details in Question 2.			

_____ This is an existing information system in which changes do not create new privacy risks. *Continue to answer questions, and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *Please describe the activities which may raise privacy concerns.*

NGS has for many years collected aerial imagery to support its mission, in the last year this has expanded to include UAS collected data. We now have video surveillance system for physical security purposes at our Norfolk, VA facility.

_____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities. *NOAA6401 collects and stores limited BII from businesses or other entities that are providing proprietary information in support of a grant application or federal acquisition actions. Occasionally this is financial information included with the acquisition package*

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID. *NOAA6401 stores PII on an ad-hoc basis as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes*

and hiring ranking are stored temporarily during the hiring phase; in addition, the system stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking. External data providers and/or customers may voluntarily share one or more of the following information types: name, telephone number and/or email address to facilitate coordination with them.

_____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

_____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

I certify the criteria implied by one or more of the questions above **apply** to the **National Geodetic Survey General Support System** and as a consequence of this applicability, I will perform and document a PIA for this IT system.

____ I certify the criteria implied by the questions above **do not apply** to the **National Geodetic Survey General Support System** and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Giovanni Sella (ISSO)

Signature of ISSO or SO: SELLA.GIOVANNI.FEDERICO.1365835140
Digitally signed by SELLA.GIOVANNI.FEDERICO.1365835140
Date: 2017.11.09 08:43:56 -05'00'

Name of Information Technology Security Officer (ITSO): John D. Parker (ITSO)

Signature of ITSO: PARKER.JOHN.D.1365835914
Digitally signed by PARKER.JOHN.D.1365835914
Date: 2017.11.09 09:11:48 -05'00'

Name of Authorizing Official (AO):Juliana Blackwell (AO)

Signature of AO: Juliana P. Blackwell
Digitally signed by BLACKWELLJULIANAP.1043590622
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=BLACKWELLJULIANAP.1043590622
Date: 2017.11.13 07:55:02 05'00'

Name of Bureau Chief Privacy Officer (BCPO): MARK GRAFF (BCPO)

Signature of BCPO: GRAFF.MARK.HYRUM.151447892
47892
Digitally signed by GRAFF.MARK.HYRUM.151447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.151447892
Date: 2017.11.13 14:37:53 05'00'

U.S. Department of Commerce
NOAA
National Geodetic Survey



Privacy Threshold Analysis
for
National Geodetic Survey General Support System
(NOAA6401)

Template version 2015-001

U.S. Department of Commerce Privacy Threshold Analysis
NOAA/National Geodetic Survey General Support System
(NOAA6401)

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: The mission of the National Geodetic Survey (NGS) is to define, maintain and provide access to the National Spatial Reference System (NSRS) to meet our nation's economic, social, and environmental needs.

NGS provides the framework for all positioning activities in the Nation. The foundational elements - latitude, longitude, elevation and shoreline information - contribute to informed decision making and impact a wide range of important activities including mapping and charting, flood risk determination, transportation, land use and ecosystem management. NGS' authoritative spatial data, models and tools are vital for the protection and management of natural and manmade resources and support the economic prosperity and environmental health of the Nation.

The major NGS projects and services are Continuously Operating Reference Stations (CORS), Height Modernization, Gravity for the Redefinition of the American Vertical Datum (GRAV-D), Airport Surveys, Online Positioning User Service (OPUS), Vertical Datum Transformation (VDatum), Global Positioning System (GPS) Satellites Orbits, Shoreline Mapping, State Advisor Program, and Emergency Response Imagery (ERI). NOAA6401 also provides general office automation, geosciences research, and training workshops.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

This is a new information system. *Continue to answer questions and complete certification.*

This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify): We now have expanded our collection of aerial data to include UAS. Although not a change, we now recognize that we do store BII data related to acquisitions. We also have video surveillance at one facility. See details in Question 2.			

This is an existing information system in which changes do not create new privacy risks. *Continue to answer questions, and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *Please describe the activities which may raise privacy concerns.*

NGS has for many years collected aerial imagery to support its mission, in the last year this has expanded to include UAS collected data. We now have video surveillance system for physical security purposes at our Norfolk, VA facility.

No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities. *NOAA6401 collects and stores limited BII from businesses or other entities that are providing proprietary information in support of a grant application or federal acquisition actions. Occasionally this is financial information included with the acquisition package*

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID. *NOAA6401 stores PII on an ad-hoc basis as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes*

and hiring ranking are stored temporarily during the hiring phase; in addition, the system stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking. External data providers and/or customers may voluntarily share one or more of the following information types: name, telephone number and/or email address to facilitate coordination with them.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

I certify the criteria implied by one or more of the questions above **apply** to the **National Geodetic Survey General Support System** and as a consequence of this applicability, I will perform and document a PIA for this IT system.

____ I certify the criteria implied by the questions above **do not apply** to the **National Geodetic Survey General Support System** and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Giovanni Sella (ISSO)

Signature of ISSO or SO: SELLA.GIOVANNI.FEDERICO.1365835140 Digitally signed by SELLA.GIOVANNI.FEDERICO.1365835140 Date: 2017.11.09 08:43:56 -05'00'

Name of Information Technology Security Officer (ITSO): John D. Parker (ITSO)

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2017.11.09 09:11:48 -05'00'

Name of Authorizing Official (AO):Juliana Blackwell (AO)

Signature of AO: Juliana P. Blackwell Digitally signed by BLACKWELLJULIANAP.1043590622 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=BLACKWELL.JULIANAP.1043590622 Date: 2017.11.13 07:55:02 05'00'

Name of Bureau Chief Privacy Officer (BCPO): MARK GRAFF (BCPO)

Signature of BCPO: GRAFF.MARK.HYRUM.151447892 Digitally signed by GRAFF.MARK.HYRUM.151447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.151447892 Date: 2017.11.13 14:37:53 05'00'

Purvis, Catrina (Federal)

Subject: Privacy Council Face to Face Meeting
Location: Rooms 12015/12017 HCHB

Start: Tuesday, February 6, 2018 8:30 AM
End: Tuesday, February 6, 2018 12:30 PM

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Purvis, Catrina (Federal)

Attachments: Privacy Council F 2 F Agenda 02 06 18.docx; CD 15 Transmittal and Routing Form.pdf; Digital Privacy Report Template.pdf; DIGITAL PRIVACY REPORT.docx; Federal Privacy Updates.docx; GDPR Background 11 17.docx; Guide to Conducting a PII Breach Table Top Exercise.docx; Identity Protection Services from GSA.docx; OMB Memo 16 14 (Identity Protection Services).pdf; SSN Collection and Mailing (002).docx; Upcoming Data Call.docx

Sending attachments

Due to the weather conditions expected tomorrow morning, the Privacy Council meeting is being rescheduled from Tuesday, January 30, 2018, to Tuesday, February 6, 2018, from 8:30 a.m. to 12:30 p.m.

If the Bureau Chief Privacy Officer cannot participate in this meeting, please ensure your bureau/operating unit has representation with the authority to make decisions on your bureau's/operating unit's behalf.

Below is the WebEx Conference/Telecom information for this meeting:

Meeting Number: (b)(6)
Meeting Host: Tahira Murphy

Join instructions for Instant Net Conference:








1. Join the meeting now: **Error! Hyperlink reference not valid.**
2. Enter the required fields
3. Indicate that you have read the Privacy Policy
4. Click on Proceed

Privacy Council Telecom Dial In: (b)(6)
Participant Passcode: (b)(6)






FORM CD-15 (12 6 73) PRESCR. BY TRANSMIT/ROUTE DAO 214 2		U.S. DEPARTMENT OF COMMERCE		DATE 01/24/2018		
NAME	BUILDING, ROOM OR REFERENCE NO.	TAKE ACTION BELOW	INITIALS AND DATE			
Catrina Purvis	Rm. 52012R	2				
Lisa Casias	Rm. 58032R	1				
ACTION ITEMS						
<table border="0" style="width: 100%;"> <tr> <td style="width: 50%; vertical-align: top;"> 1. APPROVAL/SIGNATURE 2. CLEARANCE/INITIALS 3. RECOMMENDATION OR COMMENT 4. RETURN WITH MORE DETAILS 5. INVESTIGATE AND REPORT 6. NOTE AND SEE ME 7. NOTE AND RETURN 8. NOTE AND FILE </td> <td style="width: 50%; vertical-align: top;"> 9. YOUR INFORMATION 10. PER OUR CONVERSATION 11. AS REQUESTED 12. NECESSARY ACTION 13. CIRCULATE AMONG STAFF 14. ANSWER DIRECTLY 15. PREPARE REPLY FOR SIGNATURE </td> </tr> </table> <p style="text-align: right;">OF: _____</p>					1. APPROVAL/SIGNATURE 2. CLEARANCE/INITIALS 3. RECOMMENDATION OR COMMENT 4. RETURN WITH MORE DETAILS 5. INVESTIGATE AND REPORT 6. NOTE AND SEE ME 7. NOTE AND RETURN 8. NOTE AND FILE	9. YOUR INFORMATION 10. PER OUR CONVERSATION 11. AS REQUESTED 12. NECESSARY ACTION 13. CIRCULATE AMONG STAFF 14. ANSWER DIRECTLY 15. PREPARE REPLY FOR SIGNATURE
1. APPROVAL/SIGNATURE 2. CLEARANCE/INITIALS 3. RECOMMENDATION OR COMMENT 4. RETURN WITH MORE DETAILS 5. INVESTIGATE AND REPORT 6. NOTE AND SEE ME 7. NOTE AND RETURN 8. NOTE AND FILE	9. YOUR INFORMATION 10. PER OUR CONVERSATION 11. AS REQUESTED 12. NECESSARY ACTION 13. CIRCULATE AMONG STAFF 14. ANSWER DIRECTLY 15. PREPARE REPLY FOR SIGNATURE					
COMMENTS						
<p>One "Certificate of Appreciation" and four "Certificates of Recognition" to be presented at the Privacy Council meeting on January 30, 2018.</p>						
<input type="checkbox"/> <i>Continued on reverse</i>						
FROM (Name)	BUILDING, ROOM OR REF. NO.	CODE AND EXTENSION				
Lisa Martin	Rm. 52010	x2459				

Comments (*continued*)

**Policies for Federal Agency Public Websites and Digital Services
OMB MEMO-17-06 - Data Call**

OMB 17-06 Citing	OPOG's Initial Assessment	B/OU's Response	Target for Improvement	Completion Date Given	Analysis Status	Analysis Symbol	Date	
SECTION 6.A PRIVACY PROGRAM PAGE								
Section 6.A	Does your B/OU have a central Privacy Program page? Note: This is not referencing the Privacy Policy page in the footer of the website. Example: www.commerce.gov/privacy	No https://www.XXX.doc.gov/privacy does not work	No, the page renders the XXX Privacy Policy Statement rather than a home page.	Update to point to the Privacy Policy Page. Will point it to the Privacy Program page when it is completed.	7/28/2017	Points to Digital Privacy Policy Page (DPP) https://www.XXX.doc.gov/Privacy		12/22/2017
	If so, is the Privacy page accessible in the "About" Page? (Example: https://www.commerce.gov/about)	No. If XXX will maintain its own Privacy Program page, it needs to be accessible from their About page.	There is no page only a statement	Will develop a privacy home page to link from the "About" page.	7/28/2017	Points to Privacy Policy Program (PPP) page https://www.XXX.doc.gov/XXX/privacy-policy-program		1/10/2018
	Does the website have a Privacy Policy and/or Digital Policy Page? If so, is it accessible throughout the website? (Example: http://www.osce.doc.gov/opog/privacy/digital-policy.html)	Yes, at the bottom of each page is a link. However, the page does not link to any privacy related information https://www.XXX.doc.gov/index.php/p/27 about XXX/174 XXX privacy policy statement.	This page is not working from the home page. It works from other pages on the site.	A new compliant Privacy Policy page will be developed. (Possible consideration: will reference the Departments Digital Policy)	7/28/2017	Points to Digital Privacy Policy Page https://www.XXX.doc.gov/Privacy		1/10/2018
Section 6.A.1.a	Does the website list and provide links to complete, up to date versions of your B/OU's SORNs? (Example: http://www.osce.doc.gov/opog/PrivacyAct/PrivacyAct_SORNs.html)	Unable to determine.	XXX only has 1 SORN. It is not in HTML. A pdf file will appear when the SORN link is selected from the website footer.	XXX has an existing Link to its SORN through the website footer. (May move to privacy home page).	7/28/2017	Link to SORN exists on the footer, DPP, and PPP http://www.osce.doc.gov/opog/PrivacyAct/SORNs/XXX_1.html . Needs to consistent with the link used on the PPP.		1/10/2018
	Does the website provide citations and links to all Federal Register notices that comprise the SORN for each system of records? (Example: http://www.osce.doc.gov/opog/PrivacyAct/SORNs/pat_tm_23.html)	Unable to determine.	The SORN that is being rendered is a PDF of the SORN in the Federal Register. Unsure what citations and notices are required or related.	Decide what SORN specific FR notices need to be included and provide links to them.	7/28/2017	Needs to consistent with the link used on the PPP.		1/10/2018
	For any SORNs that are comprised of multiple Federal Register notices, does the website provide a link to the unofficial consolidated versions of the SORNs that describe the current system of records and allow members of the public to view the SORN in its entirety in a single location?	Unable to determine.	Do not know what citations and notices are relevant, but the full SORN as documented in the Federal Register would be displayed.	If there are any relevant citations and notices, include them and provide links to them.	7/28/2017	Needs to consistent with the link used on the PPP.		1/10/2018
Section 6.A.1.b	Does the website list and provide links to PIAs or compelling justification to decline to post a link to a PIA? Does the B/OU's PIA webpage link to OPOG's website? (Example: http://www.osce.doc.gov/opog/privacy/compliance.html#approvedpias)	Unable to determine.	PIAs are not easily found. A PIA search was conducted on the site and found the XXX PIA document.	A Post and link to PIAs from Privacy Home page will be created.	7/28/2017	Yes, The PIA links, on the PPP, point to the PIA on the DOC/Privacy Page.		1/10/2018





Policies for Federal Agency Public Websites and Digital Services
OMB MEMO-17-06 - Data Call

OMB 17-06 Citing	OPOG's Initial Assessment	B/OU's Response	Target for Improvement	Completion Date Given	Analysis Status	Analysis Symbol	Date
Section 6.A.1.c	Does the website list and provide links to matching notices and agreements for all active matching programs in which the B/OU participates?	B/OU reported there are no matching notices or agreements.	Do not know what citations and notices are relevant.	N/A	N/A	N/A	1/10/2018
Section 6.A.1.d	Does the website have any exemptions to the Privacy Act? If yes, are the citations and links to the final rules published in the Federal Register on the B/OU website?	Did not see any exemptions to the Privacy Act.	Exemptions are listed in the SORN and applicable PIA.	Exemptions are listed in the SORN which is accessible from the website. (May need to be move to a website page)	N/A	Yes, the exemptions are listed on the PPP and points to GPO https://www.gpo.gov/fdsys/pkg/USCODE2015title5/html/USCODE2015title5part1chap5subchapIIsec552.htm .	 1/10/2018
Section 6.A.1.c	Does the website list and provide links to Privacy Act implementation rules promulgated pursuant to 5 U.S.C. § 552a(f)? (Example: http://www.osce.doc.gov/opog/PrivacyAct/PrivacyAct.html)	Unable to determine.	Exists in the SORN	Include Privacy Act implementation rules on the new Privacy Policy Page.	7/28/2017	Yes, Privacy act implementation rules are on the PPP.	 1/10/2018
Section 6.A.1.f	Does the website list and provide links to publicly available agency policies on privacy, including any directives, instructions, handbooks, manuals, or other guidance? If not, please link to OPOG's policy page. (Example: http://www.osce.doc.gov/opog/privacy/laws_and_regs.html)	Unable to determine.	Nothing besides the privacy page.	Determine if any reports exist. If needed update website and provide links on a new Privacy Policy page.	7/28/2017	Unable to determine.	 1/10/2018
Section 6.A.1.g	Does the website list and provide links to publicly available agency reports on privacy? Note: These reports need not include the agency's FISMA reports or reports provided to OMB and Congress.	Unable to determine.	No	Determine if any reports exist. If needed update website and provide links on a new Privacy Policy page.	7/28/2017	N/A	N/A 1/10/2018
Section 6.A.1.h	Does the website provide instructions on submitting a Privacy Act request for individuals who wish to request access to or amendment of their records? If not, please link to OPOG's Privacy Act page. (Example: http://www.osce.doc.gov/opog/PrivacyAct/PrivacyAct_requests.html)	Unable to determine.	No	Determine how requests will be submitted and update Privacy page.	7/28/2017	Yes, XXX links to the Privacy Act instructions on the DOC Privacy page.	 1/10/2018
Section 6.A.1.i	Does the website provide appropriate agency contact information for individuals who wish to submit a privacy related question or complaint? If not, please provide the appropriate privacy contact information.	No	No	Identify designated person and means of contact. Include in Privacy Home Page.	7/28/2017	Yes, XXX provides a link to the XXX Privacy Office and the Department's CPO.	 1/10/2018

**Policies for Federal Agency Public Websites and Digital Services
OMB MEMO-17-06 - Data Call**

OMB 17-06 Citing	OPOG's Initial Assessment	B/OU's Response	Target for Improvement	Completion Date Given	Analysis Status	Analysis Symbol	Date	
Section 6.A.1.j	Does the website list and provide a link to contact information for the Agency's Senior Agency Official for Privacy (SAOP)? If not, please use: www.commerce.gov/saop.	Did not see any links to agency's SAOP. Link to DOC's SAOP	No	Identify designated persons and means of contact. Include in Privacy Home Page.	7/28/2017	Yes, XXX provides an email link to the SAOP via the CPO@doc.gov on the DPP. However, the page does not identify the SAOP.		1/10/2018
	Does the website identify and provide contact information for the BCPO?	Could not easily find the B/OU's Chief Privacy Officer. Include contact information and email address to BCPO.	Yes	Identify designated persons and means of contact. Include in Privacy Home Page.	7/28/2017	Yes, the BCPO is identified on the PPP.		1/10/2018
Section 6.A.2	Does the B/OU maintain a sub agency , component , or program specific privacy program page? If so, the privacy program page must be accessible through www[sub agency, component, or program domain].gov/privacy. (Example: http://www.osec.doc.gov/opog/privacy/digitalpolicy.html#boupriavacy)	No	Agency level.	N/A	N/A	XXX PPP is not linked via www.XXX.doc.gov/privacy. This page is pointed to the DPP and not the PPP. The link needs to be changed to the correct page.		1/10/2018
SECTION 6. B. PRIVACY POLICIES ON AGENCY WEBSITE								
Section 6.B.1.a	Is the website written in plain language and organized in a way that is easy to understand and navigate? (Example: https://www.digitalgov.gov/resources/plainlanguagewebwritingtips/)	Unable to determine.	Yes	Will review to ensure plain language and organization (usability).	7/28/2017	The PPP is accessible via the About page; otherwise it is not easily found unless searching for it.		1/10/2018
Section 6.B.1.b	Does the Privacy Policy provide useful information that the public would need to make an informed decision about whether and how to interact with your agency? (This should include website, FAQs and other types of feedback loops.) (Example: https://www.digitalgov.gov/resources/plainlanguagewebwritingtips/)	Unable to determine.	No, current link renders an error	Will include FAQ section.	7/28/2017	Had to search to find FAQ but could not find any on Privacy, Privacy Act, SORN, etc.		1/10/2018
Section 6.B.1.c	Is the Privacy Policy updated whenever the agency makes a substantive change to the practices it describes?	Unable to determine.	Yes	OA should review Privacy Policy Content and provide OCIO with page updates when changes are made.	7/28/2017	Maintenance of Privacy Policy changes are not sent to the CPO@doc.gov.		1/10/2018
Section 6.B.1.d	Does the Privacy Policy include a time/date stamp to inform users of the last time the agency made a substantive change to the practices the privacy policy describes? Note: Must be included on every page.	Unable to determine.	No	Privacy Policy page does have an updated date and time stamp.	N/A	Not all pages contain date stamps. DPP does but the PPP does not.		1/10/2018
Section 6.B.1.e	Does the Privacy Policy adhere to all other applicable OMB requirements?	Unable to determine.	Yes	Will review to ensure all applicable OMB requirements are included.	7/28/2017	The PPP contains links to policies and a link to the policies on the DOC Privacy page.		1/10/2018

**Policies for Federal Agency Public Websites and Digital Services
OMB MEMO-17-06 - Data Call**

OMB 17-06 Citing	OPOG's Initial Assessment	B/OU's Response	Target for Improvement	Completion Date Given	Analysis Status	Analysis Symbol	Date	
Section 6.B.1.f	Does the Privacy Policy include a link to the agency's Privacy Program Page? If you do not have a page, please link to the OPOG webpage. (Example: www.commerce.gov/privacy)	Unable to determine.	No	Create link to the OPOG privacy program page.	7/28/2017	Could not find a link to the XXX or the Department's PPP on the DPP.		1/10/2018
Section 6.B.2	Does the Privacy Policy include content on the Children's Online Privacy Protection Act? If you do not have a page, please link to the OPOG webpage. (Example: http://www.oscc.doc.gov/opog/privacy/digitalpolicy.html#coppa)	Unable to determine.	No.	Will review Privacy Policy and update as required.	7/28/2017	Yes, the DPP contains a statement about COPPA and a link to the ftc.gov page https://www.ftc.gov/tips/advice/businesscenter/privacyandsecurity/children/27s privacy.		1/10/2018
SECTION 6. C. PRIVACY ACT STATEMENTS FOR ONLINE COLLECTIONS OF INFORMATION								
Section 6.C	Does the website provide a Privacy Act statement for collecting information using an online interface?	Unable to determine.	Not on main website page. Its on the applications at the point of data collection.	Not on main website page. Its on the applications at the point of data collection. Will need to be included on Privacy Home Page (link)	7/28/2017	Could not find a link to the Privacy Act statement for collecting information using an online interface or the Department's PPP on the DPP.		1/10/2018
	Does the website provide a privacy notice to cover when a Privacy Act is not required but the public still has a possibility to provide PII to the agency using an online interface anyway?	Unable to determine.	Not on main website page.	Not on main website page. Will include as necessary.	7/28/2017	Unable to find.		1/10/2018
SECTION 10. COMPLY WITH 3RD PARTY WEBSITE AND APPLICATION REQUIREMENTS								
Section 10.C	Does the B/OU use third party websites and applications? If so, do they comply with all relevant privacy protection requirements and a careful analysis of privacy implications as specified in OMB Memorandum M 10 23, Guidance for Agency Use of Third Party Websites?	No	No	N/A	N/A	N/A	N/A	1/10/2018

DIGITAL PRIVACY REPORT

- The policies for Federal Agency Public Websites and Digital Services (OMB Memorandum 17-06) will be used as the template for the analysis.
- The BCPO will be consulted for clarification.
- The report will be provided to the CPO.
- The follow icons will be used to notate the following:



- - Update is in progress



- - Update is complete



- - Indication of update was not found



- - Indication of new update is forthcoming

Federal Privacy Updates

2017 Federal Privacy Summit

The Federal Privacy Summit was held on December 12, 2017 in which there were more than 400 attendees. The keynote address was provided by Neomi Rao, Administrator of the Office of Information and Regulatory Affairs. In addition to networking session which gave attendees the opportunity to interact with Senior Agency Officials for Privacy and the Privacy Council's Committees and Working Groups, there were 16 breakout sessions on a wide variety of topics, such as shared services, privacy compliance reviews, the Paperwork Reduction Act, authentication, identifying and managing risk, and biometrics.

Updated Directive on Border Search of Electronic Devices (CBP Directive No. 3340-049A)

This directive enhances the transparency, accountability, and oversight of electronic device border searches performed by the U.S. Customs and Border Protection (CBP). The purpose of this directive is to provide guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers, tablets, removable media, disks, drives, tapes, mobile phones, cameras, music and other media players, and any other communication, electronic, or digital devices subject to inbound and outbound border searches by the CBP.

Upcoming Event

Tech Tuesday

Tuesday, February 13, 2018

Time: 1:00 p.m. 2:30 p.m.

GSA HQ 1800 F St NW

Washington DC, 20420

Room 1408

Dial-in (b)(6)

Adobe Connec (b)(6)

(b) (5)

(b) (5)

(b) (5)

Guide to Conducting a PII Breach Table Top Exercise (TTX)

Prior to Conducting this TTX

1. Review the DOC PA, PII, and BII Breach Response Plan.
2. Review OMB Memorandum 17 12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.

Breach Response Team Members

1. Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)
2. General Counsel (legal counsel)
3. Chief Information Officer (CIO) or the CIO's designee
4. Senior Agency Information Security Officer (SAISO) or the SAISO's designee
5. Chief Financial Officer/Assistant Secretary for Administration
6. Assistant Secretary for Legislative and Intergovernmental Affairs (OLIA) (legislative affairs official)
7. Chief of Staff, Office of the Secretary
8. Director, Office of Public Affairs (OPA) (communication official)
9. Director, Office of Policy and Strategic Planning
10. Director, Office of Human Resources Management
11. Office of Security (OSY), Attends on an as needed basis
12. Office of Inspector General (OIG), Advisory Role
13. Bureau Chief Privacy Officers
14. Privacy Act Officers
15. Deputy Director for Departmental Privacy Operations
16. Departmental FOIA/PA Officer

Planning

1. Establish the objectives of the TTX. Some of your objectives may be:
 - a. Improve the understanding of the DOC Breach Response Plan.
 - b. Identify opportunities to improve the DOC Breach Response Plan and the Department's preparedness.
 - c. Identify interdependencies among agency organizations and third party service providers.
2. Plan the TTX logistics.
 - a. Determine the date.
 - b. Reserve a space with an appropriate clearance level, as well as any materials or multimedia support you may need, such as computer and display, whiteboard and markers, butcher block paper, handouts, and dial in capabilities.
 - c. Set a time limit for the TTX. This will help you choose an appropriate scenario and focus the conversation appropriately during the TTX.
 - d. Assign support staff roles.

- i. Determine what role you want your privacy program to play in the exercise. Individuals who are deeply involved in planning the TTX may need to take a step back during the exercise to avoid accidentally influencing the course of the exercise. In a TTX, privacy office representatives often act in an advisor or consultant role, responding to questions from other participants, rather than the active leaders they often are in an actual breach.
- ii. Identify a facilitator (Consider using a neutral facilitator). The facilitator has the primary responsibility for exercise conduct. This includes introducing and providing scenario updates, moderating the discussions to ensure players address exercise objectives and core capabilities, and ensuring everyone contributes to the discussion and relevant issues are explored as thoroughly as possible within the allotted time.
- iii. In addition to a facilitator, you will also need staff dedicated to:
 - 1. Taking notes. These notes will form the basis of the after action report.
 - 2. Tracking “parking lot” issues.
 - 3. Documenting when Breach Response Plan steps are completed.
- e. Create a participant roster to track attendance at the TTX.
- f. Consider what role you want Senior Executive Service (SES) members and other senior leaders to play. SES member participation may stifle the conversation. Consider using SES members or other senior leaders as floaters who give out real time feedback.

A sample agenda is below:

Time	Activity
[Month Day, Year]	
0000 - 0000	Registration
0000 - 0000	Welcome and Introductions
0000 - 0000	Exercise Overview
0000 - 0000	Module 1: Initial Response – Scenario Background
0000 - 0000	Break
0000 - 0000	Module 2: Response
0000 - 0000	Module 3: Recovery
0000 - 0000	Break
0000 - 0000	Hot Wash

Time	Activity
0000 - 0000	Closing Comments
0000 - 0000	Debrief (Facilitators and Evaluators only)

3. Develop a realistic breach scenario.

a. Choosing a scenario.

- i. Consider which high value assets, applications, or processes you may want to include in the scenario.
 1. You do not have to limit yourself to high value assets, but you want to make sure the scenario has stakes. A high profile system or program, or a scenario that involves risks to the reputation or operations of the agency may be more engaging and offer more avenues for the participants to explore.
- ii. Look at the Department's recent breaches, as well as any major breaches, for ideas.
- iii. Review the Department's breach metrics to see where there are trends that may indicate a weakness or identify an issue about which you receive questions or complaints and consider developing a scenario around those fact patterns.
- iv. Consider breaches that will engage all of the participants. For example, a loss of hardcopy documents may not effectively engage a participant from the cybersecurity team. A scenario that requires cross functional collaboration (e.g., between staff supporting Freedom of Information Act (FOIA), privacy, cybersecurity, and human resources) is often a more effective TTX.
- v. Balance the complexity of the TTX with the knowledge and experience the BRT members have with handling a breach. A too simple scenario may not be an effective use of this training and awareness opportunity; a too complex scenario may make it difficult for participants to engage in the TTX.

b. Refining the scenario.

- i. After you have chosen the breach you would like to test, speak with the relevant program office and/or system owners to ensure that you understand their data and processes. The scenario should be grounded in reality.
- ii. Create a scenario that evolves over time. Create injects that complicate the scenario by adding additional facts. Provide a realistic timestamp for each update to help participants track their compliance with reporting requirements and understand how long actual breach response activities may take.
- iii. You should be able to map the DOC Breach Response Plan steps to the steps in your TTX; this will help you ensure that you have not forgotten any aspects of the DOC Breach Response Plan in the development of the scenario. Consider creating a table or grid citing back to the plan to ensure you know each BRT member's role and responsibility.
- iv. Try to make the TTX as interactive as possible. Break the scenario into modules with injects to keep participant attention and focus the discussion.

4. Create supporting artifacts, such as breach reports, supplemental reports, and after action reports.

- a. Use the Department’s breach reporting forms, including supplemental reports and after action reports, for the exercise. Using existing artifacts may highlight areas that need clarification or improvement.
 - b. You may want to create additional artifacts, such as dummy data file examples and external press reports.
 - c. Be sure to label all documents created for the TTX with “For exercise purposes only.”
 - d. It can be helpful to have packets available to the participants that include your agency’s breach response policy, the initial scenario, the injects, and any other supporting materials. The participants should not view the injects until they are directed to by the facilitator.
5. Provide an executive summary of the goals of the breach response program, its importance, and the goals and relevance of the TTX for senior leadership prior to TTX.

Execution

1. Share the TTX ground rules with the participants.
 - a. Stress that this is a learning exercise and that participants should feel comfortable asking questions or throwing out ideas. There are no wrong answers and everyone’s opinion will be considered.
 - b. Emphasize that participants should not “fight the scenario.” Every effort will have been made to ensure that the scenario is realistic and reflects actual practices.

Examples of TTX Ground Rules
<ul style="list-style-type: none"> Silence cell phones and other mobile devices during the exercise. Accept that the circumstances surrounding the event are real. This is a “no-fault” environment where varying viewpoints and disagreements are to be expected. There are no wrong answers.

2. Present the initial facts of the scenario to the participants. Use prompts to encourage interaction if the conversation is slow to start.
3. Participants should begin to identify immediate actions that should be taken, including establishing a communications plan and, if appropriate, Congressional notification plan.

Examples of Questions the BRT Should Consider
<ul style="list-style-type: none"> Is there a SORN or PIA? What other agency stakeholders or partners should be made aware of the breach? Who reports the breach to Congress? Who will need to approve any notices, notifications, and other communications? Who would be the source of the notification? Is any official designation required? How and who will fund identity protection services (IPS)? Does the CFO need to be engaged before securing IPS? Is there a vendor engaged for call center and IPS?

4. Start to provide injects to the scenario that reflect the types of information you would learn from a breach investigation.
 - a. With each inject, participants should identify the actions that should be taken based on the updated information.
 - b. You can also ask questions that explore other potential aspects of the breach. For example, if your breach involves information about members of the public only, you can ask them whether they would do anything differently if employee information was included.
5. Have participants complete a post TTX survey before leaving to get their input on the quality and strengths of the TTX, suggestions for improvement, and recommendations for future TTX scenarios.

Close-out

1. Develop an after action report/improvement plan that documents lessons learned and follow up actions for strengthening the DOC breach response process and/or the system, program, or processes that were tested in the TTX. The report/plan must provide timelines for improvement recommendation implementation and assignment to responsible parties.
 - a. Also document lessons learned for the next tabletop exercise. You can include these in the same report or a separate document.
 - b. Share the report with the BRT.
2. Review the DOC Breach Response Plan for any needed changes based on the lessons learned from the TTX.
3. If appropriate, conduct an out brief for senior leadership. The briefing should identify any unresolved issues to allow leadership to determine if any unmitigated risks are within the Department's risk tolerance.

Identity Protection Services (IPS) Multiple Award Blanket Purchase Agreement (BPA)

To best ensure federal customers have access to a pool of well qualified contractors capable of providing identity protection services to include data breach response and protection identity monitoring, GSA now offers government-wide Federal Supply Schedule (FSS), Blanket Purchase Agreements (BPAs), to provide these services.

Under the BPAs, which are in effect for the next five years, federal agencies have access to a variety of identity protection services covering both routine protection services that include:

- Consumer credit reports, address verification reports, and credit risk assessments; and
- Recovery services involving suspected or actual breaches of sensitive personally identifiable information.

Specifically, this government-wide multiple award BPA provides identity monitoring data breach response and protection services for the federal government including:

- Business information services;
- Credit monitoring services;
- Identity monitoring services;
- Identity theft insurance;
- Identity restoration services;
- Website services; and
- Call center services (related to these requirements).

Tiers of Experience

Two tiers of contractors are available under the BPAs:

- Tier 1: Is awarded only to Contractors with experience in responding to data breaches impacting populations of significant size (benchmark of 21.5 million); and
- Tier 2: Includes Contractors with general experience in providing routine data breach responses.

Tier 1 Contractors are included in Tier 2. Ordering Contracting Officers have the discretion to compete task orders (TO) at either Tier regardless of the impacted population size.

During the performance period of the BPAs, Tier 2 Contractors not selected as Tier 1 service providers can provide to the BPA Contracting Officer evidence of their experience in responding to data breaches impacting populations of significant size and based on that documentation, may be added to Tier 1.

For smaller numbers of individuals, it is recommended to use credit monitoring services under Tier 2 on the website. If the total cost of credit monitoring services falls under the purchase card threshold of \$2,500, you can contact any one of the three contractors directly, ask for a quote based on "BPA CLIN 0003A," (CLIN stands for Contract Line Item Number), and place the order directly with the contractor you choose.

Authorized Users

Any warranted Contracting Officer from authorized users of the Schedules program, within the scope of their delegated procurement authorities, may place orders against the BPA(s).

IPS BPA Ordering Period

Five years from September 01, 2015, through August 31, 2020. Orders (including order options) have their own period of performance. Any orders placed during the BPA ordering period may extend beyond that period (including the right to exercise order options) and be completed in accordance with the Contractor's FSS FAR clause 52.216-22 paragraph (d).

Order Dollar Value Limitations

Unlike most ID/IQ Contracts, BPAs do not have a dollar value ceiling. Thus there is no dollar value limitation on the size of an order.

Small Business Credit

Agencies will receive small business credit when issuing orders to small business BPA holders. For BPAs based on a Contractor Teaming Arrangement (CTA), a small business team member may be designated as the CTA lead for any task order as applicable. Hence, all CTA members have been assigned BPA numbers for this purpose. Agencies are also authorized if applicable to set-aside orders for small business. See ordering procedures for further details.

IPS BPA Award Information

Collect estimates from each contractor. POCs are listed on the contract. If the quote is under \$2,500, you may use the government purchase card.

In November 2017, three contractors offered BPA CLIN 0003A credit monitoring services. The following are the estimates received at that time based upon approximately 10 individuals for one year. You will need to call each contractor and get an estimate based upon your breach, i.e., the number of individuals required services and the duration of the service. You also will need to obtain a description of the specific services offered with the cost estimate.

Contactor	Cost Per Person Per Year	Phone	Website and Email
ID EXPERTS	\$51.58	(866) 726-4271	http://www.idexpertsCorp.com/ mailto:government@idexpertsCorp.com
IdentityForce	High Risk \$49.66 Low Risk \$15.17 Package 3 \$10.18	(508) 210-4414	http://www.identityforce.com/ mailto:sbrown@identityforce.com
LADLAS PRINCE LLC	\$38.50	(248) 875-3409	http://www.ladlasprince.com/ mailto:Amos.O.Ajani@ladlasprince.com

Contact

Email Professional Services at professionalservices@gsa.gov.

Additional information can be found at: www.gsa.gov/ipsbpa.

Government/GSA POC:

Kenny Yiu
Senior Contracting Officer
GSA, FAS, PSHC
400 15th Street SW
Auburn, WA 98001
kenny.yiu@gsa.gov
253-931-7915



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

July 1, 2016

M-16-14

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

FROM: Anne E. Rung 
United States Chief Acquisition Officer

SUBJECT: **Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response**

This memorandum updates a longstanding Office of Management and Budget (OMB) policy, first implemented in 2006, to maximize federal agency use of a government-wide solution for acquiring identity protection services when needed. This memorandum requires, with limited exceptions, that when agencies need identity protection services, agencies address their requirements by using the government-wide blanket purchase agreements (BPAs) for Identity Monitoring Data Breach Response and Protection Services awarded by the General Services Administration (GSA), referred to below as the “IPS BPAs.”

For the past decade, GSA has offered commercial credit monitoring services through government-wide BPAs established under its Federal Supply Schedules (FSS) Program. When the BPAs were launched, OMB instructed agencies to review the pricing and terms and conditions of the BPAs in addition to any other credit monitoring services they may be considering in their market research and notify OMB prior to making an award outside of the BPAs.¹

Last year, GSA partnered with other agencies on requirements for new BPAs to ensure that all agencies have access to a pool of best qualified contractors capable of providing a comprehensive range of identity protection services, including credit monitoring. For details on the IPS BPAs, including task order instructions, offered services, authorized users, order dollar value limitations, the inclusion of agency specific terms, and ordering periods, visit www.gsa.gov/ipsbpa.

Taking advantage of the IPS BPAs ensures agencies can meet their needs for expeditious delivery of best-in-class solutions from pre-approved and vetted companies at competitive pricing and reduced administrative costs. For these reasons, the IPS BPAs shall be treated as a preferred source for Federal agencies when agencies have a need for credit monitoring, breach response, and identity protection services. Consistent with category management principles, GSA, as the contract manager, will work with an interagency team to periodically review and refresh, as appropriate, the contract terms and requirements to ensure the BPAs continue to reflect the best identity protection practices and agencies’ needs.

¹ See OMB Memorandum M-07-04, *Use of Commercial Credit Monitoring Services Blanket Purchase Agreements*.

The following steps, which are effective immediately, are designed to ensure agency use of the IPS BPAs to the maximum extent practicable:

1. **Review the range of services offered under the IPS BPAs:** If the agency has an existing vehicle that overlaps with the BPAs and is planning to exercise an option, or is planning to issue a new contract that could overlap with the BPAs, take the additional steps described below.

2. **Existing contracts:**

a) **Analysis of alternatives:** As part of deciding whether to exercise an option under an existing agency contract, and in accordance with Federal Acquisition Regulation (FAR) 17.207, the agency shall analyze terms/conditions, pricing, performance, fees and savings under the agency contract relative to the IPS BPAs. The agency may also consider the impact on an incumbent small business contractor.

b) **Sharing of final analysis:** If the agency exercises the option, it shall provide the final analysis to GSA and OMB at the following URL:
<https://community.max.gov/x/CoELQ>.

c) **Agency approvals:** If an agency proceeds with exercising an option under an existing agency contract, the agency shall ensure the final analysis has been approved by the Senior Agency Official for Privacy (SAOP) and any other officials as identified by internal agency policies.

d) **Sharing of prices paid and other contract information:** If the agency exercises the option, it shall submit, using the URL provided above:

(i) a copy of the option and underlying contract vehicle and,

(ii) at the end of the option period, prices paid under the option.

3. **Planned procurements:**

a) **Analysis of alternatives:** Agencies that are considering a different vehicle to provide identity protection services shall develop an analysis of alternatives that compares the planned vehicle to the IPS BPAs in terms of: scope, period of performance, terms and conditions, pricing, performance, administrative costs (cost of full-time equivalent employees supporting award and administration of the vehicle vs. the fees that would be paid to use the IPS BPAs) customer satisfaction (if the organization has previously managed a similar vehicle), and small business impact, if any. The analysis should also highlight any unique features and/or requirements. Finally, if the agency is planning an inter-agency

contract, its evaluation should include a market analysis and a description of the agency's suitability for managing the vehicle.

- b) Sharing of analysis: If the agency proceeds with its own vehicle, it shall:
 - (i) provide the final analysis to GSA and OMB at the URL identified above; and
 - (ii) if the anticipated value of the vehicle exceeds the simplified acquisition threshold (SAT), the agency shall share a draft of the analysis with the Category Manager for Professional Services and OMB at <https://community.max.gov/x/CoELQ> for a five (5) business day review period to offer input on the analysis.
- c) Agency approvals: If, after considering any input from the Category Manager, the agency decides to proceed with its own vehicle, it shall ensure the final analysis has been approved in accordance with internal agency policies. At a minimum, the analysis shall be approved by the SAOP and, if the vehicle has an anticipated value above the SAT, by the agency's Senior Procurement Executive.
- d) Sharing of prices paid and other contract information: If the agency proceeds with its own vehicle, the agency shall submit using the URL provided above:
 - (i) a copy of the contract vehicle; and,
 - (ii) at the end of the base and each option period, prices paid under the contract vehicle.

Agencies that require contractors to provide identity protection services, or a subset thereof, as part of the security or safeguarding requirements in their contract are exempt from this guidance. However, pursuant to FAR Part 51.1 Contractor Use of Government Supply Sources, agencies may at their discretion authorize government contractors under cost-reimbursement contracts and fixed price contracts for protection of security classified information and related security equipment to use GSA sources, including the IPS BPAs, when determined to be in the best interest of the government. Additionally, agencies may seek a deviation pursuant to FAR Subpart 1.4 to address other situations where contractor access to the IPS BPAs would be beneficial.

By implementing the process described above, the government will serve the needs of impacted individuals, programs, and operations by leveraging the government's robust buying power abilities to provide cost-effective, best-in-class solutions. Agencies are encouraged to contact GSA and OMB with any potential questions or concerns regarding the implementation of included instructions.

For further questions regarding this memorandum, please contact Iulia Manolache in the OMB's Office of Federal Procurement Policy at imanolache@omb.eop.gov or (202) 395-7318.

Privacy Council Face-to-Face Meeting Agenda – February 6, 2018

Time	Topic	Presenter
08:00 – 08:30	Arrival	
08:30 – 08:40	Welcome and Introductions	Lisa Martin
08:40 – 08:50	Action Item Updates	Catrina Purvis
08:50 – 09:20	Privacy Program Coordinator Updates <ul style="list-style-type: none"> • PII Incident Metrics • PIA Compliance Metrics 	Tahira Murphy/Nate Thweatt Kathy Gioffre
09:20 – 09:30	Federal Privacy Updates <ul style="list-style-type: none"> • Federal Privacy Summit • Updated Directive on Border Search of Electronic Devices • EU General Data Protection Regulation (GDPR) • Upcoming Events 	Lisa Martin/Catrina Purvis
09:30 – 10:00	Privacy Program Highlights <ol style="list-style-type: none"> 1. Privacy Act Officer Updates 2. SSN Fraud Prevention Act Update 3. Credit Monitoring 4. DOC Website Reviews 	Michael Toland Lisa Martin/Michael Toland Lisa Martin Tahira Murphy
10:00 – 10:15	BREAK	
10:15 – 11:15	Privacy Program Improvement/Policy Reviews <ol style="list-style-type: none"> 5. FY18 PII Breach Table Top Exercise Planning 	
11:15 – 11:45	BOU Member Time <ul style="list-style-type: none"> • SharePoint Privacy Warning Banner when Logging In 	Byron Crenshaw
11:45 – 12:00	Round Table	Catrina Purvis
12:00 – 12:30	Year-End Assessment	Lisa Casias

(b) (5)

Upcoming Data Call:

- Privacy Review of Forms

Upcoming Request for Comments:

- Delegation of the Departmental OCIO Review of Security Controls

Mark Graff - NOAA Federal

From: Mark Graff NOAA Federal
Sent: Tuesday, February 6, 2018 10:44 AM
To: Murphy, Tahira
Subject: Presentation
Attachments: A 130 final.pdf; Department of Commerce PII, BII, and PA Breach Response and Notification Plan v3.pdf

I apologize, it looks like the prior email only sent Google Drive Links. Here they are as pdf files.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

CIRCULAR NO. A-130

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Managing Information as a Strategic Resource

1. Introduction
2. Purpose
3. Applicability
4. Basic Considerations
5. Policy
 - a. Planning and Budgeting
 - b. Governance
 - c. Leadership and Workforce
 - d. IT Investment Management
 - e. Information Management and Access
 - f. Privacy and Information Security
 - g. Electronic Signatures
 - h. Records Management
 - i. Leveraging the Evolving Internet
6. Government-wide Responsibilities
7. Effectiveness
8. Oversight
9. Authority
10. Definitions
11. Inquiries

Appendix I: Responsibilities for Protecting and Managing Federal Information Resources

1. Introduction
2. Purpose
3. General Requirements
4. Specific Requirements
5. Government-wide Responsibilities
6. Discussion of the Major Provisions in the Appendix
7. Other Requirements
8. References

Appendix II: Responsibilities for Managing Personally Identifiable Information

1. Purpose
2. Introduction
3. Fair Information Practice Principles
4. Senior Agency Official for Privacy
5. Agency Privacy Program
6. Managing PII Collected for Statistical Purposes Under a Pledge of Confidentiality

1. Introduction

Information and information technology (IT) resources are critical to the U.S. social, political, and economic well-being. They enable the Federal Government to provide quality services to citizens, generate and disseminate knowledge, and facilitate greater productivity and advancement as a Nation. It is important for the Federal Government to maximize the quality and security of Federal information systems, and to develop and implement uniform and consistent information resources management policies in order to inform the public and improve the productivity, efficiency, and effectiveness of agency programs. Additionally, as technology evolves, it is important that agencies manage information systems in a way that addresses and mitigates security and privacy risks associated with new information technologies and new information processing capabilities.

These new information technologies and information processing capabilities also provide significant opportunities for agencies. The deeply embedded nature of IT in all Federal agency missions and business processes, and the emergence of the digital economy, combined with the increasing interconnection of technology and public services, has changed the way we share information, changed the way we use and view technology, and has forever changed Americans' expectations. To meet expectations of the American people and facilitate innovation, the Federal Government must continue to transform itself to embrace and respond to the digital revolution by developing and maintaining a top-notch workforce and delivering secure, world-class digital services that serve the public. With IT at the core of nearly everything the Federal Government does, agencies must continually identify ways to apply new and emerging technologies that can fundamentally improve the way Government works and delivers services to the American people in the most cost-effective way possible. Delivering world-class digital services requires the Federal Government to change its approach to buying, building, and delivering IT and information. This Circular is designed to help drive the transformation of the Federal Government and the way it builds, buys, and delivers technology by institutionalizing more agile approaches intended to facilitate the rapid adoption of changing technologies, in a way that enhances information security, privacy, and management of information resources across all Federal programs and services.

2. Purpose

This Circular¹ establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources and supporting infrastructure and services. The appendices to this Circular also include responsibilities for protecting Federal information resources and managing personally identifiable information (PII). While it is the responsibility of all agency leadership, program managers, and staff to implement the requirements of this Circular, agency heads have ultimate

¹ Although this Circular touches on many specific information resources management issues such as privacy, confidentiality, information quality, dissemination, and statistical policy, those topics are covered more fully in other Office of Management and Budget (OMB) policies, which are available on the OMB website. Agencies shall implement the policies in this Circular and those in other OMB policy guidance in a mutually consistent fashion.

responsibility for ensuring that the requirements of this Circular are implemented for their agency.

3. Applicability

The requirements of this Circular apply to the information resources management activities of all agencies² of the Executive Branch of the Federal Government. The requirements of this Circular apply to management activities concerning all information resources in any medium (unless otherwise noted), including paper and electronic information. When an agency acts as a service provider, the ultimate responsibility for compliance with applicable requirements of this Circular is not shifted (to the service provider). Agencies shall describe the responsibilities of service providers in relevant agreements with the service providers. Agencies are not required to apply this Circular to national security systems (defined in 44 U.S.C. § 3552), but are encouraged to do so where appropriate. For national security systems, agencies shall follow applicable statutes, executive orders, directives, and internal agency policies.

4. Basic Considerations

Federal information is both a strategic asset and a valuable national resource. It enables the Government to carry out its mission and programs effectively. It provides the public with knowledge of the Government, society, economy, and environment past, present, and future. Federal information is also a means to ensure the accountability of Government, to manage the Government's operations, and to maintain and enhance the performance of the economy, the public health, and welfare. Appropriate access to Federal information significantly enhances the value of the information and the return on the Nation's investment in its creation. The following considerations reflect these principles:

- a. The free flow of information between the Government and the public is essential to a democratic society. Therefore, the management of Federal information resources shall protect the public's right of access to Federal information;
- b. Government agencies shall be open, transparent, and accountable to the public. Promoting openness and interoperability, subject to applicable legal and policy requirements, increases operational efficiencies, reduces costs, improves services, supports mission needs, and increases public access to valuable Federal information;
- c. Making Federal information discoverable, accessible, and usable can fuel entrepreneurship, innovation, and scientific discovery that improves the lives of Americans, and contributes significantly to national stability and prosperity, and fosters public participation in Government;
- d. The Federal Government shall provide members of the public with access to public information on Government websites. This responsibility includes taking affirmative steps to ensure and maximize the quality, objectivity, utility, and integrity of Federal information prior to public dissemination, and maintaining processes for addressing requests for correction of information disseminated publicly;

² 'Agency' means any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency.

- e. The open and efficient exchange of scientific and technical Federal information, subject to applicable security and privacy controls and the proprietary rights of others, fosters excellence in scientific research and effective use of Federal research and development resources;
- f. Federal information is a strategic asset subject to risks that must be managed to minimize harm;
- g. Protecting an individual's privacy is of utmost importance. The Federal Government shall consider and protect an individual's privacy throughout the information life cycle;
- h. While security and privacy are independent and separate disciplines, they are closely related, and it is essential for agencies to take a coordinated approach to identifying and managing security and privacy risks and complying with applicable requirements;
- i. The design of information collections shall be consistent with the intended use of the information, and the need for new information shall be balanced against the burden imposed on the public, the cost of the collection, and any privacy risks;
- j. It is essential that the Federal Government minimize the Federal information collection burden on the public, minimize the costs of its information activities, and maximize the usefulness of Government information; and
- k. Attention to the management of Federal Government records from creation to disposition is an essential component of sound information resources management that promotes public accountability. Together with records preservation, it helps protect the Federal Government's historical record and safeguards the legal and financial rights of the Federal Government and the public.

5. Policy

Agencies shall establish a comprehensive approach to improve the acquisition and management of their information resources by: performing information resources management activities in an efficient, effective, economical, secure, and privacy-enhancing manner; focusing information resources planning to support their missions; implementing an IT investment management process that links to and supports budget formulation and execution; and rethinking and restructuring the way work is performed before investing in new information systems.

a. Planning and Budgeting

Agencies shall establish agency-wide planning and budgeting processes in accordance with OMB guidance. As discussed below, important components of planning and budgeting consist of developing and maintaining a strategy for managing and maintaining their information resources, referred to as the Information Resource Management (IRM) Strategic Plan, as well as ensuring effective collaboration between agency leadership on budget activities.

1) Strategic Planning

In support of agency missions and business needs, and as part of the agency's overall strategic and performance planning processes, agencies shall develop and maintain an IRM Strategic Plan that describes the agency's technology and information resources

goals, including but not limited to, the processes described in this Circular. The IRM Strategic Plan must support the goals of the Agency Strategic Plan required by the Government Performance and Results Modernization Act of 2010 (GPRM Modernization Act). The IRM Strategic Plan shall demonstrate how the technology and information resources goals map to the agency's mission and organizational priorities. These goals shall be specific, verifiable, and measurable, so that progress against these goals can be tracked. The agency shall review its IRM Strategic Plan annually alongside the Annual Performance Plan reviews, required by the GPRM Modernization Act, to determine if there are any performance gaps or changes to mission needs, priorities, or goals. As part of the planning and maintenance of an effective information strategy, agencies shall meet the following requirements, in addition to all other requirements in this Circular:

a) Inventories

Agencies shall:

- i. Maintain an inventory³ of the agency's major information systems,⁴ information holdings, and dissemination products, at the level of detail that OMB and the agency determine is most appropriate for overseeing and managing the information resources; and
- ii. Maintain an inventory of the agency's information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to allow the agency to regularly review its PII and ensure, to the extent reasonably practicable, that such PII is accurate, relevant, timely, and complete; and to allow the agency to reduce its PII to the minimum necessary for the proper performance of authorized agency functions.⁵

b) Information Management

Agencies shall:

- i. Continually facilitate adoption of new and emerging technologies, and regularly assess the following throughout the life of each information system: the inventory of the physical and software assets associated with the system⁶; the maintainability and sustainability of the information resources and infrastructure supporting the system; and actively determine when significant upgrades,

³ The inventory of agency information resources shall include an enterprise-wide data inventory that accounts for data used in the agency's information systems.

⁴ The inventory of major information systems is required in accordance with 44 U.S.C. § 3505(c). All information systems are subject to the requirements of the Federal Information Security Modernization Act (44 U.S.C. Chapter 35) whether or not they are designated as a major information system.

⁵ This inventory may be combined with the agency's inventory of information systems, as described above.

⁶ Agencies shall ensure that physical devices, software applications, hardware platforms, and systems within the organization are inventoried initially when obtained and updated on an ongoing basis.

replacements, or disposition is required to effectively support agency missions or business functions and adequately protect agency assets;⁷ and

- ii. Ensure the terms and conditions of contracts and other agreements involving the processing, storage, access to, transmission, and disposition of Federal information are linked to the IRM strategic plan goals, and are sufficient to enable agencies to meet their policy and legal requirements.

c) Risk Management

Agencies shall:

- i. Consider information security, privacy, records management, public transparency, and supply chain security issues for all resource planning and management activities throughout the system development life cycle so that risks are appropriately managed;
- ii. Develop plan, in consultation with Chief Information Officers (CIOs), Senior Agency Officials for Records Management (SAORMs), and Senior Agency Officials for Privacy (SAOPs), for information systems and components that cannot be appropriately protected or secured and ensure that such systems are given a high priority for upgrade, replacement, or retirement;⁸
- iii. Regularly review and address risk regarding processes, people, and technology; and
- iv. Consult National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and NIST Special Publications (SPs) (e.g., 500, 800, and 1800 series guidelines).

2) Enterprise Architecture

Agencies shall develop an enterprise architecture (EA) that describes the baseline architecture, target architecture, and a transition plan to get to the target architecture. The agency's EA shall align to their IRM Strategic Plan. The EA should incorporate agency plans for significant upgrades, replacements, and disposition of information systems when the systems can no longer effectively support missions or business functions. The EA should align business and technology resources to achieve strategic outcomes. The process of describing the current and future state of the agency, and laying out a plan for transitioning from the current state to the desired future state, helps agencies to eliminate waste and duplication, increase shared services, close performance gaps, and promote engagement among Government, industry, and citizens.

⁷ The assessment process is described in NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*.

⁸ Includes hardware, software, or firmware components no longer supported by developers, vendors, or manufacturers through the availability of software patches, firmware updates, replacement parts, and maintenance contracts. NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides additional guidance on unsupported software components.

3) Planning, Programming, and Budgeting

Agencies shall, in accordance with the Federal Information Technology Acquisition Reform Act (FITARA) and related OMB policy:⁹

- a) Ensure that IT resources are distinctly identified and separated from non-IT resources during the planning, programming, and budgeting processes in a manner that affords agency CIOs appropriate visibility and specificity to provide effective management and oversight of IT resources;
- b) Ensure that the agency-wide budget development process includes the CFO, CAO, and CIO in the planning, programming, and budgeting stages for programs that include IT resources (not just programs that are primarily information- and technology-oriented);
- c) The agency head, in consultation with the CFO, CAO, CIO, and program leadership, shall define the processes by which program leadership works with the CIO to plan an overall portfolio of IT resources that achieve program and business objectives efficiently and effectively by:
 - i. Weighing potential and ongoing IT investments and their underlying capabilities against other proposed and ongoing IT investments in the portfolio; and
 - ii. Identifying gaps between planned and actual cost, schedule, and performance goals for IT investments and developing a corrective action plan to close such gaps;
- d) Ensure that the CIO approves the IT components of any plans, through a process defined by the agency head that balances IT investments with other uses of agency funding. Agencies shall also ensure that the CIO is included in the internal planning processes for how the agency uses information resources to achieve its objectives at all points in their life cycle, including operations and disposition or migration;
- e) Ensure that agency budget justification materials, in their initial budget submission to OMB, include a statement that affirms:
 - i. The CIO has reviewed and approves the IT investments portion of the budget request;
 - ii. The SAOP has reviewed the IT investments portion of the budget request to ensure that privacy requirements, as well as any associated costs, are explicitly identified and included with respect to any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII;

⁹ OMB policy documents can be located at https://www.whitehouse.gov/omb/circulars_default and https://www.whitehouse.gov/omb/memoranda_default. The Department of Defense (DoD), the Intelligence Community, and portions of other agencies that operate systems related to national security are subject to only certain portions of Federal Information Technology Acquisition Reform (FITARA) (Pub. L. 113-291), as provided for in the statute.

- iii. The CFO and CIO jointly affirm that the CIO had a significant role in reviewing planned IT support for major program objectives and significant increases and decreases in IT resources; and
- iv. The IT Portfolio includes appropriate estimates of all IT resources included in the budget request;
- f) Ensure that the CFO, CAO, and CIO define agency-wide policy for the level of detail of planned expenditure reporting for all transactions that include IT resources.

4) Business Continuity Planning

Agencies shall develop a Business Continuity Plan.¹⁰ A Business Continuity Plan to continue agency operations during times of service disruption is essential. Therefore, agencies shall develop continuity strategies in order to ensure services and access can be restored in time to meet the mission needs. Manual workarounds shall be part of the plan so business can continue while information systems are being restored.

b. Governance

In support of agency missions and business needs, and in coordination with program managers, agencies shall:

- 1) Define, implement, and maintain processes, standards, and policies applied to all information resources at the agency, in accordance with OMB guidance;
- 2) Require that the CIO, in coordination with appropriate governance boards, defines processes and policies in sufficient detail to address information resources appropriately. At a minimum, these processes and policies shall require that:
 - a) Investments and projects in development are evaluated to determine the applicability of agile development;¹¹
 - b) Open data standards are used to the maximum extent possible when implementing IT systems;
 - c) Appropriate measurements are used to evaluate the cost, schedule, and overall performance variances¹² of IT projects across the portfolio leveraging processes such

¹⁰ The Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. Chapter 35) requires each agency to develop, document, and implement an agency-wide information security program that includes plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. For additional information related to continuity planning and contingency planning, see Appendix I.

¹¹ This evaluation shall be conducted as part of the acquisition planning process and involve staff from the CIO of the department, the implementing program managers, the appropriate contracting office representatives, and other applicable agency officials;

¹² Standard definitions from budget or performance management practices, such as earned value management, shall be used for cost variance and schedule variance to measure progress.

as IT investment management, enterprise architecture, and other agency IT or performance management processes;¹³

- d) There are agency-wide policies and procedures for conducting IT investment reviews, operational analyses, or other applicable performance reviews to evaluate IT resources, including projects in development and ongoing activities;
 - e) Data and information needs are met through agency-wide data governance policies that clearly establish the roles, responsibilities, and processes by which agency personnel manage information as an asset and the relationships among technology, data, agency programs, strategies, legal and regulatory requirements, and business objectives;¹⁴ and
 - f) Unsupported information systems and system components¹⁵ are phased out as rapidly as possible, and planning and budgeting activities for all IT systems and services incorporate migration planning and resourcing to accomplish this requirement;
- 3) Ensure that the CIO is a member of governance boards that inform decisions regarding IT resources to provide for early matching of appropriate information resources with program objectives. The CIO may designate, in consultation with other senior agency officials, other agency officials to act as their representative to fulfill aspects of this responsibility so long as the CIO retains accountability;
 - 4) Require that information security and privacy be fully integrated into the system development process;
 - 5) Conduct TechStat reviews, led by the CIO, or use other applicable performance measurements to evaluate the use of agency information resources. The CIO may recommend to the agency head the modification, pause, or termination of any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation, within the terms of the relevant contracts and applicable regulations;
 - 6) Establish and maintain a process for the CIO to regularly engage with program managers to evaluate IT resources supporting each agency strategic objective. It shall be the CIO and program managers' shared responsibility to ensure that legacy and ongoing IT investments are appropriately delivering customer value and meeting the business objectives of the agency and the programs that support the agency; and
 - 7) Measure performance in accordance with the GPRA Modernization Act and OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*.

¹³ The Federal Acquisition Streamlining Act of 1994 (Pub. L. 103-355) requires agencies to achieve, on average, ninety percent of the cost and schedule goals established for major and non-major acquisition programs of the agency without reducing the performance or capabilities of the items being acquired.

¹⁴ In accordance with the information management responsibilities outlined in 44 U.S.C. § 3506(b).

¹⁵ Includes hardware, software, or firmware components no longer supported by developers, vendors, manufacturers, or communities through the availability of software patches, firmware updates, replacement parts, and maintenance contracts. NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides additional guidance on unsupported software components.

c. Leadership and Workforce

Agencies shall:

- 1) Require that the Chief Human Capital Officer (CHCO), CIO, CAO, and SAOP develop a set of competency requirements for information resources staff, including program managers, information security, privacy, and IT leadership positions, and develop and maintain a current workforce planning process to ensure that the agency can:
 - a) Anticipate and respond to changing mission requirements;
 - b) Maintain workforce skills in a rapidly developing IT environment; and
 - c) Recruit and retain the IT talent needed to accomplish the mission;
- 2) Ensure that the workforce, which supports the acquisition, management, maintenance, and use of information resources, has the appropriate knowledge and skills to facilitate the achievement of the portfolio's performance goals and, further, evaluate the extent to which the agency's executive-level workforce has appropriate information and technology-related knowledge and skills;
- 3) Implement innovative approaches and track performance of workforce development training, including cross-functional training, rotational development and assignments, and effective training and education used by the private sector, to maintain and enhance skills or obtain additional skills;
- 4) Ensure that the CHCO and CIO jointly establish an agency-wide critical element (or elements) to be included in all component or bureau CIOs' performance evaluations. In addition, the CIO shall identify key component or bureau CIOs and provide input to the rating official for these component or bureau CIOs at the time of the initial summary rating and for any required progress reviews. The rating official will consider the input from the CIO when determining the initial summary rating and discuss it with the component or bureau CIO during progress reviews;
- 5) Ensure that the CIO is involved in the recruitment, approves the selection, and provides input for the performance review of any component or bureau CIO, which includes any component or bureau leader who holds CIO duties but not necessarily the "CIO" title. The title and responsibilities of current component or bureau CIOs should be designated or transferred to other agency personnel by the agency head or their designee as appropriate, and such decisions should take into consideration recommendations from the agency CIO;
- 6) Ensure that the SAOP is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy; and
- 7) Ensure that the CIO, CHCO, SAOP, and other hiring managers take advantage of flexible hiring authorities for specialized positions, as established by the Office of Personnel Management (OPM).

d. IT Investment Management

- 1) Acquisition of Information Technology and Services

Agencies shall:

- a) Make use of adequate competition, analyze risks (including supply chain risks) associated with potential contractors and the products and services they provide, and allocate risk responsibility between Government and contractor when acquiring IT;
- b) Conduct definitive technical, cost, and risk analyses of alternative design implementations, including consideration of the full life cycle costs of IT products and services, including but not limited to, planning, analysis, design, implementation, sustainment, maintenance, re-competition, and retraining costs, scaled to the size and complexity of individual requirements;¹⁶
- c) Consider existing Federal contract solutions or shared services when developing planned information systems, available within the same agency, from other agencies, or from the private sector to meet agency needs to avoid duplicative IT investments;
- d) Acquire IT products and services in accordance with Government-wide requirements;¹⁷
- e) Ensure that decisions to improve existing information systems with custom-developed solutions or develop new information systems are initiated only when no existing alternative private sector or governmental source can efficiently meet the need, taking into account long-term sustainment and maintenance;
- f) Structure acquisitions for major IT investments into useful segments, with a narrow scope and brief duration, in order to reduce risk, promote flexibility and interoperability, increase accountability, and better match mission need with current technology and market conditions;
- g) To the extent practicable, modular contracts for IT, including orders for increments or useful segments of work, should be awarded within 180 days after the solicitation is issued. If award cannot be made within 180 days, agencies shall consider cancelling the solicitation. The IT acquired should be delivered within 18 months after the solicitation resulting in award of the contract was issued;¹⁸
- h) Align IT procurement requirements with larger agency strategic goals;
- i) Promote innovation in IT procurements, including conducting market research in order to maximize utilization of innovative ideas; and
- j) Include security, privacy, accessibility, records management, and other relevant requirements in solicitations.

2) Agency Approval

Agencies shall ensure that all acquisition strategies, plans, and requirements (as described in FAR Part 7), or interagency agreements (such as those used to support

¹⁶ Other acquisition planning provisions are set forth in the Federal Acquisition Regulation (FAR) Subpart 7.1, Acquisition Plans, and Part 10, Market Research.

¹⁷ For information regarding Government-wide requirements, refer to OMB policy and the Federal Acquisition Regulation. For the acquisition of Personal Identity Verification (PIV) and public key infrastructure (PKI) products and services, also refer to the FIPS 201 Evaluation Program at <https://www.idmanagement.gov>.

¹⁸ Pursuant to Public Contracts statute (41 U.S.C. § 2308).

purchases through another agency) that include IT are reviewed and approved by the purchasing agency's CIO. These approvals shall consider the following factors:

- a) Alignment with mission and program objectives in coordination with program leadership;
- b) Appropriateness with respect to the mission and business objectives supported by the IRM Strategic Plan;
- c) Inclusion of innovative solutions;
- d) Appropriateness of contract type for IT-related resources;
- e) Appropriateness of IT-related portions of statement of needs or statement of work;
- f) Ability to deliver functionality in short increments;
- g) Inclusion of Government-wide IT requirements, such as information security; and
- h) Opportunities to migrate from end-of-life software and systems, and to retire those systems.

3) Investment Planning and Control

Agencies are responsible for establishing a decision-making process that shall cover the life of each information system and include explicit criteria for analyzing the projected and actual costs, benefits, and risks, including information security and privacy risks, associated with the IT investments. Agencies shall designate IT investments according to relevant statutes, regulations, and guidance in OMB Circular A-11, and execute processes commensurate with the size, scope, duration, and delivery risk of the investment. The IT investment processes shall encompass planning, budgeting, procurement, management, and assessment. For further guidance related to investment planning, refer to OMB Circular A-11, including the Capital Programming Guide. At a minimum, agencies shall ensure that:

- a) All IT resources (see "Information Technology Resources" definition) are included in IT investment planning documents or artifacts;
- b) Decisions related to major IT investments are supported by business cases with appropriate evidence;
- c) IT investments implement an agile development approach, as appropriate;¹⁹
- d) IT investments support and enable core mission and operational functions and processes related to the agency's missions and business requirements;
- e) IT capital investment plans and budgetary requests are reviewed to ensure that Government-wide requirements, as well as any associated costs, are explicitly identified and included, with respect to any IT resources. This includes IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and

¹⁹ For additional information, refer to OMB memoranda at https://www.whitehouse.gov/omb/memoranda_default.

- f) Decisions to improve, enhance, or modernize existing IT investments or to develop new IT investments are made only after conducting an alternatives analysis that includes both government-provided (internal, interagency, and intra-agency where applicable) and commercially available options, and the option representing the best value to the Government has been selected.

4) Selection Criteria and Requirements

Agencies shall consider the following factors when analyzing IT investments:

- a) Qualitative and quantitative research methods are used to determine the goals, needs, and behaviors of current and prospective managers and users of the service to strengthen the understanding of requirements;
- b) All decisions concerning the selection of information system technologies and services including decisions to acquire or develop custom or duplicative solutions shall be merit-based and consider factors such as, but not limited to, ability to meet operational or mission requirements, total life cycle cost of ownership, performance, security, interoperability, privacy, accessibility, ability to share or reuse, resources required to switch vendors, and availability of quality support. Consistent with the FAR, contracts for custom software development are to include contractual provisions that reaffirm the right to reuse the software throughout the Federal Government;
- c) Agencies shall consider use of suitable existing Federal information technology resources and commercially-available solutions in order to ensure effective management of Federal resources. Consistent with law and regulation, agencies should consider and evaluate the suitability of existing Federal information technologies and related services, including software, Federal shared services, and commercially-available solutions before embarking upon new developments of software and information technologies; and
- d) Information systems security levels are commensurate with the impact that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information consistent with NIST standards and guidelines.

5) IT Investment Design and Management

Agencies shall implement the following requirements:

- a) Information systems and processes must support and maximize interoperability and access to information, where appropriate, by using documented, scalable, and continuously available application programming interfaces and open machine-readable formats;
- b) IT investments must facilitate interoperability, application portability, and scalability across networks of heterogeneous hardware, software, and communications platforms;
- c) Information systems, technologies, and processes shall facilitate accessibility under the Rehabilitation Act of 1973, as amended; in particular, see specific electronic and

IT accessibility requirements commonly known as “section 508” requirements (29 U.S.C. § 794d);

- d) Records management functions and retention and disposition requirements must be fully incorporated into information life cycle processes and stages, including the design, development, implementation, and decommissioning of information systems, particularly Internet resources to include storage solutions and cloud-based services such as software as a service, platform as a service, and infrastructure as a service; and
- e) IT investments use an Earned Value Management System (EVMS) and Integrated Baseline Review, when appropriate, as required by FAR Subpart 34.2. When an EVMS is required, agencies must have a documented process for accepting a contractor’s EVMS. Agencies are encouraged to share information about their acceptance process with other agencies and to consider recognizing each other’s acceptance of an EVMS so that a contractor is not required to complete a duplicative process. When an EVMS is not required, implement a baseline validation process as part of an overall investment risk management strategy consistent with OMB guidance.

e. Information Management and Access

- 1) Agencies shall incorporate the following steps, as appropriate, in planning, budgeting, governance, and other policies:
 - a) Federal information is properly managed throughout its life cycle, including all stages through which the information passes, such as: creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition;
 - b) Federal information is managed by making information accessible, discoverable, and usable by the public to the extent permitted by law and subject to privacy, security (which includes confidentiality), or other valid restrictions pertaining to access, use, dissemination, and disclosure;
 - c) Federal information is managed consistent with applicable records retention and disposition requirements;
 - d) Federal information and information systems are managed in a manner that identifies and mitigates privacy and security risks; and
 - e) Federal information is managed with clearly designated roles and responsibilities to promote effective and efficient design and operation of information resources management processes within their agency.
- 2) Agencies have a responsibility to provide information to the public consistent with their missions and subject to Federal law and policy. Agencies will discharge this responsibility by:
 - a) Publishing public information online in a manner that promotes analysis and reuse for the widest possible range of purposes, meaning that the information is publicly accessible, machine-readable, appropriately described, complete, and timely. This

includes providing such public information in a format(s) accessible to employees and members of the public with disabilities;²⁰

- b) Avoiding establishing, or permitting others to establish on their behalf, exclusive, restricted, or other distribution arrangements that interfere with the agency's ability to disseminate its public information on a timely and equitable basis;
 - c) Avoiding charging fees or royalties for public information or establishing unnecessary restrictions on the resale or re-dissemination of public information by the public. Agencies shall not, unless specifically authorized by statute, establish fees that exceed the cost of dissemination to the public, restrict or regulate the use, resale, or re-dissemination of public information by the public; or establish any mechanism that interferes with the timely and equitable availability of public information to the public;²¹
 - d) As appropriate, making Government publications available to depository libraries through the Government Publishing Office regardless of format;²²
 - e) Taking advantage of all dissemination channels, including Federal, State, local, tribal, and territorial governments, libraries and educational institutions, for-profit and nonprofit organizations, and private sector entities, in discharging agency information dissemination responsibilities; and
 - f) Considering the impact of providing agency information and services over the Internet for individuals who do not own computers or lack Internet access and, to the extent practicable, pursuing additional or alternative modes of delivery to ensure that such information and services are accessible to, and their availability is not diminished for, such individuals.
- 3) Agencies shall establish policies, procedures, and standards that enable data governance so that information is managed and maintained according to relevant statute, regulations, and guidance.
 - 4) Agencies shall collect or create information in a way that supports downstream interoperability among information systems and streamlines dissemination to the public, where appropriate, by creating or collecting all new information electronically by default, in machine-readable open formats, using relevant data standards, that upon creation includes standard extensible metadata in accordance with OMB guidance.
 - 5) Agencies shall include appropriate provisions in contracts, and other agreements, to encourage recipients of Federal funding to maximize access to data developed under an award and to prepare data management plans that describe data to be created in funded programs and approaches for long-term preservation and access to created data.

²⁰ Pursuant to Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794d).

²¹ Pursuant to the Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35).

²² Pursuant to the Depository Library Act of 1962 (44 U.S.C. Chapter 19).

- 6) Agencies shall ensure that there is a mechanism for the public to provide feedback about public information.
- 7) Agencies shall manage information in accordance with the following principles as appropriate:
 - a) Providing notice of Federal agency practices for the creation, collection, use, processing, preservation, storage, maintenance, disclosure, dissemination, and disposal of information, as appropriate;
 - b) Providing adequate notice when initiating, substantially modifying, or terminating dissemination of significant information that the public may be using;
 - c) Identifying the source of the information disseminated to the public, if from outside the agency, where practicable;
 - d) Considering target audiences of Federal information when determining format, frequency of update, and other information management decisions;
 - e) Considering the impact of decisions and actions in each stage of the information life cycle on other stages;
 - f) Considering the effects of information management actions on members of the public and State, local, tribal and territorial governments and their access to Federal information and ensure consultation with the public and those governments as appropriate;
 - g) Seeking to satisfy new information needs through interagency or intergovernmental sharing of information, or through nongovernmental sources, where lawful and appropriate, before creating or collecting new information; and
 - h) Complying with all applicable statutes and policies governing the disclosure or dissemination of information, including those related to the quality, privacy, security, accessibility, and other valid access, use, and dissemination restrictions.

f. Privacy and Information Security²³

1) Privacy

Agencies shall:

- a) Establish and maintain a comprehensive privacy program that ensures compliance with applicable privacy requirements, develops and evaluates privacy policy, and manages privacy risks;²⁴
- b) Designate an SAOP who has agency-wide responsibility and accountability for developing, implementing, and maintaining an agency-wide privacy program to

²³ Although this section includes requirements for protecting Federal information resources, this area is covered more fully in the Appendices to this Circular.

²⁴ When considering privacy risks, privacy programs shall consider the risks to an individual or individuals associated with the agency's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of their PII.

ensure compliance with all applicable statutes, regulations, and policies regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems, developing and evaluating privacy policy, and managing privacy risks at the agency;²⁵

- c) Monitor Federal law, regulation, and policy for changes that affect privacy;
- d) Limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of agency functions;
- e) To the extent reasonably practicable, ensure that PII is accurate, relevant, timely, and complete, and reduce all PII to the minimum necessary for the proper performance of authorized agency functions;
- f) Take steps to eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to the use of Social Security numbers as a personal identifier;
- g) Comply with all applicable privacy-related laws, including the requirements of the Privacy Act,²⁶ and ensure that the Privacy Act system of records notices are published, revised, and rescinded, as required;
- h) Maintain all records with PII in accordance with applicable records retention or disposition schedules approved by the National Archives and Records Administration (NARA);
- i) Conduct privacy impact assessments when developing, procuring, or using IT, in accordance with the E-Government Act,²⁷ and make the privacy impact assessments available to the public in accordance with OMB policy;
- j) Maintain and post privacy policies on all agency websites, mobile applications, and other digital services, in accordance with the E-Government Act and OMB policy; and
- k) Ensure that the SAOP and the agency's privacy personnel closely coordinate with the agency CIO, senior agency information security officer, and other agency offices and officials, as appropriate.

²⁵ The SAOP shall be designated by the head of the agency, pursuant to Executive Order 13719, *Establishment of the Federal Privacy Council* (2016), and OMB guidance.

²⁶ Agencies should also consult OMB policies on privacy, and OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.

²⁷ Section 208(b) of the E-Government Act requires agencies, absent an applicable exception under that section, to conduct a PIA before: (i) developing or procuring IT that collects, maintains, or disseminates information that is in an identifiable form; or (ii) initiating a new collection of information that – (I) will be collected, maintained, or disseminated using IT; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

2) Information Security

To provide proper safeguards, agencies shall:

- a) Ensure that the CIO designates a senior agency information security officer to develop and maintain an agency-wide information security program in accordance with the Federal Information Security Modernization Act of 2014 (FISMA);
- b) Protect information in a manner commensurate with the risk that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information; and
- c) Implement security policies issued by OMB, as well as requirements issued by the Department of Commerce, the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Office of Personnel Management (OPM). This includes applying the standards and guidelines contained in the NIST FIPS, NIST SPs (e.g., 800 series guidelines), and where appropriate and directed by OMB, NIST Interagency or Internal Reports (NISTIRs).²⁸

g. Electronic Signatures²⁹

To support the transition to electronic government, agencies shall:

- 1) Allow individuals or entities that deal with the agencies the option to submit information or transact with the agency electronically, when practicable, and for agencies to maintain records electronically, when practicable. Electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form;³⁰
- 2) Promote the use of electronic contract formation, signatures, and recordkeeping in private commerce by establishing legal equivalence between: contracts written on paper and contracts in electronic form; pen-and-ink signatures and electronic signatures; and other legally required written documents (termed “records”) and the same information in electronic form; and³¹

²⁸ NISTIRs describe research of a technical nature of interest to a specialized audience.

²⁹ In support of Government Paperwork Elimination Act (GPEA) and Electronic Signatures in Global and National Commerce Act (E-Sign), the Federal Chief Information Officers Council maintains guidance on use of Electronic Signatures (E-Signatures) in Federal organization transactions. The Federal Chief Information Officers Council guidance, *Use of Electronic Signatures in Federal Organization Transactions*, can be located at <https://www.idmanagement.gov>. This guidance expands upon OMB guidance.

³⁰ Pursuant to the Government Paperwork Elimination Act of 1998 (44 U.S.C. § 3504).

³¹ Pursuant to E-Sign (15 U.S.C. Chapter 96). E-Sign applies broadly to commercial, consumer, and business transactions affecting interstate or foreign commerce, and to transactions regulated by both Federal and State Government.

- 3) Develop and implement processes to support use of digital signatures, a form of electronic signature, for employees and contractors.³²

h. Records Management

Agencies shall:

- 1) Designate a senior agency official for records management (SAORM) who has overall agency-wide responsibility for records management;
- 2) Institute records management programs that provide documentation of agency activities;³³
- 3) Manage electronic records in accordance with Government-wide requirements. This includes:
 - a) Managing all permanent electronic records electronically to the fullest extent possible for eventual transfer and accessioning by NARA in an electronic format; and
 - b) Managing all email records electronically and retaining them in an appropriate electronic system that supports records management and litigation requirements, including the capability to identify, retrieve, and retain the records for as long as they are needed;
- 4) Ensure the ability to access, retrieve, and manage records throughout their life cycle regardless of form or medium;
- 5) Ensure agency records managed by the SAORM are treated as information resources and follow the requirements in this Circular;
- 6) Establish and obtain the approval of the Archivist of the United States for retention schedules for Federal records in a timely fashion;
- 7) Ensure the proper and timely disposition of Federal records in accordance with a retention schedule approved by the Archivist of the United States; and
- 8) Provide training and guidance, as appropriate, to all agency employees and contractors regarding their Federal records management responsibilities.

i. Leveraging the Evolving Internet

In a global and connected economy, it is essential for the United States and the Federal Government to strive to ensure that Internet-based technologies remain competitive. The Federal Government needs to continue to lead in innovation, contribute to the free flow of information, participate in an open and available market, and do this in a way that is scalable and secure. Networking demands, escalating with the continued emergence of connecting technologies, has grown well beyond initial capabilities. The use of the newest Internet Protocol (currently, Internet Protocol Version 6 [IPv6]) is an essential part of accomplishing

³² Digital signatures can help agencies streamline mission or business processes and transition manual processes to more automated processes to include, for example, online transactions.

³³ Additional information regarding adequate and proper documentation is available in 36 C.F.R. § 1222.22.

these goals and ensuring that the network infrastructure can meet our needs for growing capacity, security, and privacy, and keep the United States competitive in the ever-escalating global electronic economy. Therefore, agencies shall:

- 1) Implement agency-wide processes requiring that all IT acquisitions using Internet Protocol conform to the FAR; and³⁴
- 2) Ensure that all public-facing Internet services and enterprise networks fully support the newest version of Internet Protocol as required by OMB policy.

6. Government-wide Responsibilities

a. Department of Commerce

The Secretary of Commerce shall:

- 1) Develop and issue standards and guidelines for the security and privacy of information in Federal information systems and systems which create, collect, process, store, transmit, disseminate, or dispose of information on behalf of the Federal Government;³⁵
- 2) Provide OMB and the agencies with scientific and technical advisory services relating to the development and use of IT;³⁶
- 3) Conduct studies and evaluations concerning telecommunications technology, and the improvement, expansion, testing, operation, and use of Federal telecommunications systems, and advise the Director of OMB and appropriate agencies of the recommendations that result from such studies;³⁷
- 4) Develop, in consultation with the Secretary of State and the Director of OMB, plans, policies, and programs relating to international telecommunications issues affecting Federal information activities;³⁸
- 5) Identify needs for standardization of telecommunications and information processing technology, and develop standards, in consultation with the Secretary of Defense and the Administrator of General Services, to ensure efficient application of such technology;³⁹

³⁴ When acquiring information technology using Internet Protocol, agencies must include the appropriate Internet Protocol compliance requirements in accordance with § 11.002(g) of the FAR. For additional information, refer to <https://www.acquisition.gov/>.

³⁵ National Institute of Standards and Technologies (NIST) Act, 15 U.S.C. § 278g-3.

³⁶ Pursuant to the NIST Act (15 U.S.C. § 278g-3).

³⁷ Pursuant to the National Telecommunications and Information Administration (NTIA) Organization Act, as amended (47 U.S.C. § 902(b)(2)(F)).

³⁸ Pursuant to the NTIA Organization Act, as amended (47 U.S.C. §902(b)(2)(G)).

³⁹ Pursuant to the NIST Act, 15 U.S.C. §§ 272(b), 278g-3, and OMB A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.

- 6) Ensure that the Federal Government is represented in the development of national and international (in consultation with the Secretary of State) IT standards, and advise the Director of OMB on such activities;⁴⁰
- 7) Evaluate new information technologies to assess their security vulnerabilities, with technical assistance from the Department of Defense (DOD) and DHS;
- 8) Solicit and consider the recommendations of the Information Security and Privacy Advisory Board regarding such standards and guidelines;⁴¹ and
- 9) Lead the development of a Cybersecurity Framework to reduce cyber risks to critical infrastructure pursuant to Executive Order 13636, Improving Critical Infrastructure Cybersecurity.

b. Department of Homeland Security

The Secretary of Homeland Security shall:⁴²

- 1) Perform its responsibilities under FISMA, including assisting OMB in carrying out its statutory authorities and functions of information security oversight and policy responsibilities;⁴³
- 2) Develop and oversee the implementation of binding operational directives pursuant to FISMA;⁴⁴
- 3) Monitor agency implementation of information security policies and practices;
- 4) Convene meetings with senior agency officials to help ensure effective implementation of information security policies and procedures;
- 5) Coordinate Government-wide efforts on information security policies and practices, including consultation with the Federal Chief Information Officers Council, and the Director of NIST;
- 6) Provide operational and technical assistance to agencies in implementing policies, principles, standards, and guidelines on information security, including implementation of standards promulgated under 40 U.S.C. § 11331, including by:
 - a) Operating the Federal information security incident center established under 44 U.S.C. § 3556;
 - b) Upon request by an agency, deploying technology to assist the agency to continuously diagnose and mitigate cyber threats and vulnerabilities, with or without reimbursement;

⁴⁰ Pursuant to NIST Act, 15 U.S.C. §§ 272(b), 273, 278g-3 and OMB A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.

⁴¹ Pursuant to the National Institute of Standards and Technology Act (15 U.S.C. §278g-4).

⁴² Pursuant to FISMA (44 U.S.C. § 3553).

⁴³ FISMA, 44 U.S.C. § 3553(b)(1).

⁴⁴ FISMA, 44 U.S.C. § 3553(b)(2).

- c) Compiling and analyzing data on agency information security; and
 - d) Developing and conducting targeted operational evaluations, including threat and vulnerability assessments, on the information systems;
- 7) Consult with the Director of NIST regarding any binding operational directives that implements the standards and guidelines developed by NIST;
 - 8) Coordinate the development of binding operational directives and the oversight of the implementation of such directives with OMB to ensure consistency with OMB policies;
 - 9) Ensure that binding operational directives do not conflict with the guidelines issued under 40 U.S.C. § 11331;
 - 10) Take other actions as the Director of OMB or the Secretary, in consultation with the Director of OMB, may determine necessary to carry out the implementation of effective agency information security policies and practices for information systems;
 - 11) Manage Government-wide information security programs and provide and operate Federal information security shared services, in coordination with OMB and in accordance with OMB policies;
 - 12) Provide, as appropriate, intelligence and other information about cyber threats, vulnerabilities, and incidents to agencies to assist in risk assessments conducted under FISMA;⁴⁵ and
 - 13) Solicit and consider the recommendations of the Information Security Privacy Advisory Board, established by the National Institute of Standards and Technology Act (NIST Act).⁴⁶
- c. Federal Chief Information Officers Council (Federal CIO Council)
- Pursuant to the E-Government Act of 2002, the Federal CIO Council shall:⁴⁷
- 1) Develop recommendations for OMB on Government information resources management policies and requirements;
 - 2) Share experiences, ideas, best practices, and innovative approaches related to information resources management;
 - 3) Assist OMB in the identification, development, and coordination of multiagency projects and other innovation initiatives to improve Federal Government performance through use of IT;
 - 4) Promote the development and use of common performance measures for agency information resources management, as further described in statute;

⁴⁵ 44 U.S.C. § 3556(a)(4).

⁴⁶ Pursuant to DHS current practices.

⁴⁷ E-Government Act of 2002 (44 U.S.C. § 3603).

- 5) Work as appropriate with NIST and OMB to develop recommendations on IT standards developed under the NIST Act and promulgated under section 11331 of title 40, and maximize the use of commercial standards, as further described in statute;
- 6) Work with OPM to assess and address the hiring, training, classification, and professional development needs of the Federal Government related to information resources management;
- 7) Work with the Archivist of the United States to assess how the Federal Records Act can be addressed effectively by Federal information resources management activities; and
- 8) Solicit perspectives from the Chief Financial Officers Council, Federal Acquisition Officers Council, Chief Human Capital Officers' Council, Budget Officers Advisory Council, and other key groups in the Federal Government, as well as industry, academia, and other Federal, State, local, tribal and territorial governments, on matters of concern to the Council as appropriate.

d. Federal Privacy Council

Pursuant to Executive Order 13719, the Federal Privacy Council shall:⁴⁸

- 1) Develop recommendations for OMB on Federal Government privacy policies and requirements;
- 2) Coordinate and share ideas, best practices, and approaches for protecting privacy and implementing appropriate privacy safeguards;
- 3) Assess and recommend how best to address the hiring, training, and professional development needs of the Federal Government with respect to privacy matters;
- 4) Perform other privacy-related functions, consistent with law, as designated by the Chair of the Federal Privacy Council; and
- 5) In performing its duties, engage in appropriate coordination as described in Executive Order 13719.⁴⁹

⁴⁸ Executive Order 13719, *Establishment of the Federal Privacy Council* (2016).

⁴⁹ Executive Order 13719, *Establishment of the Federal Privacy Council* (2016) at § 4(d), "Coordination":

- (i) The Chair and the Privacy Council shall coordinate with the Federal Chief Information Officers Council (CIO Council) to promote consistency and efficiency across the executive branch when addressing privacy and information security issues. In addition, the Chairs of the Privacy Council and the CIO Council shall coordinate to ensure that the work of the two councils is complementary and not duplicative.
- (ii) The Chair and the Privacy Council should coordinate, as appropriate, with such other interagency councils and councils and offices within the Executive Office of the President, as appropriate, including the President's Management Council, the Chief Financial Officers Council, the President's Council on Integrity and Efficiency, the National Science and Technology Council, the National Economic Council, the Domestic Policy Council, the National Security Council staff, the Office of Science and Technology Policy, the Interagency Council on Statistical Policy, the Federal Acquisition Regulatory Council, and the Small Agency Council.

e. General Services Administration

The Administrator of General Services shall:

- 1) Provide a Government-wide network services contract that leverages shared solutions for many agencies;⁵⁰
- 2) Ensure that contract vehicles and services made available to agencies are cost-effective and provide for capabilities that are consistent with Government-wide requirements;⁵¹
- 3) Assist OMB in setting strategic direction for electronic government and overseeing Government-wide implementation, and recommend changes relating to Government-wide strategies and priorities;⁵²
- 4) Promote innovative uses of IT by agencies, particularly initiatives involving multiagency collaboration, through support of pilot projects, research, experimentation, and the use of innovative technologies;⁵³
- 5) Maintain a Federal public key infrastructure (PKI) framework to allow efficient interoperability among agencies when using digital certificates;⁵⁴ and
- 6) Ensure that effective controls are in place to protect the confidentiality, integrity, and availability of the Federal PKI framework components managed and overseen by the agency, to include performing information security continuous monitoring of the Federal PKI.

f. National Archives and Records Administration

The Archivist of the United States shall:

- 1) Administer the Federal Records Act and NARA regulations (36 CFR Subchapter B Records Management);⁵⁵
- 2) Develop regulations relating to electronic records management;⁵⁶
- 3) Work with agencies to ensure the transfer of permanent Federal electronic records to the National Archives of the United States in digital or electronic form to the greatest extent possible;⁵⁷

⁵⁰ Pursuant to the Clinger-Cohen Act (also known as the “Information Technology Management Reform Act of 1996”) (40 U.S.C. § 11314(b)).

⁵¹ Pursuant to the Clinger-Cohen Act (also known as the “Information Technology Management Reform Act of 1996”) (40 U.S.C. §§ 11302, 11314(a)).

⁵² Pursuant to the E-Government Act of 2002 (44 U.S.C. § 3602).

⁵³ Pursuant to the E-Government Act of 2002 (44 U.S.C. § 3602).

⁵⁴ Federal PKI provides the government with a common infrastructure to administer digital certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

⁵⁵ Pursuant to the Federal Records Act of 1950, as amended, codified (44 U.S.C. Chapters 21, 29, 31, 33).

⁵⁶ Pursuant to the Federal Records Act of 1950, as amended, codified (44 U.S.C. Chapters 31 and 33).

⁵⁷ Pursuant to the Federal Records Act of 1950, as amended, codified (44 U.S.C. Chapters 21, 29, 31, 33).

- 4) Ensure agency compliance with records management requirements, provide records management training, and facilitate public access to high-value Government records;⁵⁸ and
- 5) Serve as the Executive Agent for the Controlled Unclassified Information (CUI) program.⁵⁹

g. Office of Personnel Management

The Administrator of the Office of Personnel Management shall:⁶⁰

- 1) Analyze, on an ongoing basis, the workforce needs of the Federal Government related to IT and information resources management, in conjunction with relevant agencies;
- 2) Identify training needs of the Federal Government workforce related to IT and information resources management;
- 3) Oversee the development of curricula, training methods, and training priorities that correspond to the projected personnel needs related to IT and information resources management; and
- 4) Assess the training of employees in IT disciplines to address information resources management needs.

7. Effectiveness

This Circular is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

8. Oversight

The Director of OMB shall use IT planning reviews, fiscal budget reviews, information collection reviews, management reviews, and such other measures as the Director deems necessary to evaluate the adequacy and efficiency of each agency's information resources management and compliance with this Circular.

The Director of OMB may, consistent with statute and upon written request of an agency, grant a waiver from particular requirements of this Circular. Requests for waivers must detail the reasons why a particular waiver is sought, identify the duration of the waiver sought, and include a plan for the prompt and orderly transition to full compliance with the requirements of this Circular. Notice of each waiver request must be published promptly by the agency in the Federal Register, with a copy of the waiver request made available to the public on request.

⁵⁸ Pursuant to the Federal Records Act of 1950, as amended, codified (44 U.S.C. Chapters 21, 29, 31, 33).

⁵⁹ Pursuant to Executive Order 13556, *Controlled Unclassified Information*.

⁶⁰ Pursuant to the E-Government Act of 2002 (44 U.S.C. § 3501 note; Pub. L. 107-347, § 209(b)(1)).

9. Authority

OMB issues this Circular pursuant to the Clinger-Cohen Act (also known as the “Information Technology Management Reform Act of 1996”) (40 U.S.C. § 11101-11704); E-Government Act of 2002 (44 U.S.C. Chapters 35 and 36); Federal Information Security Modernization Act of 2014 (44 U.S.C. Chapter 35, Subchapter II); Federal Information Technology Acquisition Reform Act (FITARA) (Pub. L. 113-291)⁶¹; Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35); Privacy Act of 1974, as amended (5 U.S.C. § 552a); Digital Accountability and Transparency Act of 2014 (Pub. L. 113-101); Electronic Signatures in Global and National Commerce Act (E-Sign) (15 U.S.C. Chapter 96); Government Paperwork Elimination Act of 1998 (44 U.S.C. § 3504); Government Performance and Results Act (GPRA) of 1993, as amended by the Government Performance and Results Modernization Act (GPRA Modernization Act) of 2010 (5 U.S.C. § 306 and 31 U.S.C. §§ 1115 et seq.); Office of Federal Procurement Policy Act (41 U.S.C. Chapter 7); Budget and Accounting Procedures Act of 1950, as amended (31 U.S.C. Chapter 11); Chief Financial Officers Act (31 U.S.C. § 3512 et seq.); and Executive Order 13719, Establishment of the Federal Privacy Council (2016).

10. Definitions

a. The following definitions are applicable within this policy:

- 1) ‘Accessibility’ means information technology products or services that are in full compliance with the standards of section 508 of the Rehabilitation Act of 1973.⁶²
- 2) ‘Adequate security’ means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.
- 3) ‘Agency’ means any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency.
- 4) ‘Agency Strategic Plan’ means a plan that provides general and long-term goals that the agency aims to achieve, the actions the agency will take to realize those goals, the

⁶¹ Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, Pub. L. 113-291. Further references in the text that refer to “FITARA” refer to these sections.

⁶² The United States Architectural and Transportation Barriers Compliance Board’s (Access Board) Information and Communication Technology Standards and Guidelines for information and communications technologies (ICT), known as the Section 508 Standards. The 508 standards apply to ICT developed, procured, maintained, or used by Federal agencies covered by section 508 of the Rehabilitation Act of 1973 (29 U.S.C. § 794d), as amended. Accessibility also refers to the guidelines for telecommunications equipment and customer premises equipment covered by Section 255 of the Communications Act of 1934 (47 U.S.C. § 151 *et seq.*).

strategies planned, how the agency will deal with challenges and risks that may hinder achieving results, and the approaches it will use to monitor its progress.⁶³

- 5) ‘Agile Development’ means a development methodology that uses an iterative approach to deliver solutions incrementally through close collaboration and frequent reassessment.
- 6) ‘Authorization to Operate’ means the official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.
- 7) ‘Authorization boundary’ means all components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected.⁶⁴
- 8) ‘Authorization package’ means the essential information that an authorizing official uses to determine whether to authorize the operation of an information system or the use of a designated set of common controls. At a minimum, the authorization package includes the information system security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.
- 9) ‘Authorizing official’ means a senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation.
- 10) ‘Binding Operational Directive’ means a compulsory direction from the Department of Homeland Security to an agency that is for the purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk; shall be in accordance with policies, principles, standards, and guidelines issued by the Director of the Office of Management and Budget; and may be revised or repealed by the Director if the direction issued on behalf of the Director is not in accordance with policies and principles developed by the Director (44 U.S.C. § 3552).
- 11) ‘Business Continuity Plan’ means a plan that focuses on sustaining an organization’s mission or business processes during and after a disruption, and may be written for

⁶³ For additional information, refer to the Government Performance and Results Act (GPRA) of 1993, as amended by the Government Performance and Results Modernization Act (GPRA Modernization Act) of 2010 (5 U.S.C. § 306 and 31 U.S.C. § 1115 *et seq.*); and OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*.

⁶⁴ Agencies have significant flexibility in determining what constitutes an information system and its associated boundary.

mission or business processes within a single business unit or may address the entire organization's processes.⁶⁵

- 12) 'Chief Information Officer' means the senior official that provides advice and other assistance to the head of the agency and other senior management personnel of the agency to ensure that IT is acquired and information resources are managed for the agency in a manner that achieves the agency's strategic goals and information resources management goals; and is responsible for ensuring agency compliance with, and prompt, efficient, and effective implementation of, the information policies and information resources management responsibilities, including the reduction of information collection burdens on the public.
- 13) 'Chief Information Officers Council' means the Council codified in the E-Government Act of 2002 (44 U.S.C § 101).
- 14) 'Common control' means a security or privacy control that is inherited by multiple information systems or programs.⁶⁶
- 15) 'Controlled Unclassified Information' means information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.
- 16) 'Critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health safety, or any combination of those matters (42 U.S.C. § 5195c(e)).
- 17) 'Cybersecurity' means prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.
- 18) 'Dissemination' means the government-initiated distribution of information to a nongovernment entity, including the public. The term 'dissemination,' as used within this Circular, does not include distribution limited to Federal Government employees, intra- or interagency use or sharing of Federal information, and responses to requests for agency records under the Freedom of Information Act (5 U.S.C. § 552) or the Privacy Act (5 U.S.C. § 552a).
- 19) 'Enterprise architecture' (a) means (i) a strategic information asset base, which defines the mission; (ii) the information necessary to perform the mission; (iii) the technologies necessary to perform the mission; and (iv) the transitional processes for implementing

⁶⁵ The Federal Information Security Modernization Act (44 U.S.C. § 3554(b)) requires each agency to develop, document, and implement an agency-wide information security program that includes plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

⁶⁶ A control is inherited by an information system when the control is selected for the system but the control is developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system.

new technologies in response to changing mission needs; and (b) includes (i) a baseline architecture; (ii) a target architecture; and (iii) a sequencing plan (44 U.S.C. § 3601).

- 20) 'Environment of operation' means the physical surroundings in which an information system processes, stores, and transmits information.
- 21) 'Executive agency' has the meaning defined in Title 41, Public Contracts section 133 (41 U.S.C. § 133).
- 22) 'Federal information' means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.
- 23) 'Federal information system' means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency.
- 24) 'Federal Privacy Council' means the Council established by Executive Order 13719.⁶⁷
- 25) 'Government publication' means information that is published as an individual document at Government expense, or as required by law, in any medium or form (44 U.S.C. § 1901).
- 26) 'Hybrid control' means a security or privacy control that is implemented for an information system in part as a common control and in part as a system-specific control.
- 27) 'Incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies (44 U.S.C. § 3552).
- 28) 'Information' means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms.
- 29) 'Information dissemination product' means any recorded information, regardless of physical form or characteristics, disseminated by an agency, or contractor thereof, to the public.
- 30) 'Information life cycle' means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion.
- 31) 'Information management' means the planning, budgeting, manipulating, and controlling of information throughout its life cycle. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology.
- 32) 'Information resources' means information and related resources, such as personnel, equipment, funds, and information technology (44 U.S.C. § 3502).

⁶⁷ Executive Order 13719, *Establishment of the Federal Privacy Council* (2016).

- 33) 'Information resources management' means the process of managing information resources to accomplish agency missions. The term encompasses an agency's information and the related resources, such as personnel, equipment, funds, and information technology (44 U.S.C. § 3502).
- 34) 'Information Resource Management Strategy' means a strategy that demonstrates how information resources management decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions (44 U.S.C. 3506 (b)(2)).
- 35) 'Information security' means the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:
 - a) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
 - b) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
 - c) Availability, which means ensuring timely and reliable access to and use of information (44 U.S.C. § 3552).
- 36) 'Information security architecture' means an embedded, integral part of the enterprise architecture that describes the structure and behavior of the enterprise security processes, information security systems, personnel, and organizational subunits, showing their alignment with the enterprise's mission and strategic plans.
- 37) 'Information security continuous monitoring' means maintaining ongoing awareness of information security, vulnerabilities, threats, and incidents to support agency risk management decisions.⁶⁸
- 38) 'Information security continuous monitoring program' means the compendium of methods, tools, and techniques necessary to implement the agency information continuous monitoring strategy in a way that is sufficient to inform risk-based decisions and maintain operations within established risk tolerances. The program includes determining monitoring metrics, establishing monitoring frequencies, and developing a monitoring architecture.
- 39) 'Information security continuous monitoring strategy' means a comprehensive plan to address monitoring requirements and activities at each organizational tier (organization, mission or business process, and information system).
- 40) 'Information system security plan' means a formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.⁶⁹

⁶⁸ The terms *continuous* and *ongoing* in this context mean that security controls and agency risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect agency information.

⁶⁹ The information system security plan and the privacy plan may be integrated into one consolidated document.

- 41) 'Information security program plan' means a formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.
- 42) 'Information system' means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. § 3502).
- 43) 'Information system life cycle' means all phases in the useful life of an information system, including planning, acquiring, operating, maintaining, and disposing. (See also OMB A-11 Part 7, *Capital Programming Guide* and OMB Circular A-131, *Value Engineering* for more information regarding the costs and management of assets through their complete life cycle.)
- 44) 'Information system resilience' means the ability of an information system to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities, and to recover to an effective operational posture in a time frame consistent with mission needs.
- 45) 'Information technology' means any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use (40 U.S.C. § 11101).
- 46) 'Information technology investment' means an expenditure of information technology resources to address mission delivery and management support. This may include a project or projects for the development, modernization, enhancement, or maintenance of a single information technology asset or group of information technology assets with related functionality, and the subsequent operation of those assets in a production environment. These investments shall have a defined life cycle with start and end dates, with the end date representing the end of the currently estimated useful life of the investment, consistent with the investment's most current alternatives analysis if applicable.
- 47) 'Information Technology Investment Management' means a decision-making process that, in support of agency missions and business needs, provides for analyzing, tracking, and evaluating the risks, including information security and privacy risks, and results of

all major investments made by an agency for information systems. The process shall cover the life of each system and shall include explicit criteria for analyzing the projected and actual costs, benefits, and risks, including information security and privacy risks, associated with the investments.⁷⁰

- 48) ‘Information technology resources’ means all agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, or other activity related to the life cycle of information technology; acquisitions or interagency agreements that include information technology and the services or equipment provided by such acquisitions or interagency agreements; but does not include grants that establish or support information technology not operated directly by the Federal Government.
- 49) ‘Initial authorization’ means the initial risk determination and risk acceptance decision based on a zero-base review⁷¹ of the information system conducted prior to its entering the operations or maintenance phase of the system development life cycle. The zero-base review includes an assessment of all security and privacy controls (i.e., system-specific, hybrid, and common controls) contained in an information system security plan or in a privacy plan and implemented within an information system or the environment in which the system operates.
- 50) ‘Interagency agreement’ means, for the purposes of this document, a written agreement entered into between two or more Federal agencies that specifies the goods to be furnished or tasks to be accomplished by one agency (the servicing agency) in support of the other(s) (the requesting agency), including assisted acquisitions as described in OMB Memorandum: *Improving the Management and Use of Interagency Acquisitions* and other cases described in FAR Part 17.
- 51) ‘Major information system’ means a system that is part of an investment that requires special management attention as defined in OMB guidance⁷² and agency policies, a “major automated information system” as defined in 10 U.S.C. § 2445, or a system that is part of a major acquisition as defined in the OMB Circular A-11, *Capital Programming Guide*, consisting of information resources.⁷³
- 52) ‘Major information technology investment’ means an investment that requires special management attention as defined in OMB guidance and agency policies, a “major automated information system” as defined in 10 U.S.C. § 2445, or a major acquisition as

⁷⁰ See the Clinger Cohen Act of 1996 (40 U.S.C. § 11302) for statutory requirements.

⁷¹ A zero-base review of an information system is the first complete security assessment performed in order to provide the authorizing official with a comprehensive set of security-related information to facilitate making an appropriate risk determination.

⁷² For example, an information system requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

⁷³ All information systems are subject to the requirements of the Federal Information Security Modernization Act (44 U.S.C. Chapter 35) whether or not they are designated as a major information system.

defined in the OMB Circular A-11, *Capital Programming Guide*, consisting of information resources.

- 53) 'National security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy (44 U.S.C. § 3552).
- 54) 'Ongoing authorization' means the risk determinations and risk acceptance decisions subsequent to the initial authorization, taken at agreed-upon and documented frequencies in accordance with the agency's mission or business requirements and agency risk tolerance. Ongoing authorization is a time-driven or event-driven authorization process whereby the authorizing official is provided with the necessary and sufficient information regarding the security and privacy state of the information system to determine whether the mission or business risk of continued system operation is acceptable.
- 55) 'Open data' means publicly available data that are made available consistent with relevant privacy, confidentiality, security, and other valid access, use, and dissemination restrictions, and are structured in a way that enables the data to be fully discoverable and usable by end users. Generally, open data are consistent with principles, explained in OMB guidance, of such data being public, accessible, machine-readable, described, reusable, complete, timely, and managed post-release.
- 56) 'Overlay' means a specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. (See "tailoring" definition.)
- 57) 'Personally identifiable information' means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
- 58) 'Privacy continuous monitoring' means maintaining ongoing awareness of privacy risks and assessing privacy controls at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.
- 59) 'Privacy continuous monitoring program' means an agency-wide program that implements the agency's privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to

information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at an agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks.

- 60) 'Privacy continuous monitoring strategy' means a formal document that catalogs the available privacy controls implemented at an agency across the agency risk management tiers and ensures that the controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.
- 61) 'Privacy control' means the administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.
- 62) 'Privacy control assessment' means the assessment of privacy controls to determine whether the controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks. A privacy control assessment is both an assessment and a formal document detailing the process and the outcome of the assessment.
- 63) 'Privacy impact assessment' means an analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis.
- 64) 'Privacy program plan' means a formal document that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.
- 65) 'Privacy plan' means a formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls.⁷⁴
- 66) 'Program management control' means, in the context of information security and privacy, a control that is generally implemented at the agency level, independent of any

⁷⁴ The privacy plan and the information system security plan may be integrated into one consolidated document.

particular information system, and essential for managing information security or privacy programs.

- 67) ‘Provisioned IT Service’ means an information technology service that is owned, operated, and provided by an outside vendor or external government organization, and consumed by the agency.
- 68) ‘Public information’ means any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public (44 U.S.C. Chapter 35).
- 69) ‘Reauthorization’ means the risk determination and risk acceptance decision that occurs after an initial authorization. In general, reauthorization actions may be time-driven or event-driven; however, under ongoing authorization, reauthorization is typically an event-driven action initiated by the authorizing official or directed by the Risk Executive (function) in response to an event that drives risk above the previously agreed-upon agency risk tolerance.
- 70) ‘Records’ means all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them (44 U.S.C. § 3301).
- 71) ‘Records management’ means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations (44 U.S.C. § 2901(2)).
- 72) ‘Resilience’ means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.
- 73) ‘Risk’ means a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.⁷⁵
- 74) ‘Risk management’ means the program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.
- 75) ‘Risk management strategy’ means the description of how an agency intends to assess risk, respond to risk, and monitor risk, making explicit and transparent the risk

⁷⁵ Risk can include both information security and privacy risks.

perceptions that organizations routinely use in making both investment and operational decisions.

- 76) 'Risk response' means accepting, avoiding, mitigating, sharing, or transferring risk to agency operations, agency assets, individuals, other organizations, or the Nation.
- 77) 'Security category' means the characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on agency operations, agency assets, individuals, other organizations, and the Nation.
- 78) 'Security control' means the safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.
- 79) 'Security control assessment' means the testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.
- 80) 'Security control baseline' means the set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.
- 81) 'Senior Agency Official for Privacy' means the senior official, designated by the head of each agency, who has agency-wide responsibility for privacy, including implementation of privacy protections; compliance with Federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals.
- 82) 'Senior Agency Official for Records Management' means the senior official who has direct responsibility for ensuring that the agency efficiently and appropriately complies with all applicable records management statutes, regulations, NARA policy and OMB policy.
- 83) 'Supply chain' means a linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.
- 84) 'Supply chain risk' means risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
- 85) 'Supply chain risk management' means the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of information and communications technology product and service supply chains.
- 86) 'System-specific control' means a security or privacy control for an information system that is implemented at the system level and is not inherited by any other information system.

- 87) ‘Systems security engineering’ means a specialty engineering discipline of systems engineering. It applies scientific, mathematical, engineering, and measurement concepts, principles, and methods to deliver, consistent with defined constraints and necessary trade-offs, a trustworthy asset protection capability that satisfies stakeholder requirements; is seamlessly integrated into the delivered system; and presents residual risk that is deemed acceptable and manageable to stakeholders.
- 88) ‘Tailoring’ means the process by which security control baselines are modified by identifying and designating common controls; applying scoping considerations; selecting compensating controls; assigning specific values to agency-defined control parameters; supplementing baselines with additional controls or control enhancements; and providing additional specification information for control implementation. The tailoring process may also be applied to privacy controls. (See “overlay” definition.)
- 89) ‘TechStat’ means a face-to-face, evidence-based accountability review of an IT investment that enables the Federal Government to intervene to turn around, halt, or terminate IT projects that are failing or are not producing results for the American people.
- 90) ‘Trustworthy information system’ means an information system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.
- b. Terms that are not specifically defined in this section are assumed to have standard dictionary meanings, or are defined in other OMB policy.

11. Inquiries

All questions or inquiries should be addressed to the Office of Management and Budget, Washington, D.C. 20503. Telephone: (202) 395-0379 or (202) 395-3785 or Email: A130@omb.eop.gov.

Appendix I to OMB Circular A-130
Responsibilities for Protecting and Managing Federal Information Resources

1. Introduction

Agencies of the Federal Government depend on the secure acquisition, processing, storage, transmission, and disposition of information to carry out their core missions and business functions. This allows diverse information resources ranging from large enterprise information systems (or systems of systems) to small mobile computing devices to collect, process, store, maintain, transmit, and disseminate this information. The information relied upon is subject to a range of threats that could potentially harm or adversely affect organizational operations (e.g., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. These threats include environmental disruptions, purposeful attacks, structural failures, human errors, and other threats that can compromise Federal information resources. Personnel at all levels of the Federal Government must understand how to manage information security and protect privacy.

Federal agencies must implement information security programs and privacy programs with the flexibility to meet current and future information management needs and the sufficiency to comply with Federal requirements and manage risks. Emerging technologies and services may continue to shift the ways in which agencies acquire, develop, manage, and use information and technology. As technologies and services continue to change, so will the threat environment. Agency programs must have the capability to identify, respond to, and recover from current threats while protecting their information resources and the privacy of the individuals whose information they maintain. The programs must also have the capability to address new and emerging threats. To be effective, information security and privacy considerations must be part of the day-to-day operations of agencies. This can best be accomplished by planning for the requisite security and privacy capabilities as an integral part of the agency strategic planning and risk management processes, not as a separate activity. This includes, but is not limited to, the integration of Federal information security and privacy requirements (and security and privacy controls) into the enterprise architecture, system development life cycle activities, systems engineering processes, and acquisition processes.

To ensure that Federal agencies can successfully carry out their assigned missions and business operations in an environment of sophisticated and complex threats, they must deploy systems that are both trustworthy and resilient. To increase the level of trustworthiness and resilience of Federal information systems, the systems should employ technologies that can significantly increase the built-in protection capability of those systems and make them inherently less vulnerable. This can require a significant investment in appropriate architectures and the application of systems engineering concepts and principles in the design of Federal information systems.

As Federal agencies take advantage of emerging information technologies and services to obtain more effective mission and operational capabilities, achieve greater efficiencies, and reduce costs, they must also apply the principles and practices of risk management, information security, and privacy to the acquisition and use of those technologies and services. While there are certain security and privacy requirements and associated controls that are mandatory, agencies are

required to employ risk-based approaches and decision making to ensure that security and privacy capabilities are sufficient to protect agency assets, operations, and individuals. Such risk-based approaches involve framing, assessing, responding to, and monitoring security and privacy risks on an ongoing basis. Risk-based approaches can also support potential performance improvements and cost savings when agencies make decisions about maintaining, modernizing, or replacing existing information technologies and services or implementing new technologies and services that leverage internal, other government, or private sector innovative and market-driven solutions. These responsibilities extend to the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of Federal information when such information is hosted by non-Federal entities on behalf of the Federal Government. Ultimately, agency heads remain responsible and accountable for ensuring that information management practices comply with all Federal requirements, that information security and privacy programs are appropriately managed, and that Federal information is adequately protected commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information.

2. Purpose

This Appendix establishes minimum requirements for Federal information security programs, assigns Federal agency responsibilities for the security of information and information systems, and links agency information security programs and agency management control systems established in accordance with OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Controls*. This Appendix also establishes requirements for Federal agency privacy programs, assigns responsibilities for privacy program management, and describes how agencies should take a coordinated approach to implementing information security and privacy controls. Additionally, this Appendix incorporates requirements of statute, such as FISMA (44 U.S.C. Chapter 35), the E-Government Act of 2002 (44 U.S.C. Chapters 35 and 36), the Paperwork Reduction Act (44 U.S.C. Chapter 35), and the Privacy Act of 1974, and responsibilities assigned in executive orders and Presidential directives.

3. General Requirements

- a. Agencies shall implement an agency-wide risk management process that frames, assesses, responds to, and monitors information security and privacy risk on an ongoing basis across the three organizational tiers (i.e., organization level, mission or business process level, and information system level).⁷⁶
- b. Agencies shall develop, implement, document, maintain, and oversee agency-wide information security and privacy programs including people, processes, and technologies to:
 - 1) Provide for agency information security and privacy policies, planning, budgeting, management, implementation, and oversight;

⁷⁶ NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, provides additional information on risk management processes and strategies. See also Section 5.b of this Appendix.

- 2) Protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide for their confidentiality, integrity, and availability;
 - 3) Provide adequate security for all information created, collected, processed, stored, transmitted, disseminated, or disposed of by or on behalf of the agency, to include Federal information residing in contractor information systems and networks;
 - 4) Cost-effectively manage information security and privacy risks, which includes reducing such risks to an acceptable level;
 - 5) Implement a risk management framework to guide and inform the categorization of Federal information and information systems; the selection, implementation, and assessment of security and privacy controls; the authorization of information systems and common controls; and the continuous monitoring of information systems;
 - 6) Implement security and privacy controls, and verify that they are operating as intended, and continuously monitored and assessed; put procedures in place so that security and privacy controls remain effective over time, and that steps are taken to maintain risk at an acceptable level within organizational risk tolerance;
 - 7) Employ systems security engineering principles, concepts, and techniques during the life cycle of information systems to facilitate the development, deployment, operation, and sustainment of trustworthy and adequately secure systems;
 - 8) Implement supply chain risk management principles to protect against the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software, as well as poor manufacturing and development practices throughout the system development life cycle;
 - 9) Implement policies and procedures to ensure that all personnel are held accountable for complying with agency-wide information security and privacy requirements and policies;
 - 10) Ensure that, in a timely manner, agency CIOs and SAOPs are made aware of information systems and components that cannot be appropriately protected or secured and that such systems are given a high priority for upgrade, replacement, or retirement;⁷⁷ and
 - 11) Ensure ongoing collaboration between the senior agency information security officer and the SAOP to ensure coordination of security and privacy activities.
- c. Agencies that share PII shall require, as appropriate, other agencies and entities with which they share PII to maintain the PII in an information system with a particular NIST FIPS Publication 199 confidentiality impact level, as determined by the agency sharing the PII.
- d. Agencies that share PII with other agencies or entities shall impose, where appropriate, conditions (including the selection and implementation of particular security and privacy controls) that govern the creation, collection, use, processing, storage, maintenance,

⁷⁷ Until such information systems or components are appropriately dispositioned, agencies are expected to immediately implement interim remediation measures such as limiting access or connectivity.

dissemination, disclosure, and disposal of the PII through written agreements, including contracts, data use agreements, information exchange agreements, and memoranda of understanding.

- e. Agencies shall protect Controlled Unclassified Information (CUI) and shall apply NIST FIPS and NIST (800-series) SPs, as appropriate. This includes limiting the disclosure of proprietary information to that which is legally authorized, and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists.
- f. Agencies shall ensure compliance with all applicable statutory, regulatory, and policy requirements and develop and maintain effective information security and privacy programs. This includes using privacy impact assessments and other tools to manage privacy risks.
- g. Agencies shall implement policies issued by OMB, as well as requirements issued by the Department of Commerce, DHS, GSA, and OPM. This includes applying the standards and guidelines contained in NIST FIPS, NIST (800-series) SPs, and, where appropriate and directed by OMB, NISTIRs.

4. Specific Requirements⁷⁸

a. Security Categorization

Agencies shall:

- 1) Identify authorization boundaries for information systems in accordance with NIST SPs 800-18 and 800-37; and
- 2) Categorize information and information systems, in accordance with FIPS Publication 199 and NIST SP 800-60, considering potential adverse security and privacy impacts to organizational operations and assets, individuals, other organizations, and the Nation.

b. Planning, Budgeting, and Enterprise Architecture

Agencies shall:

- 1) Identify and plan for the resources needed to implement information security and privacy programs;
- 2) Ensure that information security and privacy are addressed throughout the life cycle of each agency information system, and that security and privacy activities and costs are identified and included in IT investment capital plans and budgetary requests;
- 3) Plan and budget to upgrade, replace, or retire any information systems for which security and privacy protections commensurate with risk cannot be effectively implemented;

⁷⁸ The requirements in this section represent those areas deemed to be of fundamental importance to the achievement of effective agency information security programs and those areas deemed to require specific emphasis by OMB. The security programs developed and executed by agencies need not be limited to the aforementioned areas but can employ a comprehensive set of safeguards and countermeasures based on the principles, concepts, and methodologies defined NIST standards and guidelines.

- 4) Ensure that investment plans submitted to OMB as part of the budget process meet the information security and privacy requirements appropriate for the life cycle stage of the investment; and
- 5) Incorporate Federal information security and privacy requirements into the agency's enterprise architecture to ensure that risk is addressed and information systems achieve the necessary levels of trustworthiness, protection, and resilience.

c. Plans, Controls, and Assessments

Agencies shall:

- 1) Develop and maintain an information security program plan that provides an overview of the organization-wide information security requirements and documents the program management controls and common controls in place or planned for meeting those requirements;
- 2) Develop and maintain a privacy program plan that provides an overview of the agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks, and any other information determined necessary by the agency's privacy program;
- 3) Employ a system life cycle process that incorporates the principles, concepts, methods, and techniques of systems security engineering to ensure the development of trustworthy and resilient information systems;
- 4) Develop supply chain risk management plans as described in NIST SP 800-161 to ensure the integrity, security, resilience, and quality of information systems;
- 5) Employ a process to select and implement security controls for information systems and the environments in which those systems operate⁷⁹ that satisfies the minimum information security requirements in FIPS Publication 200 and security control baselines in NIST SP 800-53, tailored as appropriate;⁸⁰
- 6) Employ a process to select and implement privacy controls for information systems and programs that satisfies applicable privacy requirements in OMB guidance, including, but not limited to, Appendix I to this Circular and OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*;
- 7) Implement information system security using sound systems security engineering principles, concepts, methods, practices, and techniques;
- 8) Develop and maintain security plans for information systems to document which security controls have been selected and how those controls have been implemented;

⁷⁹ The environment of operation includes the physical surroundings in which an information system processes, stores, and transmits information. Agencies should take the environment into account when selecting, implementing, documenting, and assessing security controls.

⁸⁰ Agencies must conduct tailoring activities in accordance with OMB policy.

- 9) Develop and maintain a privacy plan that details the privacy controls selected for an information system that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls;
- 10) Deploy effective security controls to provide Federal employees and contractors with multifactor authentication, digital signature, and encryption capabilities that provide assurance of identity and are interoperable Government-wide and accepted across all Executive Branch agencies;
- 11) Adhere to Government-wide requirements in the deployment and use of identity credentials used by employees and contractors accessing Federal facilities;⁸¹
- 12) Designate common controls in order to provide cost-effective security and privacy capabilities that can be inherited by multiple agency information systems or programs;⁸²
- 13) Conduct and document assessments of all selected and implemented security and privacy controls to determine whether security and privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable requirements and to manage security and privacy risks;
- 14) Conduct and document security and privacy control assessments prior to the operation of an information system, and periodically thereafter, consistent with the frequency defined in the agency information security continuous monitoring (ISCM) and privacy continuous monitoring (PCM) strategies and the agency risk tolerance;
- 15) Use agency plans of action and milestones (POA&Ms), and make available or provide access to OMB, DHS, inspectors general, and the U.S. Government Accountability Office, upon request, to record and manage the mitigation and remediation of identified weaknesses and deficiencies, not associated with accepted risks, in agency information systems; and
- 16) Obtain approval from the authorizing official for connections from the information system, as defined by its authorization boundary, to other information systems based on the risk to the agency's operations and assets, individuals, other organizations, and the Nation.

⁸¹ NIST SP 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, provides additional information on the use of PIV Credentials, the Government-wide standard identity credential, in physical access control systems. Physical access controls systems, which include, for example, servers, databases, workstations and network appliances in either shared or isolated networks, are considered information systems.

⁸² When common controls protect multiple agency information systems of differing impact levels, the controls shall be implemented at the highest impact level among the systems. If such controls cannot be implemented at the highest impact level of the information systems, agencies shall factor this situation into their assessments of risk and take appropriate risk mitigation actions (e.g., adding security controls, changing assigned values of security control parameters, implementing compensating controls, changing certain aspects of mission or business processes, or separating the higher impact system into its own domain where it can be afforded appropriate levels of protection).

d. Authorization to Operate and Continuous Monitoring

Agencies shall:

- 1) Designate senior Federal officials to formally authorize an information system to operate and authorize agency-designated common controls for use;⁸³
- 2) Complete an initial authorization to operate for each information system and all agency-designated common controls based on a determination of, and explicit acceptance of, the risk to agency operations and assets, individuals, other organizations, and the Nation, and prior to operational status;
- 3) Transition information systems and common controls to an ongoing authorization process when eligible for such a process and with the formal approval of the respective authorizing officials;
- 4) Reauthorize information systems and common controls as needed, on a time- or event-driven basis in accordance with agency risk tolerance;
- 5) Develop and maintain an ISCM strategy to address information security risks and requirements across the organizational risk management tiers;⁸⁴
- 6) Implement and update, in accordance with organization-defined frequency, the ISCM strategy to reflect the effectiveness of deployed controls; significant changes to information systems; and adherence to Federal statutes, policies, directives, instructions, regulations, standards, and guidelines;
- 7) Ensure that all selected and implemented controls are addressed in the ISCM strategy and are effectively monitored on an ongoing basis, as determined by the agency's ISCM program;⁸⁵
- 8) Establish and maintain an ISCM program that:
 - a) Provides an understanding of agency risk tolerance and helps officials set priorities and manage information security risk consistently throughout the agency;
 - b) Includes metrics that provide meaningful indications of security status and trend analysis at all risk management tiers;
 - c) Ensures the continued effectiveness of all security controls selected and implemented by monitoring controls with the frequencies specified in the ISCM strategy;
 - d) Verifies compliance with information security requirements derived from organizational missions or business functions, Federal statutes, directives, instructions, regulations, policies, standards and guidelines;

⁸³ Common controls are authorized for operation in the same manner as system-specific controls.

⁸⁴ NIST SP 800-39, *Managing Information Security Risk*, defines three risk management tiers for managing information security risk within organizations. These include an organization or governance tier, mission or business process tier, and information system tier.

⁸⁵ For greater efficiency, the ISCM and PCM strategies may be consolidated into a single unified continuous monitoring strategy. Similarly, the ISCM and PCM programs may also be consolidated into a single unified continuous monitoring program.

- e) Is informed by all applicable agency IT assets to help maintain visibility into the security of those assets and the protection of PII associated with those assets;
 - f) Ensures knowledge and control of changes to information systems that have potential to affect security;
 - g) Maintains awareness of threats and vulnerabilities that have the potential to affect security, including the mitigation of those threats and vulnerabilities;
- 9) Develop and maintain a PCM strategy, a formal document that:
- a) Catalogs the available privacy controls implemented at the agency across the agency risk management tiers; and
 - b) Ensures that the privacy controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks;
- 10) Establish and maintain an agency-wide PCM program that implements the agency's PCM strategy and:
- a) Conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks;
 - b) Identifies assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks;
 - c) Maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; and
 - d) Monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII;
- 11) Ensure that a robust ISCM program and PCM program are in place before agency information systems are eligible for ongoing authorization; and
- 12) Leverage available Federal shared services, where practicable and appropriate.
- e. Privacy Controls for Federal Information Systems and Programs

The SAOP has agency-wide responsibility and accountability for developing, implementing, and maintaining an agency-wide privacy program to manage privacy risks, develop and evaluate privacy policy, and ensure compliance with all applicable statutes, regulations, and policies regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems. The SAOP shall:

- 1) Develop and maintain a privacy program plan that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the SAOP and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the

program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks;

- 2) Develop and maintain a PCM strategy and PCM program to maintain ongoing awareness of privacy risks and assess privacy controls at a frequency sufficient to ensure compliance with applicable privacy requirements and manage privacy risks;
- 3) Conduct and document the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across all agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks;
- 4) Identify assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks;
- 5) Designate which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls at the agency;
- 6) Review IT capital investment plans and budgetary requests to ensure that privacy requirements (and associated privacy controls), as well as any associated costs, are explicitly identified and included, with respect to any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII;
- 7) Review and approve, in accordance with NIST FIPS Publication 199 and NIST SP 800-60, the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII;⁸⁶
- 8) Review and approve the privacy plans for agency information systems prior to authorization, reauthorization, or ongoing authorization;
- 9) Review authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to ensure compliance with applicable privacy requirements and manage privacy risks, prior to authorizing officials making risk determination and acceptance decisions; and
- 10) Coordinate with the CIO, the senior agency information security officer, and other agency officials in implementation of these requirements.

f. Incident Detection, Response, and Recovery

It is essential that agencies react appropriately to incidents after employing a risk-based approach to selecting and implementing their security and privacy controls for their information and information systems.

⁸⁶ The categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII will depend on the sensitivity level of the PII, the privacy risks, and the associated risk to agency operations, agency assets, individuals, other organizations, and the Nation. Agencies should generally categorize information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII at the moderate or high confidentiality impact level. See Appendix II for additional information regarding the sensitivity level of PII.

Agencies shall:⁸⁷

- 1) Develop and implement incident management policies and procedures, in accordance with OMB policies and NIST guidelines that address incident detection, response, and recovery. This includes developing and implementing appropriate activities to identify the occurrence of an incident; developing and implementing appropriate activities to take action regarding a detected incident; and developing and implementing the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to an incident;
- 2) Designate sensitive positions and execute commensurate security clearance levels for appropriate agency personnel;
- 3) Establish clear roles and responsibilities to ensure the oversight and coordination of incident response activities and that incidents are documented, reported, investigated, and handled;
- 4) Periodically test incident response procedures to ensure effectiveness of such procedures;
- 5) Document lessons learned for incident response and update procedures annually or as required by OMB or DHS;
- 6) Ensure that processes are in place to verify corrective actions;
- 7) Maintain formal incident response capabilities and mechanisms to include notification to affected individuals and adequate training and awareness for employees and contractors on how to report and respond to incidents;
- 8) Implement formal incident management policies to include definitions, detection and analysis, containment, internal and external notification and reporting requirements, incident reporting methods, post-incident procedures, roles and responsibilities, and guidance on how to mitigate impacts to the agency and its respondents following an incident;
- 9) Report incidents to OMB, DHS, the CIO, the SAOP, their respective inspectors general and general counsel, law enforcement, and Congress in accordance with procedures issued by OMB; and
- 10) Provide reports on incidents as required by FISMA, OMB policy, DHS binding operational directives, Federal information security incident center guidelines, NIST guidelines, and agency procedures.

⁸⁷ Pursuant to FISMA (44 U.S.C. Chapter 35).

g. Contingency Planning⁸⁸

Agencies shall:

- 1) Develop and test contingency plans⁸⁹ for information systems that:
 - a) Identify essential missions and business functions and associated contingency requirements;
 - b) Provide recovery objectives, restoration priorities, and metrics;
 - c) Address contingency roles and responsibilities; and
 - d) Address maintaining essential missions, functions, and services despite a disruption, compromise, or failure of information systems.
- 2) Provide for the recovery and reconstitution of information systems to a known state after a disruption, compromise, or failure.

h. Awareness and Training

Agencies shall:

- 1) Develop, maintain, and implement mandatory agency-wide information security and privacy awareness and training programs for all employees and contractors;
- 2) Ensure that the security and privacy awareness and training programs are consistent with applicable policies, standards, and guidelines issued by OMB, NIST, and OPM;
- 3) Apprise agency employees about available security and privacy resources, such as products, techniques, or expertise;
- 4) Provide foundational as well as more advanced levels of security and privacy training to information system users (including managers, senior executives, and contractors) and ensure that measures are in place to test the knowledge level of information system users;
- 5) Provide role-based security and privacy training to employees and contractors with assigned security and privacy roles and responsibilities, including managers, before authorizing access to Federal information or information systems or performing assigned duties;

⁸⁸ The Federal Information Security Modernization Act of 2014 (44 U.S.C. Chapter 35) requires each agency to develop, document, and implement an agency-wide information security program that includes plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.

⁸⁹ Testing of contingency plans must be consistent with the assessment procedures in NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*. In addition, Homeland Security Presidential Directive 20, *National Continuity Directive*, requires the establishment and maintenance of an effective national continuity capability. Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements*, provides direction for the further development of continuity plans and programs.

- 6) Establish rules of behavior, including consequences for violating rules of behavior, for employees and contractors that have access to Federal information or information systems, including those that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and
 - 7) Ensure that employees and contractors have read and agreed to abide by the rules of behavior for the Federal information and information systems for which they require access prior to being granted access.
- i. Specific Safeguarding Measures to Reinforce the Protection of Federal Information and Information Systems⁹⁰
- Agencies shall:
- 1) Implement a policy of least functionality by only permitting the use of networks, systems, applications, and data, as well as programs, functions, ports, protocols, or services that are necessary in meeting mission or business needs;
 - 2) Implement policies of least privilege at multiple layers – network, system, application, and data so that users have role-based access to only the information and resources that are necessary for a legitimate purpose;
 - 3) Implement a policy of separation of duties to address the potential for abuse of authorized privileges and help to reduce the risk of malicious activity without collusion;
 - 4) Isolate sensitive or critical information resources (e.g., information systems, system components, applications, databases, and information) into separate security domains with appropriate levels of protection based on the sensitivity or criticality of those resources;
 - 5) Implement access control policies for information resources that ensure individuals have appropriate authorization and need, and that the appropriate level of identity proofing or background investigation is conducted prior to granting access;
 - 6) Protect administrator, user, and system documentation related to the design, development, testing, operation, maintenance, and security of the hardware, firmware, and software components of information systems;
 - 7) Continuously monitor, log, and audit the execution of information system functions by privileged users (that ordinary users are not authorized to perform) to detect misuse and to help reduce the risk from insider threats;
 - 8) Prohibit the use of unsupported information systems and system components, and ensure that systems and components that cannot be appropriately protected or secured are given a high priority for upgrade or replacement;⁹¹

⁹⁰ NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides information on additional security safeguarding measures.

⁹¹ Includes hardware, software, or firmware components no longer supported by developers, vendors, or manufacturers through the availability of software patches, firmware updates, replacement parts, and maintenance contracts. NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides additional guidance on unsupported software components.

- 9) Implement and maintain current updates and patches for all software and firmware components of information systems;⁹²
- 10) For systems that promote public access, ensure that identity proofing, registration, and authentication processes provide assurance of identity consistent with security and privacy requirements, in accordance with Executive Order 13681,⁹³ OMB policy, and NIST standards and guidelines;
- 11) Require use of multifactor authentication for employees and contractors in accordance with Government-wide identity management standards;⁹⁴
- 12) Develop and implement processes to support use of digital signatures for employees and contractors;
- 13) Ensure that all public key infrastructure (PKI) certificates used by an agency and issued in accordance with Federal PKI policy validate to the Federal PKI trust anchor when being used for user signing, encrypting purposes, authentication and authorization;⁹⁵
- 14) Encrypt all FIPS 199 moderate-impact and high-impact information at rest and in transit, unless encrypting such information is technically infeasible or would demonstrably affect the ability of agencies to carry out their respective missions, functions, or operations; and the risk of not encrypting is accepted by the authorizing official and approved by the agency CIO, in consultation with the SAOP (as appropriate);⁹⁶
- 15) Implement the current encryption algorithms and validated cryptographic modules in accordance with NIST standards and guidelines;
- 16) Ensure that only individuals or processes acting on behalf of individuals with legitimate need for access have the ability to decrypt sensitive information;
- 17) Implement data-level protection and access controls to ensure the security of and access to Federal information; and

⁹² Security-relevant software and firmware updates include, for example, patches, service packs, hot fixes, device drivers, basic input output system (BIOS), and antivirus signatures.

⁹³ Executive Order 13681, *Improving the Security of Consumer Financial Transactions*, October 2014.

⁹⁴ Pursuant to Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, NIST FIPS 201 describes the initial Government-wide identity management standard for employees and contractors as a smartcard form factor (the PIV card). With the emergence of a newer generation of computing devices and in particular with mobile devices, the use of PIV cards has evolved technically to include other form factors that can be deployed directly with mobile devices as specified in NIST SP 800-157. The PIV credential associated with this alternative is called a Derived PIV Credential. Derived PIV Credentials are based on the general concept of derived credentials in NIST SP 800-63. Issuing a Derived PIV credential to PIV card holders does not require repeating identity proofing and vetting processes. The user simply proves possession and control of a valid PIV Card to receive a Derived PIV Credential.

⁹⁵ The trust anchor refers to the Federal PKI root certificate operated by the Federal PKI Management Authority. This root certificate is the trusted source of all Federal PKI certificates. For additional information, refer to <https://www.idmanagement.gov> and Federal PKI policy.

⁹⁶ The encryption of organizational information when in transit over a network and when at rest in storage devices ensures that such information is persistently protected and promotes a defense-in-depth security strategy.

- 18) Ensure that all Federal systems and services identified in the Domain Name System are protected with Domain Name System Security (DNSSEC) and that all systems are capable of validating DNSSEC protected information.⁹⁷

j. Non-Federal Entities

Agencies shall:

- 1) Ensure that terms and conditions in contracts and other agreements involving the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of Federal information, incorporate security and privacy requirements and are sufficient to enable agencies to meet Federal and agency-specific requirements pertaining to the protection of Federal information;⁹⁸
- 2) Provide oversight of information systems used or operated by contractors or other entities on behalf of the Federal Government or that collect or maintain Federal information on behalf of the Federal Government, to include:
 - a) Documenting and implementing policies and procedures for information security and privacy oversight, to include ensuring appropriate vetting and access control processes for contractors and others with access to information systems containing Federal information;
 - b) Ensuring that security and privacy controls of such information systems and services are effectively implemented and comply with NIST standards and guidelines and agency requirements;
 - c) Ensuring that these information systems are included in the agency's inventory of information systems;
 - d) Ensuring that the interface characteristics, security requirements, and the nature of the information communicated is documented for each interface between these systems and agency-owned or operated information systems;
 - e) Ensuring that procedures are in place for incident response for these information systems including timelines for notification of affected individuals and reporting to OMB, DHS, and other entities as required in OMB guidance;
 - f) Requiring agreements (e.g., memoranda of understanding, interconnection security agreements, contracts) for interfaces between these information systems and agency-owned or operated information systems; and
- 3) Consistent with the agency's authority, ensure that the requirements of the Privacy Act apply to a Privacy Act system of records when a contractor operates the system of records on behalf of the agency to accomplish an agency function;
- 4) Collaborate with non-Federal entities and other agencies as appropriate to ensure that security and privacy requirements pertaining to these non-Federal entities, such as State,

⁹⁷ DNSSEC is a critical component of the Internet infrastructure. DNSSEC enables clients to cryptographically verify that each such translation is provided by a server with the authority to do so, and that the translation response from the server was not modified before reaching the client.

⁹⁸ For additional information and associated requirements pertaining to IT acquisitions, refer to the FAR.

local, tribal, and territorial governments, are consistent to the greatest extent possible;
and

- 5) Ensure that terms and conditions of contracts and other agreements include sufficient provisions for Federal Government notification and access, as well as cooperation with agency personnel and Inspectors General.

k. Mitigation of Deficiencies and Issuance of Status Reports

Agencies shall correct deficiencies that are identified through information security and privacy assessments, ISCM and PCM programs, or internal or external audits and reviews, to include OMB reviews. OMB Circular A-123, *Management's Responsibility for Internal Controls*, provides guidance to determine whether a deficiency in controls is material when so judged by the agency head against other agency deficiencies. Material deficiencies must be included in the annual Federal Managers Financial Integrity Act (FMFIA) report, and remediation tracked and managed through the agency's POA&M process. Less significant deficiencies need not be included in the FMFIA report, but must be tracked and managed through the agency's POA&M process.

l. Reporting

Agencies shall provide performance metrics information and FISMA reports in accordance with processes established by OMB and DHS pursuant to FISMA.

m. Independent Evaluations

Pursuant to FISMA, agencies shall:⁹⁹

- 1) Perform an independent evaluation of the information security programs and practices to determine the effectiveness of such programs and practices, as further described in statute.¹⁰⁰ The evaluation may include an evaluation of their privacy program and practices, as appropriate. Each evaluation shall include:
 - a) Testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's Federal information systems;¹⁰¹
 - b) An assessment of the effectiveness of the information security policies, procedures, and practices of the agency; and
 - c) Separate presentations, as appropriate, regarding information security relating to national security systems.

⁹⁹ FISMA (44 U.S.C. § 3555).

¹⁰⁰ FISMA (44 U.S.C. § 3555).

¹⁰¹ Agencies have flexibility in implementing the baseline controls in SP 800-53; however, agencies are required to justify, in their security plans or overlays, any tailoring actions.

5. Discussion of the Major Provisions in the Appendix

This section provides additional information regarding the requirements in this appendix.

a. NIST Standards and Guidelines

NIST standards and guidelines associate each information system with an impact level. The standards and guidelines also provide a corresponding starting set of baseline security controls and tailoring guidance¹⁰² to ensure that the set of security controls in the information system security plan (approved by the authorizing official) and privacy controls in the privacy plan (approved by the SAOP) satisfy the information security, privacy, and mission or business protection needs of the agency.

For non-national security programs and information systems, agencies must apply NIST guidelines unless otherwise stated by OMB. FIPS are mandatory.¹⁰³ There is flexibility within NIST's guidelines (specifically in the 800-series) in how agencies apply those guidelines. Unless specified by additional implementing policy by OMB, the concepts and principles described in NIST guidelines must be applied. However, NIST guidelines generally allow agencies latitude in their application. Consequently, the application of NIST guidelines by agencies can result in different solutions that are equally acceptable and compliant with the guidelines.

For legacy information systems, agencies are expected to meet the requirements of, and be in compliance with, NIST standards and guidelines within one year of their respective publication dates unless otherwise directed by OMB. The one-year compliance date for revisions to NIST publications applies only to new or updated material in the publications. For information systems under development or for legacy systems undergoing significant changes, agencies are expected to meet the requirements of, and be in compliance with, NIST standards and guidelines immediately upon deployment of the systems.

b. Risk Management Strategy

Managing risk is a complex, multifaceted activity that requires the involvement of the entire agency from senior leaders and executives providing the strategic vision and top-level goals and objectives for the agency; to mid-level leaders planning, executing, and managing projects; to individuals on the front lines operating the information systems supporting the agency's missions or business functions. Risk management is a comprehensive process that requires agencies to establish the context in which risk-based decisions are made; assess risk; respond to risk once determined; and monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of agencies. Risk management is conducted as an agency-wide activity to ensure that risk-based decision-making is integrated into every aspect of the agency's planning and operations.

¹⁰² Agencies must conduct tailoring activities in accordance with OMB policy.

¹⁰³ Pursuant to FISMA (44 U.S.C. Chapter 35).

A key aspect of the risk management process is the development of the risk management strategy. The risk management strategy describes how an agency intends to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that agencies routinely use in making both investment and operational decisions. Establishing a realistic and credible risk management strategy requires that agencies identify their risk assumptions, risk constraints, risk tolerance, and priorities and trade-offs. The risk management strategy also includes any strategic-level decisions by senior leaders and executives regarding the management of risk to agency operations and assets, individuals, other organizations, and the Nation. The risk management strategy guides and informs the use and application of the Risk Management Framework.

c. Risk Management Framework

The Risk Management Framework, as described in NIST SP 800-37, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. The Risk Management Framework requires agencies to categorize each information system and the information processed, stored, and transmitted by each system based on a mission or business impact analysis. Agencies select an initial set of baseline security controls for the information system based on the security categorization and then tailor the security control baseline as needed, based on an organizational assessment of risk and local conditions, as described in NIST SP 800-53. After implementing the security controls, agencies assess the controls using appropriate assessment methods as described in NIST SP 800-53A to determine whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

The authorization to operate the system is based on a determination of the risk to agency operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of the system and the decision by the authorizing official that this risk is acceptable. Subsequent to the authorization decision and as part of an information security continuous monitoring strategy and program, agencies monitor the security controls in the system on an ongoing basis, as described in NIST SP 800-137. Monitoring includes, but is not limited to, assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated agency officials on an ongoing basis.

An effective implementation of the Risk Management Framework ensures that managing information system-related risks is consistent with the agency's mission or business objectives and overall risk management strategy, and risk tolerance established by the senior leadership through the risk executive function¹⁰⁴ as discussed in NIST SP 800-39. It also ensures that the requisite security and privacy requirements and controls are integrated into

¹⁰⁴ The *risk executive function* is an individual or group within an agency that helps to ensure that: (i) risk-related considerations for individual information systems, to include the authorization to operate decisions, are viewed from an agency-wide perspective with regard to the overall strategic goals and objectives of the agency in carrying out its missions and business functions; and (ii) managing information system-related risks is consistent across the agency, reflects the agency's risk tolerance, and is considered along with other agency risks affecting its missions or business functions.

the agency's enterprise architecture and system development life cycle processes. Finally, the Risk Management Framework supports consistent, well-informed, and ongoing authorization decisions, transparency of risk management information, reciprocity, and information sharing.

d. Security Control Baselines

It is important to achieve adequate security for Federal information and information systems and a consistent level of protection for such information and systems Government-wide. To meet this objective, agencies must select an appropriate set of security controls for their information systems that satisfies the minimum security requirements set forth in FIPS Publication 200. The security controls must include one of the three security control baselines from NIST SP 800-53 that are associated with the designated categorization (impact levels) of their information systems. The security control baselines define the set of minimum security controls for a low-impact, moderate-impact, or high-impact information system and provide a starting point for the tailoring process. Agencies are required to tailor the security control baselines to customize their safeguarding measures for specific missions, business lines, and operational environments and to do so in a cost-effective, risk-based manner. Tailoring allows agencies to designate common controls; apply scoping considerations; select compensating controls; assign specific values to agency-defined control parameters; supplement baselines with additional controls when necessary; and provide additional specification information for control implementation. Agencies must include a justification, in their information system security plans or overlays, for any tailoring actions that result in changes to the initial security control baselines. Agencies are not permitted to make changes to security control baselines when such changes result in control selections that are inconsistent with security requirements set forth in Federal statutes, executive orders, regulations, directives, or policies.

Agencies may also develop overlays for specific types of information or communities of interest (e.g., all web-based applications, all health care-related systems) as part of the security control selection process. Overlays provide a specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information as part of the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay may be more stringent or less stringent than the original security control baseline and can be applied to multiple information systems.

All selected security controls must be documented in an information system security plan and implemented. Agencies can use the priority code designations associated with each security control in NIST SP 800-53 to assist in making sequencing decisions for control implementation. This prioritization helps to ensure that the foundational security controls upon which other controls depend are implemented first, thus enabling agencies to deploy controls in a more structured and timely manner in accordance with available resources. Independent evaluations, when conducted, shall focus on the effectiveness of the security controls selected and implemented (as documented in agency information system security plans after all tailoring actions have been completed on the security control baselines) and the justification for any decisions to change the control baselines.

e. Security and Privacy Assessments

Agencies must ensure that periodic testing and evaluation of the effectiveness of information security and privacy policies, procedures, and practices are performed with a frequency depending on risk, but at least annually. However, this general requirement to test and evaluate the effectiveness of information security and privacy policies, procedures, and practices does not imply that agencies must assess every selected and implemented security and privacy control at least annually. Rather, agencies must continuously monitor all implemented security and privacy controls (i.e., system-specific, hybrid, and common controls) with a frequency determined by the agency in accordance with the ISCM and PCM strategies. These strategies will define the specific security and privacy controls selected for assessment during any one-year period (i.e., the annual assessment window) with the understanding that all controls may not be formally assessed every year. Rotational assessment of security and privacy controls is consistent with the transition to ongoing authorization and assumes the information system has completed an initial authorization where all controls were formally assessed for effectiveness. As the transition to ongoing authorization progresses and agency ISCM programs mature, agencies must ensure that assessment frequencies are determined in accordance with NIST SP 800-137.

Security and privacy control assessments shall ensure that security and privacy controls selected by agencies are implemented correctly, operating as intended, and effective in satisfying security and privacy requirements. The risk may change over time based on changes in the threat, agency missions or business functions, personnel, technology, or environments of operation. Consequently, maintaining a capability for real-time or near real-time analysis of the threat environment and situational awareness following an incident is paramount. The type, rigor, and frequency of control assessments, which is established by the agency's risk tolerance and risk management strategy, shall be commensurate with the level of awareness necessary for effectively determining information security and privacy risk. Technical security tools such as malicious code scanners, vulnerability assessment products (which look for known security weaknesses, configuration errors, and the installation of the latest patches), and penetration testing can assist in the ongoing assessment of information systems.

f. Authorizing Official

The authorizing official is a senior agency official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations and assets, individuals, other organizations, and the Nation. Authorizing officials have budgetary oversight for an information system or be responsible for the mission or business operations supported by the system. Through the authorization process, authorizing officials are responsible and accountable for the risks associated with information system operations. Because information security is closely related to the privacy protections required for PII, authorizing officials are also responsible and accountable for the privacy risks that arise from the operation of an information system. Accordingly, authorizing officials must be in management positions with a level of authority commensurate with understanding and accepting such information system-related security and privacy risks.

Since the SAOP is the senior official, designated by the head of each agency, who has overall agency-wide responsibility for privacy, agencies must consider input and recommendations submitted by the SAOP in the authorization decision. Additionally, the SAOP has responsibility for reviewing the authorization package for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII, to ensure that privacy risks are managed prior to system authorization. In situations where the authorizing official and SAOP cannot reach a final resolution regarding the appropriate protection for the agency information and information system, the head of the agency must review the associated risks and requirements and make a final determination regarding the issuance of the authorization to operate.¹⁰⁵

Agencies can choose from several different approaches when planning for and conducting authorizations. These include an authorization with a single authorizing official, an authorization with multiple authorizing officials, or leveraging an existing authorization (see Section 6j, *Joint and Leveraged Authorizations*). Agencies can, at their discretion, include the CIO or the SAOP as a co-authorizing official with a senior agency official who has budgetary oversight for an information system or is responsible for the mission or line of business supported by the system being authorized for operation. Regardless of the approach used, only Federal Government personnel may serve as an authorizing official.

g. Authorization to Operate

The authorization to operate an information system and the authorization of agency-designated common controls granted by senior Federal officials provide an important quality control for agencies. The decision to authorize an information system to operate shall be based on a review of the authorization package and includes an assessment of compliance with applicable requirements and risk to agency operations and assets, individuals, other organizations, and the Nation. As stated above, the decision to authorize a system, or agency-defined common controls, shall be made by the appropriate authorizing official. Since the information system security plan and privacy plan establish the security and privacy controls selected for implementation, those plans are a critical part of the authorization package and shall form the basis for the authorization, supplemented by more specific information as needed.

In the event that there is a change in authorizing officials, the new authorizing official reviews the current authorization decision document, authorization package, and any updated documents created as a result of the continuous monitoring activities. If the new authorizing official is willing to accept the currently documented risk, then the official signs a new authorization decision document, thus formally transferring responsibility and accountability for the information system or the common controls and explicitly accepting the risk. If the new authorizing official is not willing to accept the previous authorization results (including the identified risk), a reauthorization action may need to be initiated or the new authorizing

¹⁰⁵ The head of the agency is the highest-level senior official or executive within an agency with the overall responsibility to provide information security protections commensurate with the risk and magnitude of harm (i.e., impact) to organizational operations and assets, individuals, other organizations, and the Nation.

official may instead establish new terms and conditions for continuing the original authorization, but not extend the original authorization termination date.

h. Ongoing Authorization

Ongoing authorization¹⁰⁶ is a process whereby the authorizing official makes risk determination and risk acceptance decisions subsequent to the initial authorization, taken at agreed-upon and documented frequencies in accordance with the agency's risk tolerance and mission or business requirements. In order to implement an ongoing authorization process, and move from a static, point-in-time authorization process to a dynamic, near real-time ongoing authorization process for information systems and controls, two conditions must be met by agencies. First, the information system or common controls must have been granted an initial authorization to operate by the designated authorizing official. Second, ISCM and PCM programs must be in place to monitor all implemented security and privacy controls with the appropriate degree of rigor¹⁰⁷ and at the appropriate frequencies in accordance with applicable ISCM and PCM strategies, OMB guidance, and NIST guidelines. Ongoing authorization can either be a time-driven or event-driven process whereby the authorizing official is provided with the necessary and sufficient information regarding the near real-time state of the information system and inherited common controls to determine whether all applicable security and privacy requirements have been satisfied and the mission or business risk is acceptable. Effective ongoing authorization requires robust ISCM and PCM strategies and effective operational ISCM and PCM programs.

Agencies must define and implement a process to designate information systems or common controls that have satisfied the two conditions noted in the previous paragraph and are to be transitioned to ongoing authorization. The process includes the means for the authorizing official to formally acknowledge that the information system or common controls are being managed under an ongoing authorization process and accept the responsibility for ensuring that all necessary activities associated with the ongoing authorization process are performed. Until a formal approval is obtained from the authorizing official to transition to ongoing authorization, information systems (and common controls) remain under a static authorization process with specific authorization termination dates enforced by the agency.

i. Reauthorization

Reauthorization consists of a review of the information system similar to the review carried out during the initial authorization but conducted during the operations or maintenance phase of the system development life cycle rather than prior to that phase. In general, reauthorization actions may be time-driven or event-driven. However, under ongoing authorization, reauthorization is typically an event-driven action initiated by the authorizing official or directed by the Risk Executive (function) in response to an event or significant

¹⁰⁶ For additional information on Ongoing Authorization and its relationship to initial authorization and reauthorization, refer to NIST *Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real Time Risk Management*, <http://csrc.nist.gov/publications>.

¹⁰⁷ The term rigor is used in conjunction with security control assessments and monitoring. It is typically associated with the application of assessment methods described in NIST SP 800-53A, and in particular, the attribute of depth which addresses the formality and comprehensiveness of the assessment or monitoring activity.

change that increases information security or privacy risk above the previously agreed-upon agency risk tolerance. A significant change is defined as a change that is likely to affect the security or privacy state of an information system.

The reauthorization process differs from the initial authorization inasmuch as the authorizing official can initiate a complete zero-base review of the information system or common controls, or a targeted review based on the type of event or significant change that triggered the reauthorization, the assessment of risk related to the event, the risk response of the agency, and the agency risk tolerance. Reauthorization is a separate activity from the ongoing authorization process, though security- and privacy-related information from the agency's ISCM and PCM programs may still be leveraged to support reauthorization. Note also that reauthorization actions may necessitate a review of and changes to the ISCM or PCM strategy, which may in turn affect ongoing authorization.

j. Joint and Leveraged Authorizations

Agencies are encouraged to use joint and leveraged authorizations whenever practicable.¹⁰⁸ Joint authorizations can be used when multiple agency officials either from the same agency or different agencies, have a shared interest in authorizing an information system or common controls. The participating officials are collectively responsible and accountable for the system and the common controls and jointly accept the risks that may adversely impact agency operations and assets, individuals, other organizations, and the Nation. Agencies choosing a joint authorization approach should work together on the planning and the execution of the Risk Management Framework tasks described in NIST SP 800-37 and document their agreement and progress in implementing the tasks. The specific terms and conditions of the joint authorization are established by the participating parties in the joint authorization including, for example, the process for ongoing determination and acceptance of risk. The joint authorization remains in effect only as long as there is mutual agreement among authorizing officials and the authorization meets the requirements established by Federal or agency policies.

Leveraged authorizations can be used when an agency chooses to accept some or all of the information in an existing authorization package generated by another agency based on the need to use the same information resources (e.g., information system or services provided by the system).¹⁰⁹ The leveraging agency reviews the owning agency's authorization package as the basis for determining risk to the leveraging agency. The leveraging agency considers risk factors such as the time elapsed since the authorization results were produced, differences in environments of operation (if applicable), the impact of the information to be processed, stored, or transmitted, and the overall risk tolerance of the leveraging agency. The leveraging agency may determine that additional security measures are needed and negotiate with the owning agency to provide such measures. To the extent that a leveraged authorization includes an information system that creates, collects, uses, processes, stores,

¹⁰⁸ NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, provides guidance on joint and leveraged security authorizations.

¹⁰⁹ Agencies using leveraged authorization information from other (owning) agencies shall ensure that such information is included as part of their own Risk Management Framework to provide the appropriate context for managing risk within the leveraging organizations.

maintains, disseminates, discloses, or disposes of PII, leveraging agencies must consult their SAOP. The SAOP may determine that additional measures are required to manage privacy risks prior to leveraging the authorization.

k. Continuous Monitoring

Agencies must develop ISCM and PCM strategies and implement ISCM and PCM activities in accordance with applicable statutes, directives, policies, instructions, regulations, standards, and guidelines. Agencies have the flexibility to develop an overarching ISCM and PCM strategy (e.g., at the agency, bureau, or component level) that addresses all information systems, or continuous monitoring strategies that address each agency information system individually. The ISCM and PCM strategies must document all available security and privacy controls selected and implemented by agencies, including the frequency of and degree of rigor associated with the monitoring process. ISCM and PCM strategies, which must be approved by the appropriate agency authorizing official and SAOP, respectively, must also include all common controls inherited by agency information systems.

l. Critical Infrastructure

Agencies that operate information systems that are part of the critical infrastructure must conduct a risk assessment to ensure that security controls for those systems are appropriately tailored (including the deployment of additional controls, when necessary), thus providing the required level of protection for critical Federal missions and business operations. In addition, agencies must ensure that the privacy controls assigned to critical infrastructure meet applicable privacy requirements and manage privacy risks. This includes the continuous monitoring of deployed security and privacy controls in information systems designated as critical infrastructure to determine the ongoing effectiveness of those controls against current threats; improving the effectiveness of those controls, when necessary; managing associated changes to the systems and environments of operation; and satisfying specific protection and compliance requirements in statutes, executive orders, directives, and policies required for critical infrastructure protection.

m. Encryption

When the assessed risk indicates the need, agencies must encrypt Federal information at rest and in transit unless otherwise protected by alternative physical and logical safeguards implemented at multiple layers, including networks, systems, applications, and data. Encrypting information at rest and in transit helps to protect the confidentiality and integrity of such information by making it less susceptible to unauthorized disclosure or modification. Agencies must apply encryption requirements to Federal information categorized as either moderate or high impact in accordance with FIPS Publication 199 unless encrypting such information is technically unfeasible or would demonstrably affect their ability to carry out their respective mission, functions, or operations. In situations where the use of encryption is technically infeasible, for example, due to an aging legacy system, agencies must initiate the appropriate system or system component upgrade or replacement actions at the earliest opportunity to be able to accommodate such safeguarding technologies. Authorizing officials who choose to operate information systems without the use of required encryption technologies must carefully assess the risk in doing so, and they must receive written

approval for the exception from the agency CIO, in consultation with the SAOP (as appropriate). Only FIPS-validated cryptography is approved for use in Federal information systems covered by this policy.

n. Digital Signatures

Digital signatures can mitigate a variety of security vulnerabilities by providing authentication and non-repudiation capabilities, and ensuring the integrity of Federal information whether such information is used in day-to-day operations or archived for future use. Additionally, digital signatures can help agencies streamline mission or business processes and transition manual processes to more automated processes to include, for example, online transactions. Because of the advantages provided by this technology, OMB expects agencies to implement digital signature capabilities in accordance with Federal PKI policy, and NIST standards and guidelines. For employees and contractors, agencies must require the use of the digital signature capability of Personal Identity Verification (PIV) credentials. For individuals that fall outside the scope of PIV applicability, agencies should leverage approved Federal PKI credentials when using digital signatures.

o. Identity Assurance

Identity assurance is an essential element of an effective information security program. To streamline the process of citizens, businesses, and other partners¹¹⁰ securely accessing Government services online requires a risk-appropriate demand of identity assurance. Identity assurance, in an online context, is the ability of an agency to determine that a claim to a particular identity made by an individual can be trusted to actually be the individual's true identity.¹¹¹ Citizens, businesses, and other partners that interact with the Federal Government need to have and be able to present electronic identity credentials to identify and authenticate themselves remotely and securely when accessing Federal information resources. An agency needs to be able to know, to a degree of certainty commensurate with the risk determination, that the presented electronic identity credential truly represents the individual presenting the credential before a transaction is authorized.¹¹² To transform processes for citizens, businesses, and other partners accessing Federal services online, OMB expects agencies to use a standards-based federated identity management approach that enables security, privacy, ease-of-use, and interoperability among electronic authentication systems.¹¹³

¹¹⁰ "Other partners" may include contractors not subject to the NIST FIPS 201 identity standard.

¹¹¹ Pursuant to Executive Order 13681, *Improving the Security of Consumer Financial Transactions*, agencies making personal data accessible to citizens through digital applications shall require the use of multiple factors of authentication and an effective identity proofing process, as appropriate.

¹¹² NIST SP 800-63, *Electronic Authentication Guidance*, provides additional guidance on identity assurance.

¹¹³ The requirements in this paragraph focus on citizens, businesses, and other partners that interact with the Federal Government. For Federal employees and contractors, with long-term access to Federal facilities and information systems, agencies are required to follow Personal Identity Verification requirements in accordance with OMB policy and NIST standards and guidelines.

p. Unsupported Information System Components

Unsupported information system components (e.g., when developers or vendors are no longer providing critical software patches) provide a substantial opportunity for adversaries to exploit weaknesses discovered in the currently installed components. Prohibit the use of unsupported information systems and system components, and ensure that systems and components that cannot be appropriately protected or secured are given a high priority for upgrade or replacement. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission or business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option. For such systems, agencies can establish in-house support, for example, by developing customized patches for critical software components or securing the services of external providers who through contractual relationships, provide ongoing support for the designated unsupported components. Such contractual relationships can include, for example, open source software value-added vendors.

q. Cybersecurity Framework

The Cybersecurity Framework was developed by NIST in response to Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*. The Framework describes five core cybersecurity functions (i.e., Identify, Protect, Detect, Respond, and Recover) that may be helpful in raising awareness and facilitating communication among agency stakeholders, including executive leadership. The Cybersecurity Framework may also be helpful in improving communications across organizations, allowing cybersecurity expectations to be shared with business partners, suppliers, and among sectors. The Framework is not intended to duplicate the current information security and risk management practices in place within the Federal Government. However, in the course of managing information security risk using the established NIST Risk Management Framework and associated security standards and guidelines required by FISMA, agencies can leverage the Cybersecurity Framework to complement their current information security programs. NIST is responsible for providing guidance on how agencies can use the Cybersecurity Framework and in particular, how the two frameworks can work together to help agencies develop, implement, and continuously improve their information security programs.

r. FISMA Applicability to Non-Federal Entities

FISMA describes Federal agency security responsibilities as including “information collected or maintained by or on behalf of an agency” and “information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.” FISMA requires each agency to provide information security for the information and “information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.” This includes services that are either fully or partially provided, including agency-hosted, outsourced, and cloud-based solutions.

Additionally, because FISMA applies to Federal information and information systems, in certain circumstances, its requirements also apply to a specific class of IT that the Clinger-Cohen Act of 1996 (40 U.S.C. § 11101(6)) did not include, i.e., “equipment that is acquired

by a Federal contractor incidental to a Federal contract.” Therefore, when Federal information is used within incidentally acquired equipment, the agency continues to be responsible and accountable for ensuring that FISMA requirements are met for such information.

s. **Controlled Unclassified Information**

The Controlled Unclassified Information program, established by Executive Order 13556, is a system that standardizes and simplifies the way the agencies handle unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies. The program emphasizes the openness and uniformity of Government-wide practices. Its purpose is to address inefficient and confusing processes that have historically led to inconsistent marking and safeguarding as well as restrictive dissemination policies.

6. Other Requirements

Agencies must adhere to all other applicable information requirements such as privacy requirements in accordance with the Privacy Act of 1974, and its implementing OMB guidance; confidentiality protection requirements in accordance with the Confidentiality Information Protection and Statistical Efficiency Act of 2002 (CIPSEA) and its implementing OMB guidance; applicable requirements of statutes, and regulations pertaining to management of Federal records; and other relevant statutes, executive orders, Presidential directives, and policies.

7. References¹¹⁴

a. The following references are used within this policy:

- 1) Executive Order 13556, *Controlled Unclassified Information*, November 2010.
- 2) Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 2013.
- 3) Executive Order 13681, *Improving the Security of Consumer Financial Transactions*, October 2014.
- 4) Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2004.
- 5) Homeland Security Presidential Directive 20 (National Security Presidential Directive 51), *National Continuity Policy*, May 2007.
- 6) Federal Continuity Directive 1 (FCD 1), *Federal Executive Branch National Continuity Program and Requirements*, February 2008.
- 7) National Communications System (NCS) Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, July 2007.

¹¹⁴ Statutes, executive orders, and Presidential directives relevant to this appendix are listed in the Authorities section of the main body. Additionally, OMB policy documents can be located at https://www.whitehouse.gov/omb/circulars_default and https://www.whitehouse.gov/omb/memoranda_default.

- 8) National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.
- 9) National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*.
- 10) National Institute of Standards and Technology Federal Information Processing Standards Publication 201, *Personal Identity Verification of Federal Employees and Contractors*.
- 11) National Institute of Standards and Technology Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*.
- 12) National Institute of Standards and Technology Special Publication 800-30, *Guide for Conducting Risk Assessments*.
- 13) National Institute of Standards and Technology Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.
- 14) National Institute of Standards and Technology Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*.
- 15) National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*.
- 16) National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.
- 17) National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*.
- 18) National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*.
- 19) National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*.
- 20) National Institute of Standards and Technology Special Publication 800-63, *Electronic Authentication Guideline*.
- 21) National Institute of Standards and Technology Special Publication 800-73, *Interfaces for Personal Identity Verification*.
- 22) National Institute of Standards and Technology Special Publication 800-76, *Biometric Specifications for Personal Identity Verification*.
- 23) National Institute of Standards and Technology Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*.

- 24) National Institute of Standards and Technology Special Publication 800-79, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*.
 - 25) National Institute of Standards and Technology Special Publication 800-116, *Guidelines for the Use of PIV Credentials in Physical Access Control Systems (PACS)*.
 - 26) National Institute of Standards and Technology Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*.
 - 27) National Institute of Standards and Technology Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*.
 - 28) National Institute of Standards and Technology Special Publication 800-157, *Guidelines for Derived Personal Identity Verification Credentials*.
 - 29) National Institute of Standards and Technology Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*.
 - 30) National Institute of Standards and Technology Special Publication 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*.
 - 31) National Institute of Standards and Technology Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*.
 - 32) National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*.
 - 33) National Institute of Standards and Technology *Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management*.
- b. References in this section without specific publication dates or revision numbers refer to the most recent updates to those publications.

Appendix II to OMB Circular A-130 Responsibilities for Managing Personally Identifiable Information

1. Purpose

This Appendix outlines some of the general responsibilities for Federal agencies managing information resources that involve personally identifiable information (PII) and summarizes the key privacy requirements included in other sections of this Circular. The requirements included in this Appendix apply to PII in any form or medium, including paper and electronic media. Although all of the requirements referenced in this Appendix concern the management of PII, some of the requirements are not solely the responsibility of agencies' privacy programs. The inclusion of shared requirements in this Appendix is not intended to suggest that agencies' privacy programs are solely or primarily responsible for meeting such requirements; however, agencies' privacy programs shall play a key role in meeting requirements that involve PII. This Appendix does not provide a comprehensive account of all the statutory and policy requirements associated with managing PII and protecting privacy. Agencies shall consult law, regulation, and policy, including OMB guidance, to understand all applicable requirements.

The main body of this Circular establishes general policies for Federal agencies managing information resources. Appendix I to this Circular establishes requirements for information security and privacy programs and provides guidance on how agencies should take a coordinated approach when managing Federal information resources. This Appendix and Appendix I are companion documents; it is important to review the appendices together in order to understand the coordination between privacy and security. As noted in the citations, all of the requirements summarized in the tables in this Appendix come from the main body or Appendix I to this Circular.

Previous versions of Circular A-130 included information about the reporting and publication requirements of the Privacy Act of 1974 ("Privacy Act") and additional OMB guidance. This information is being revised and will be reissued in OMB Circular A-108.¹¹⁵ This Appendix does not extend or interpret the Privacy Act, including agency requirements under the Privacy Act.

2. Introduction

The Federal Government necessarily creates, collects, uses, processes, stores, maintains, disseminates, discloses, and disposes of PII to carry out missions mandated by Federal statute. The term PII, as defined in this Circular, refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, the agency shall perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize

¹¹⁵ Agencies shall continue to apply the requirements in Appendix I of the 2000 version of Circular A-130 regarding review, reporting, and publication pertaining to the Privacy Act until OMB issues a revised version of those requirements in OMB Circular A-108.

that information that is not PII can become PII whenever additional information becomes available in any medium and from any source that would make it possible to identify an individual.

Once the agency determines that an information system contains PII, the agency shall then consider the privacy risks and the associated risk to agency operations, agency assets, individuals, other organizations, and the Nation. When considering privacy risks, the agency shall consider the risks to an individual or individuals associated with the agency's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of their PII. In particular, the agency shall evaluate the sensitivity of each individual data element that is PII, as well as all of the data elements together. The sensitivity level of the PII will depend on the context, including the purpose for which the PII is created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed. For example, the sensitivity level of a list of individuals' names may depend on the source of the information, the other information associated with the list, the intended use of the information, the ways in which the information will be processed and shared, and the ability to access the information. In addition, when determining the privacy and associated risks, the agency shall also consider the volume of PII. A higher volume of PII about a single individual or multiple individuals may pose increased privacy or associated risks.

3. Fair Information Practice Principles

The Fair Information Practice Principles (FIPPs) are a collection of widely accepted principles that agencies should use when evaluating information systems, processes, programs, and activities that affect individual privacy. The FIPPs are not OMB requirements; rather, they are principles that should be applied by each agency according to the agency's particular mission and privacy program requirements.

Rooted in a 1973 Federal Government report from the Department of Health, Education, and Welfare Advisory Committee, "Records, Computers and the Rights of Citizens," the FIPPs have informed Federal statute and the laws of many U.S. states and foreign nations, and have been incorporated in the policies of many organizations around the world. The precise expression of the FIPPs has varied over time and in different contexts. However, the FIPPs retain a consistent set of core principles that are broadly relevant to agencies' information management practices. For purposes of this Circular, the FIPPs are as follows:

- a. *Access and Amendment.* Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.¹¹⁶
- b. *Accountability.* Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to

¹¹⁶ The Access and Amendment principle is included as part of the "Individual Participation" privacy control family in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems*. OMB is including Access and Amendment as a stand-alone principle in this Circular to emphasize the importance of allowing individuals to access and amend their information when appropriate.

PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.

- c. *Authority.* Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.¹¹⁷
- d. *Minimization.* Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.¹¹⁸
- e. *Quality and Integrity.* Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.
- f. *Individual Participation.* Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.
- g. *Purpose Specification and Use Limitation.* Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.
- h. *Security.* Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.
- i. *Transparency.* Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.¹¹⁹

4. Senior Agency Official for Privacy

Agencies are required to designate a Senior Agency Official for Privacy (SAOP) who has agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirements and managing privacy risks. The SAOP shall have a central policy-making role and shall ensure that the agency considers the privacy impact of all agency actions and policies that involve PII. The SAOP's review of privacy risks should begin at the earliest planning and

¹¹⁷ The Authority principle is included as part of the "Purpose Specification" privacy control family in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems*. OMB is including Authority as a stand-alone principle in this Circular to emphasize the importance of identifying a specific authority for creating, collecting, using, processing, storing, maintaining, disseminating, or disclosing PII.

¹¹⁸ In some versions of the FIPPs, the "minimization" principle is referred to under a different name, such as "collection limitation."

¹¹⁹ In some versions of the FIPPs, the "transparency" principle is referred to under a different name, such as "openness."

development stages of agency actions and policies that involve PII, and should continue throughout the life cycle of the information.

The SAOP shall ensure that the agency complies with applicable privacy requirements in statute, regulation, and policy.

5. Agency Privacy Program

In order to manage Federal information resources that involve PII, agencies shall develop, implement, document, maintain, and oversee agency-wide privacy programs that include people, processes, and technologies. Among other things, where PII is involved, agencies' privacy programs shall play a key role in information security, records management, strategic planning, budget and acquisition, contractors and third parties, workforce, training, incident response, and implementing the Risk Management Framework. This Appendix does not provide a comprehensive account of all the statutory and policy requirements associated with managing PII and protecting privacy. Agencies shall consult law, regulation, and policy, including OMB guidance, to understand all applicable requirements.

Agencies' privacy programs are led by the SAOP and are responsible for ensuring compliance with applicable privacy requirements, developing and evaluating privacy policy, and managing privacy risks. At the discretion of the SAOP and consistent with applicable law, other qualified agency personnel may perform particular privacy functions that are assigned to the SAOP. Many of the requirements summarized in this Appendix are shared requirements and are not solely the responsibility of agencies' privacy programs. The inclusion of shared requirements in this Appendix is intended to convey that agencies' privacy programs shall be responsible to the extent that the requirements pertain to the management of PII.

a. General Requirements

Agencies shall have comprehensive privacy programs that ensure compliance with applicable privacy requirements, develop and evaluate privacy policy, and manage privacy risks. The following table summarizes many of the general privacy requirements that are set forth in this Circular. While some of the requirements summarized in the table are not exclusively privacy requirements, they may still require the involvement of agencies' privacy programs.

Responsibility	Description	Citation
Establish and maintain a comprehensive privacy program.	Agencies shall establish and maintain a comprehensive privacy program that ensures compliance with applicable privacy requirements, develops and evaluates privacy policy, and manages privacy risks.	Main Body § 5(f)(1)(a); Appendix I §§ 3(b), 3(f), 4(e).
Ensure compliance with privacy requirements and manage privacy risks.	Agencies shall ensure compliance with all applicable statutory, regulatory, and policy requirements and use privacy impact assessments and other tools to manage privacy risks. Agencies shall cost-effectively manage privacy risks and reduce such risks to an acceptable level.	Main Body §§ 4(g), 5(e)(1)(d), 5(f)(1)(a); Appendix I § 3(a), 3(b)(4), 3(f), 3(g).

Responsibility	Description	Citation
Monitor Federal law, regulation, and policy for changes.	Agencies shall monitor Federal law, regulation, and policy for changes that affect privacy.	Main Body § 5(f)(1)(c).
Develop and maintain a privacy program plan.	Agencies shall develop and maintain a privacy program plan that provides an overview of the agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the SAOP and other privacy officials and staff, the strategic goals and objectives of the privacy program, the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks, and any other information determined necessary by the agency's privacy program.	Appendix I § 4(c)(2), 4(e)(1).
Designate a Senior Agency Official for Privacy.	The head of each agency shall designate an SAOP who has agency-wide responsibility and accountability for developing, implementing, and maintaining an agency-wide privacy program to ensure compliance with all applicable statutes, regulations, and policies regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems, developing and evaluating privacy policy, and managing privacy risks at the agency.	Main Body § 5(f)(1)(b); Appendix I § 4(e).
Ensure coordination between privacy and other programs.	Agencies shall ensure that the SAOP and the agency's privacy personnel closely coordinate with the agency CIO, senior agency information security officer, and other agency offices and officials, as appropriate.	Main Body §§ 4(h), 5(f)(1)(k); Appendix I §§ 3(b)(11), 4(e)(10).
Ensure that privacy is addressed throughout the life cycle of each information system.	Agencies shall ensure that privacy is addressed throughout the life cycle of each agency information system.	Main Body §§ 4(g), 5(a)(1)(c)(i), 5(b)(4); Appendix I § 4(b)(2).
Incorporate privacy requirements into enterprise architecture.	Agencies shall incorporate Federal privacy requirements into the agency's enterprise architecture to ensure that risk is addressed and information systems achieve the necessary levels of trustworthiness, protection, and resilience.	Appendix I § 4(b)(5).
Comply with the Privacy Act.	Agencies shall comply with the requirements of the Privacy Act and ensure that Privacy Act system of records notices are published, revised, and rescinded, as required.	Main Body § 5(f)(1)(g).
Conduct privacy impact assessments.	Agencies shall conduct privacy impact assessments in accordance with the E-Government Act and make the privacy impact assessments available to the public in accordance with OMB policy.	Main Body § 5(f)(1)(i).

Responsibility	Description	Citation
Balance the need for information collection with the privacy risks.	Agencies shall ensure that the design of information collections is consistent with the intended use of the information, and the need for new information is balanced against any privacy risks.	Main Body § 4(i).
Comply with requirements for disclosure and dissemination.	Agencies shall comply with all applicable privacy statutes and policies governing the disclosure or dissemination of information and comply with any other valid access, use, and dissemination restrictions.	Main Body § 5(e)(1)(b)-(d), 5(e)(7)(h).
Maintain and post privacy policies on websites, mobile applications, and other digital services.	Agencies shall maintain and post privacy policies on all agency websites, mobile applications, and other digital services, in accordance with the E-Government Act and OMB policy.	Main Body § 5(f)(1)(j).
Provide performance metrics and reports.	Agencies shall provide performance metrics information and reports in accordance with processes established by OMB and DHS pursuant to FISMA.	Appendix I § 4(1).

b. Considerations for Managing PII

Agencies’ privacy programs shall maintain an inventory of PII, regularly review all PII maintained by the agency, and comply with applicable requirements regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII. In addition, agencies’ privacy programs shall impose, where appropriate, conditions on other agencies and entities to which PII is being disclosed that govern the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of the PII. The following table summarizes the privacy requirements in this Circular that pertain to the general management of PII. While some requirements summarized in the table are not exclusively privacy requirements, they may still require the involvement of agencies’ privacy programs.

Responsibility	Description	Citation
Maintain an inventory of agency information systems that involve PII and regularly review and reduce PII to the minimum necessary.	Agencies shall maintain an inventory of the agency’s information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to allow the agency to regularly review its PII and ensure, to the extent reasonably practicable, that such PII is accurate, relevant, timely, and complete; and to allow the agency to reduce its PII to the minimum necessary for the proper performance of authorized agency functions.	Main Body § 5(a)(1)(a)(ii), 5(f)(1)(e).
Eliminate unnecessary collection, maintenance, and use of Social Security numbers.	Agencies shall take steps to eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to the use of Social Security numbers as a personal identifier.	Main Body § 5(f)(1)(f).

Responsibility	Description	Citation
Follow approved records retention schedules for records with PII.	Agencies shall ensure that all records with PII are maintained in accordance with applicable records retention or disposition schedules approved by NARA.	Main Body § 5(f)(1)(h).
Limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.	Agencies shall limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of agency functions.	Main Body § 5(f)(1)(d).
Require entities with which PII is shared to maintain the PII in an information system with a particular categorization level.	Agencies that share PII shall require, as appropriate, other agencies and entities with which they share PII to maintain the PII in an information system with a particular NIST FIPS Publication 199 confidentiality impact level, as determined by the agency sharing the PII.	Appendix I § 3(c).
Impose conditions on the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of shared PII through agreements.	Agencies that share PII with other agencies or entities shall impose, where appropriate, conditions (including the selection and implementation of particular security and privacy controls) that govern the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of the PII through written agreements, including contracts, data use agreements, information exchange agreements, and memoranda of understanding.	Appendix I § 3(d).

c. Budget and Acquisition

Agencies’ privacy programs shall have the resources needed to manage Federal information resources that involve PII. This will require privacy programs to play a key role in the development of the agencies’ budget requests, as well as any decisions to acquire or develop information system technologies and services. The following table summarizes the privacy requirements in this Circular that pertain to budget and acquisition activities. While some of the requirements summarized in the table are not exclusively privacy requirements, they may still require the involvement of agencies’ privacy programs.

Responsibility	Description	Citation
Identify and plan for resources needed for privacy program.	Agencies shall identify and plan for the resources needed to implement privacy programs.	Appendix I § 4(b)(1).
Include privacy requirements in IT solicitations.	Agencies shall include privacy requirements in solicitations for IT and services.	Main body § 5(d)(1)(j).

Responsibility	Description	Citation
Establish a process to evaluate privacy risks for IT investments.	Agencies shall consider privacy when analyzing IT investments, and establish a decision-making process that shall cover the life of each information system and include explicit criteria for analyzing the projected and actual costs, benefits, and risks, including privacy risks, associated with the IT investments.	Main Body § 5(d)(3), 5(d)(4)(b).
Ensure that privacy risks are addressed and costs are included in IT capital investment plans and budgetary requests.	The SAOP shall review IT capital investment plans and budgetary requests to ensure that privacy requirements (and associated privacy controls), as well as any associated costs, are explicitly identified and included, with respect to any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII. Agencies shall ensure that agency budget justification materials, in their initial budget submission to OMB, include a statement affirming that the SAOP has conducted the necessary review.	Main Body § 5(a)(3)(e)(ii), 5(d)(3)(e); Appendix I § 4(b)(2), 4(e)(6).
Ensure that investment plans meet the privacy requirements appropriate for the life cycle stage of the investment.	Agencies shall ensure that investment plans submitted to OMB as part of the budget process meet the privacy requirements appropriate for the life cycle stage of the investment.	Appendix I § 4(b)(4).
Upgrade, replace, or retire unprotected information systems.	Agencies shall plan and budget to upgrade, replace, or retire any information systems for which protections commensurate with risk cannot be effectively implemented.	Appendix I § 4(b)(3).
Ensure that SAOPs are made aware of information systems and components that cannot be protected.	Agencies shall ensure that, in a timely manner, SAOPs are made aware of information systems and components that cannot be appropriately protected or secured, and that such systems are given a high priority for upgrade, replacement, or retirement.	Main Body § 5(a)(1)(c)(ii); Appendix I § 3(b)(10).

d. Contractors and Third Parties

Agencies’ privacy programs shall ensure that entities that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of information on behalf of a Federal agency or that operate or use information systems on behalf of a Federal agency, comply with the privacy requirements in law and OMB policies. The following table summarizes the privacy requirements in this Circular that pertain to contractors and third parties. While some of the requirements summarized in the table are not exclusively privacy requirements, they may still require the involvement of agencies’ privacy programs.

Responsibility	Description	Citation
Ensure that contracts and other agreements incorporate privacy requirements.	Agencies shall ensure that terms and conditions in contracts, and other agreements involving the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of Federal information, incorporate privacy requirements and are sufficient to enable agencies to meet Federal and agency-specific requirements pertaining to the protection of Federal information.	Main Body § 5(a)(1)(b)(ii); Appendix I § 4(j)(1).
Maintain agency-wide privacy training for all employees and contractors.	Agencies shall develop, maintain, and implement mandatory agency-wide privacy awareness and training programs for all employees and contractors.	Appendix I § 4(h)(1)-(2), (4)-(7).
Ensure that the Privacy Act applies to contractors where required.	Agencies shall, consistent with the agency's authority, ensure that the requirements of the Privacy Act apply to a Privacy Act system of records when a contractor operates the system of records on behalf of the agency to accomplish an agency function.	Appendix I § 4(j)(3).
Oversee information systems operated by contractors.	Agencies shall provide oversight of information systems used or operated by contractors or other entities on behalf of the Federal Government or that collect or maintain Federal information on behalf of the Federal Government.	Appendix I § 4(j)(2).
Implement policies on privacy oversight of contractors.	Agencies shall document and implement policies and procedures for privacy oversight of contractors and other entities, to include ensuring appropriate vetting and access control processes for contractors and others with access to information systems containing Federal information.	Appendix I § 4(j)(2)(a).
Ensure implementation of privacy controls for contractor information systems.	Agencies shall ensure that privacy controls of information systems and services used or operated by contractors or other entities on behalf of the agency are effectively implemented and comply with NIST standards and guidelines and agency requirements.	Appendix I § 4(j)(2)(b).
Maintain an inventory of contractor information systems.	Agencies shall ensure that information systems used or operated by contractors or other entities on behalf of the agency are included in the agency's inventory of information systems.	Appendix I § 4(j)(2)(c).
Ensure that incident response procedures are in place for contractor information systems.	Agencies shall ensure that procedures are in place for incident response for information systems used or operated by contractors or other entities on behalf of the agency, including timelines for notification of affected individuals and reporting to OMB, DHS, and other entities as required in OMB guidance.	Appendix I § 4(j)(2)(e).

e. Privacy Impact Assessments

As a general matter, an agency shall conduct a privacy impact assessment (PIA) under section 208(b) of the E-Government Act of 2002, absent an applicable exception under that section,

when the agency develops, procures, or uses information technology to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.¹²⁰ A PIA is an analysis of how PII is handled to ensure that handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or activity, and evaluate ways to mitigate privacy risks. A PIA is both an analysis and a formal document detailing the process and the outcome of the analysis.

A PIA is one of the most valuable tools Federal agencies use to ensure compliance with applicable privacy requirements and manage privacy risks. Agencies shall conduct and draft a PIA with sufficient clarity and specificity to demonstrate that the agency fully considered privacy and incorporated appropriate privacy protections from the earliest stages of the agency activity and throughout the information life cycle. In order to conduct a meaningful PIA, the agency's SAOP shall work closely with the program managers, information system owners, information technology experts, security officials, counsel, and other relevant agency officials.

Moreover, a PIA is not a time-restricted activity that is limited to a particular milestone or stage of the information system or PII life cycles. Rather, the privacy analysis shall continue throughout the information system and PII life cycles. Accordingly, a PIA shall be considered a living document that agencies are required to update whenever changes to the information technology, changes to the agency's practices, or other factors alter the privacy risks associated with the use of such information technology.

In addition to serving as an important analytical tool for agencies, a PIA also serves as notice to the public regarding the agency's practices with respect to privacy and information technology. All PIAs shall be drafted in plain language and shall be posted on the agency's website, unless doing so would raise security concerns or reveal classified or sensitive information. Although PIAs are generally required by law, such as by the E-Government Act of 2002, agencies may also develop policies to require PIAs in circumstances where a PIA would not be required by law.

f. Workforce Management

Agencies' privacy programs shall play a key role in workforce management activities. The SAOP shall be involved in assessing the hiring and professional development needs at the agency with respect to privacy. The following table summarizes the privacy requirements in this Circular that pertain to workforce management activities. While some of the requirements summarized in the table are not exclusively privacy requirements, they may still require the involvement of agencies' privacy programs.

¹²⁰ See 44 U.S.C. § 3501 note; Pub. L. 107-347, § 208(b). Section 208(b) of the E-Government Act requires agencies, absent an applicable exception under this section, to conduct a PIA before: (i) developing or procuring IT that collects, maintains, or disseminates information that is in an identifiable form; or (ii) initiating a new collection of information that – (I) will be collected, maintained, or disseminated using IT; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

Responsibility	Description	Citation
Ensure that the SAOP is involved in assessing and addressing privacy hiring, training, and professional development needs.	Agencies shall ensure that the SAOP is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy.	Main Body § 5(c)(6).
Maintain a workforce planning process.	Agencies shall ensure that the CHCO, CIO, CAO, and SAOP develop and maintain a current workforce planning process to ensure that the agency can anticipate and respond to changing mission requirements, maintain workforce skills in a rapidly developing IT environment, and recruit and retain the IT talent needed to accomplish the mission.	Main Body § 5(c)(1).
Develop a set of privacy competency requirements.	Agencies shall ensure that the CHCO, CIO, CAO, and SAOP develop a set of competency requirements for information resources staff, including program managers and information security, privacy, and IT leadership positions.	Main Body § 5(c)(1).
Ensure that the workforce has the appropriate knowledge and skill.	Agencies shall ensure that the workforce, which supports the acquisition, management, maintenance, and use of information resources, has the appropriate knowledge and skill.	Main Body § 5(c)(2).
Take advantage of flexible hiring authorities for specialized positions.	Agencies shall ensure that the CIO, CHCO, SAOP, and other hiring managers take advantage of flexible hiring authorities for specialized positions, as established by OPM.	Main Body § 5(c)(7).

g. Training and Accountability

Agencies’ privacy programs shall develop, maintain, and provide agency-wide privacy awareness and training programs for all employees and contractors. In addition, the privacy program shall establish rules of behavior for employees and contractors with access to PII and hold agency personnel accountable for complying with applicable privacy requirements and managing privacy risks. The following table summarizes the privacy requirements in this Circular that pertain to training and accountability activities. Some of the requirements summarized in the table are not solely privacy requirements but may require the involvement of agencies’ privacy programs.

Responsibility	Description	Citation
Maintain agency-wide privacy training for all employees and contractors.	Agencies shall develop, maintain, and implement mandatory agency-wide privacy awareness and training programs for all employees and contractors.	Appendix I § 4(h)(1).
Ensure that privacy training is consistent with applicable policies.	Agencies shall ensure that the privacy awareness and training programs are consistent with applicable policies, standards, and guidelines issued by OMB, NIST, and OPM.	Appendix I § 4(h)(2).

Responsibility	Description	Citation
Apprise agency employees about available privacy resources.	Agencies shall apprise agency employees about available privacy resources, such as products, techniques, or expertise.	Appendix I § 4(h)(3).
Provide foundational and advanced privacy training.	Agencies shall provide foundational as well as more advanced levels of privacy training to information system users (including managers, senior executives, and contractors) and ensure that measures are in place to test the knowledge level of information system users.	Appendix I § 4(h)(4).
Provide role-based privacy training to appropriate employees and contractors.	Agencies shall provide role-based privacy training to employees and contractors with assigned privacy roles and responsibilities, including managers, before authorizing access to Federal information or information systems or performing assigned duties.	Appendix I § 4(h)(5).
Hold personnel accountable for complying with privacy requirements and policies.	Agencies shall implement policies and procedures to ensure that all personnel are held accountable for complying with agency-wide privacy requirements and policies.	Appendix I § 3(b)(9).
Establish rules of behavior for employees and contractors with access to PII and consequences for violating the rules.	Agencies shall establish rules of behavior, including consequences for violating rules of behavior, for employees and contractors that have access to Federal information or information systems, including those that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.	Appendix I § 4(h)(6).
Ensure that employees and contractors read and agree to rules of behavior.	Agencies shall ensure that employees and contractors have read and agreed to abide by the rules of behavior for the Federal information and information systems for which they require access prior to being granted access.	Appendix I § 4(h)(7).

h. Incident Response

Agencies’ privacy programs shall develop and implement incident management and response capabilities. The following table summarizes the privacy requirements in this Circular that pertain to incident response. While some of the requirements summarized in the table are not solely privacy requirements, they may still require the involvement of agencies’ privacy programs.

Responsibility	Description	Citation
Maintain formal incident management and response policies and capabilities.	Agencies shall maintain formal incident response capabilities and mechanisms, implement formal incident management policies, and provide adequate training and awareness for employees and contractors on how to report and respond to incidents.	Appendix I § 4(f)(1), (7)-(8).

Responsibility	Description	Citation
Establish roles and responsibilities to ensure oversight and coordination of incident response.	Agencies shall establish clear roles and responsibilities to ensure the oversight and coordination of incident response activities and that incidents are documented, reported, investigated, and handled.	Appendix I § 4(f)(3).
Periodically test incident response procedures.	Agencies shall periodically test incident response procedures to ensure effectiveness of such procedures.	Appendix I § 4(f)(4).
Document incident response lessons learned and update procedures.	Agencies shall document lessons learned for incident response and update procedures annually or as required by OMB or DHS.	Appendix I § 4(f)(5).
Ensure that processes are in place to verify corrective actions.	Agencies shall ensure that processes are in place to verify corrective actions.	Appendix I § 4(f)(6).
Report incidents in accordance with OMB guidance.	Agencies shall report incidents to OMB, DHS, the CIO, the SAOP, their respective inspectors general and general counsel, law enforcement, and Congress in accordance with procedures issued by OMB.	Appendix I § 4(f)(9).
Provide reports on incidents as required.	Agencies shall provide reports on incidents as required by FISMA, OMB policy, DHS binding operational directives, Federal information security incident center guidelines, NIST guidelines, and agency procedures.	Appendix I § 4(f)(10).

i. Risk Management Framework¹²¹

Agencies’ privacy programs have responsibilities under the Risk Management Framework, which is also covered in Appendix I to this Circular. The Risk Management Framework provides a disciplined and structured process that integrates information security, privacy, and risk management activities into the information system development life cycle. This Circular requires agencies to use the Risk Management Framework to manage privacy risks beyond those that are typically included under the “confidentiality” objective of the term “information security.”¹²² While many privacy risks relate to the unauthorized access or disclosure of PII,

¹²¹ Traditionally, the Risk Management Framework was a framework to help agencies address information security and related risks in the authorization process for Federal information systems. As explained in this Appendix, this Circular integrates agencies’ privacy programs into the Risk Management Framework process. NIST has published a suite of standards and guidelines that describe how to implement an agency-wide risk management framework. As of the date of this publication, many of the existing NIST standards and guidelines that detail how to implement an agency-wide risk management framework do not fully address the role of privacy and agencies’ privacy programs. In the future, NIST may revise or develop standards and guidelines to further clarify how privacy and agencies’ privacy programs are integrated into the Risk Management Framework.

¹²² The term “information security,” as defined in law and in this Circular, includes three objectives: integrity, availability, and confidentiality. The term “confidentiality” means “preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.” See 44 U.S.C. § 3552.

privacy risks may also result from other activities, including the creation, collection, use, and retention of PII; the inadequate quality or integrity of PII; and the lack of appropriate notice, transparency, or participation.¹²³

The Risk Management Framework has the following steps:

- 1) *Categorize.* Agencies shall categorize each information system and the information processed, stored, and transmitted by that information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on agency operations, agency assets, individuals, other organizations, and the Nation.¹²⁴ Each information system is categorized at low, moderate, or high impact according to the criteria in NIST standards and guidelines. The SAOP is responsible for reviewing and approving the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.

The categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII will depend on the sensitivity of the PII, the privacy risks, and the associated risk to agency operations, agency assets, individuals, other organizations, and the Nation. Agencies should generally categorize information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII at the moderate or high confidentiality impact level.

- 2) *Select.* Agencies shall select security and privacy controls for each information system. A security control is a safeguard or countermeasure prescribed for an information system or an agency to protect the confidentiality, integrity, and availability of the system and its information. Security controls primarily pertain to security but they can also enhance privacy. Agencies shall select an initial set of baseline security controls for the information system based on the security categorization and then tailor the security control baseline, as needed, based on an assessment of security risk and local conditions.¹²⁵

A privacy control is an administrative, technical, or physical safeguard employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.¹²⁶ In order to help agencies satisfy privacy requirements and manage privacy risks, NIST has developed a set of privacy controls, based on the FIPPs, in Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information*

¹²³ Refer to the Fair Information Practice Principles in section 3 of this Appendix.

¹²⁴ See National Institute of Standards and Technology FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004), available at <http://csrc.nist.gov/publications>.

¹²⁵ The use of a privacy overlay may assist agencies in effectively selecting and tailoring security controls for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.

¹²⁶ Privacy risks can include risks beyond those that are typically included under the “confidentiality” prong of the term “information security.” Agencies shall use privacy controls to manage all privacy risks associated with PII or an information system, regardless of whether those risks would be considered information security risks.

Systems and Organizations.¹²⁷ Agencies are required to use the NIST privacy controls and shall implement a privacy control selection process for information systems. Agencies shall use NIST privacy controls in a manner that is consistent with the agency's authorities, missions, and operational needs.

For privacy controls, the SAOP is responsible for designating which controls the agency will treat as program management, common, information system-specific, and hybrid controls. Privacy program management controls are controls that are generally implemented at the agency level and essential for managing the agency's privacy program. Program management controls are distinct from common, information system-specific, and hybrid controls because program management controls are independent of any particular information system. Agencies shall document program management controls in their privacy program plan.

The other types of controls—common, information system-specific, and hybrid controls—are necessarily implemented, at least in part, at the information system level. Common controls are controls that are inherited by multiple information systems. When a control is inherited by an information system, the control is selected for the information system but the control is developed, implemented, assessed, authorized, and monitored by programs or officials other than those responsible for the information system. Information system-specific controls are controls that are implemented for a particular information system or the portion of a hybrid control that is implemented for a particular information system. Hybrid controls are controls that are implemented for an information system in part as a common control and in part as an information system-specific control.

The determination as to whether a privacy control is a common, hybrid, or information system-specific control is based on context. By assigning privacy controls to an information system as information system-specific, hybrid, or common controls, the agency assigns responsibility and accountability to specific agency programs or officials for the overall development, implementation, assessment, authorization, and monitoring of those controls. Privacy controls designated by the agency as common controls are, in most cases, managed by an agency program or official other than the information system owner. Moreover, privacy controls designated as information system-specific controls may be the primary responsibility of information system owners and their respective authorizing officials. In all cases, the management of privacy controls shall be subject to the coordination and oversight of the SAOP.

- 3) *Implement*. Agencies shall implement the security and privacy controls selected for an information system and document how the controls are deployed. Agencies shall develop and maintain security plans and privacy plans for an information system that provide an overview of the security and privacy requirements for the information system and describe the security and privacy controls in place or planned for meeting those requirements. All privacy controls that are selected for an information system shall be

¹²⁷ National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013), available at <http://csrc.nist.gov/publications>.

documented in the privacy plan for the information system. The security plan and the privacy plan may be separate or integrated into one consolidated document.

- 4) *Assess.* Agencies shall assess the security and privacy controls using appropriate methods to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and managing risks. The SAOP shall conduct an initial assessment of the privacy controls selected for an information system prior to operation, and shall assess the privacy controls periodically thereafter at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks. If a PIA is conducted for the information system, the agency may incorporate the initial assessment of the privacy controls into the PIA process.
- 5) *Authorize.* Agencies shall authorize an information system prior to operation and periodically thereafter. Authorization of an information system is an explicit acceptance of the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation, based on the implementation of the security and privacy controls. The determination to authorize an information system shall be made by an agency's authorizing official or officials (which may include the SAOP) and shall be based on a review of the information system authorization package, which includes the security plan, the privacy plan, documented assessments of the security and privacy controls, and any relevant plans of action and milestones.

Authorizing officials are responsible and accountable for the risks associated with an information system. However, since the SAOP is the senior official, designated by the head of each agency, who has agency-wide responsibility for privacy, agencies shall consider recommendations submitted by the SAOP in the decision to authorize an information system. In addition, the SAOP is responsible for reviewing the authorization package for an information system that creates, collects, uses, processes, stores, maintains, disseminates, discloses, or disposes of PII, to ensure compliance with applicable privacy requirements and manage privacy risks prior to system authorization.

- 6) *Monitor.* Agencies shall monitor and assess security and privacy controls selected for an information system and shall continue to monitor and assess those controls on an ongoing basis. This includes assessing the effectiveness of the security and privacy controls, documenting changes to the information system, analyzing the security and privacy impact associated with the changes, and reporting the state of the system to appropriate agency officials. The type, rigor, and frequency of control assessments shall be sufficient to account for risks that change over time based on changes in the threat environment, agency missions and business functions, personnel, technology, or environments of operation.

The ongoing assessment of privacy risks and privacy controls is referred to as privacy continuous monitoring (PCM). The SAOP shall develop and maintain a written PCM strategy that catalogs the available privacy controls implemented at the agency across the agency risk management tiers and ensures that the controls are effectively monitored

on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.

In addition, the SAOP shall establish and maintain a PCM program to implement the PCM strategy. The PCM program is an agency-wide program that is responsible for: maintaining ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitoring changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and conducting privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and management of privacy risks.

Although the term “privacy continuous monitoring” is new to this Circular, the concept of conducting an ongoing assessment of privacy risks is not new. For many IT systems, agencies are already required to conduct PIAs that involve an analysis of privacy risks throughout the life cycle of the information system and the PII, and the drafting of a living document that is updated whenever changes to the IT or the agency’s practices alter the privacy risks associated with the use of the IT.¹²⁸ In fact, for IT systems for which a PIA is conducted, agencies may use the PIA as the principal tool to satisfy the requirement to assess the privacy controls for an information system.

The requirement for agencies to implement the Risk Management Framework is described in more detail in Appendix I to this Circular. The following table summarizes the privacy requirements in this Circular that pertain to the Risk Management Framework. While some of the requirements summarized in the table are not exclusively privacy requirements, they may still require the involvement of the agencies’ privacy programs.

Responsibility	Description	Citation
Implement a risk management framework.	Agencies shall implement a risk management framework to guide and inform the categorization of Federal information and information systems; the selection, implementation, and assessment of privacy controls; the authorization of information systems and common controls; and the continuous monitoring of information systems.	Appendix I § 3(a), 3(b)(5).
Review and approve the categorization of information systems that involve PII.	The SAOP shall review and approve, in accordance with NIST FIPS Publication 199 and NIST Special Publication 800-60, the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.	Appendix I § 4(a)(2), 4(e)(7).

¹²⁸ Refer to section 5.e of this Appendix for additional information about PIAs.

Responsibility	Description	Citation
Designate program management, common, information system-specific, and hybrid privacy controls.	The SAOP shall designate which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls at the agency. Agencies shall designate common controls in order to provide cost-effective privacy capabilities that can be inherited by multiple agency information systems or programs.	Appendix I § 4(c)(12), 4(e)(5).
Implement a privacy control selection process.	Agencies shall employ a process to select and implement privacy controls for information systems and programs that satisfies applicable privacy requirements in OMB guidance, including, but not limited to, Appendix I to this Circular and OMB Circular A-108, <i>Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act</i> .	Appendix I § 4(c)(6).
Develop, approve, and maintain privacy plans for information systems.	The SAOP shall review and approve the privacy plans for agency information systems prior to authorization, reauthorization, or ongoing authorization. Agencies shall develop and maintain a privacy plan that details the privacy controls selected for an information system that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls.	Appendix I § 4(c)(9), 4(e)(8).
Identify privacy control assessment methodologies and metrics.	The SAOP shall identify assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks.	Appendix I § 4(e)(4).
Conduct assessments of privacy controls.	The SAOP shall conduct and document the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across all agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks. Agencies shall conduct and document privacy control assessments prior to the operation of an information system, and periodically thereafter, consistent with the frequency defined in the agency privacy continuous monitoring strategy and the agency risk tolerance.	Appendix I §§ 3(b)(6), 4(c)(13)-(14), 4(e)(3).
Correct deficiencies that are identified in information systems.	Agencies shall correct deficiencies that are identified through privacy assessments, the privacy continuous monitoring program, or internal or external audits and reviews, to include OMB reviews. Agencies shall use agency plans of action and milestones to record and manage the mitigation and remediation of identified weaknesses and deficiencies, not associated with accepted risks, in agency information systems.	Appendix I § 4(c)(15), 4(k).

Responsibility	Description	Citation
Develop and maintain a privacy continuous monitoring strategy.	The SAOP shall develop and maintain a privacy continuous monitoring strategy, a formal document that catalogs the available privacy controls implemented at the agency across the agency risk management tiers and ensures that the privacy controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.	Appendix I § 4(d)(9), 4(e)(2).
Establish and maintain a privacy continuous monitoring program.	The SAOP shall establish and maintain an agency-wide privacy continuous monitoring program that implements the agency's privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks. Agencies shall ensure that a robust privacy continuous monitoring program is in place before agency information systems are eligible for ongoing authorization.	Appendix I §§ 3(b)(6), 4(d)(10)-(11), 4(e)(2).
Review authorization packages for information systems that involve PII.	The SAOP shall review authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to ensure compliance with applicable privacy requirements and manage privacy risks, prior to authorizing officials making risk determination and acceptance decisions.	Appendix I § 4(e)(9).
Encrypt moderate-impact and high-impact information.	Agencies shall encrypt all NIST FIPS Publication 199 moderate-impact and high-impact information at rest and in transit, unless encrypting such information is technically infeasible or would demonstrably affect the ability of agencies to carry out their respective missions, functions, or operations; and the risk of not encrypting is accepted by the authorizing official and approved by the agency CIO, in consultation with the SAOP (as appropriate).	Appendix I § 4(i)(14).

6. Managing PII Collected for Statistical Purposes Under a Pledge of Confidentiality

The Nation relies on the flow of credible statistics to support the decisions of individuals, households, governments, businesses, and other organizations. Any loss of trust in the relevance, accuracy, objectivity, or integrity of the Federal statistical system and its products can foster uncertainty about the validity of measures our Nation uses to monitor and assess performance, progress, and needs.

Given the importance of robust and objective official Federal statistics, agencies and components charged with the production of these statistics are assigned particular responsibility. Specifically, information acquired by an agency or component under a pledge of confidentiality¹²⁹ and for exclusively statistical purposes shall be used by officers, employees, or agents of the agency exclusively for statistical purposes.¹³⁰ As defined in the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), statistical purpose refers to the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that comprise such groups; it includes the development, implementation, or maintenance of methods, technical or administrative procedures, or information resources that support such purposes.¹³¹ These agencies and components shall protect the integrity and confidentiality of this information against unauthorized access, use, disclosure, modification, or destruction throughout the life cycle of the information. Further, these agencies and components shall adhere to legal requirements and should follow best practices for protecting the confidentiality of data, including training their employees and agents, and ensuring the physical and information system security of confidential information.

¹²⁹ The term “confidentiality” can have multiple meanings. For example, in the context of general information security, the term means “preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.” *See* 44 U.S.C. § 3552. However, for the purposes of section 6 of Appendix II to this Circular, the term “confidentiality” refers to the requirement that “data or information acquired by an agency under a pledge of confidentiality for exclusively statistical purposes shall not be disclosed by an agency in identifiable form, for any use other than an exclusively statistical purpose, except with the informed consent of the respondent.” *See* 44 U.S.C. § 3501 note; Pub. L. 107–347, § 512(b)(1).

¹³⁰ 44 U.S.C. § 3501 note; Pub. L. 107-347, § 512(a). There are some narrowly-delineated, authorized, nonstatistical uses of information collected for statistical purposes that are noted in Section 504 of CIPSEA, including providing information to a law enforcement agency for the prosecution of submissions to the collecting agency of false statistical information under statutes that authorize criminal or civil penalties for the provision of false statistical information, unless such disclosure or use would otherwise be prohibited under Federal law.

¹³¹ 44 U.S.C. § 3501 note; Pub. L. 107-347, § 502(9)(A)).

United States Department of Commerce

Privacy Act, Personally Identifiable Information (PII), and Business Identifiable Information (BII) Breach Notification Plan

The goal of the Department of Commerce is to ensure that all Departmental Information Processes are compliant with and adhere to all Privacy Laws, Mandates, and Best Practices.

**Version 3.0
July 2017**



Department of Commerce PII, BII, and PA Breach Response and Notification Plan



COMMERCE PRIVACY MISSION STATEMENT

The Department of Commerce is committed to safeguarding personal privacy. Individual trust in the privacy and security of personally identifiable information is a foundation of trust in government and commerce in the 21st Century. As an employer, a collector of data on millions of individuals and companies, the developer of information-management standards and a federal advisor on information management policy, the Department strives to be a leader in best privacy practices and privacy policy. To further this goal, the Department assigns a high priority to privacy considerations in all systems, programs, and policies.

This Plan establishes governing policies and procedures for privacy incident handling at the Department of Commerce (DOC). The policies and procedures are based on applicable laws, Presidential Directives, and Office of Management and Budget (OMB) directives. It was originally developed in response to memoranda issued by the OMB and has been revised according to the most recent memoranda issued in 2017.¹

Please contact the DOC Senior Agency Official for Privacy (SAOP)/ Chief Privacy Officer (CPO) in the Office of Privacy and Open Government (OPOG) at cpo@doc.gov or (202) 482-1190 concerning questions about this Plan or the DOC Privacy Program.

¹ OMB Memorandum regarding “Preparing for and Responding to a Breach of Personally Identifiable Information”, issued on January 3, 2017 ([OMB M-17-12](#)).



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Table of Contents

1.0 INTRODUCTION.....	1
1.1 PURPOSE	1
1.2 BACKGROUND.....	1
1.3 SCOPE	2
1.4 AUTHORITIES	2
2.0 DEFINITIONS AND EXAMPLES	3
3.0 ROLES AND RESPONSIBILITIES	7
3.1 BUREAU/OPERATING UNIT CIRT (BOU CIRT).....	7
3.2 BUREAU CHIEF PRIVACY OFFICER (BCPO)	9
3.3 ENTERPRISE SECURITY OPERATIONS CENTER (ESOC)	11
3.4 SENIOR AGENCY OFFICIAL FOR PRIVACY (SAOP)/CHIEF PRIVACY OFFICER (CPO)	11
3.5 DOC PII BREACH RESPONSE TASK FORCE	12
3.6 OFFICE OF THE CHIEF INFORMATION OFFICER (OCIO)	13
3.7 OFFICE OF GENERAL COUNSEL (OGC)/BUREAU CHIEF COUNSEL (BCC).....	13
3.8 OFFICE OF INSPECTOR GENERAL (OIG)	13
3.9 OFFICE OF LEGISLATIVE AND INTERGOVERNMENTAL AFFAIRS (OLIA).....	13
3.10 PRIVACY COUNCIL.....	14
3.11 OFFICE OF PUBLIC AFFAIRS (OPA)	14
3.12 SUPERVISOR/MANAGER	14
3.13 EMPLOYEE/CONTRACTOR	14
4.0 DOC PII/BII/PA INCIDENT RESPONSE PROCESS	15
5.0 RISK OF HARM ANALYSIS FACTORS AND RATING ASSIGNMENT.....	17
6.0 BREACH NOTIFICATION AND REMEDIATION	19
6.1 NOTIFYING INDIVIDUALS	19
6.2 METHOD OF NOTIFICATION.....	20
6.3 NOTIFICATION/REPORTING REQUIREMENTS	21
7.0 CONSEQUENCES	21
APPENDIX A – DOC PII INCIDENT REPORT CONTENT	22
APPENDIX B – RISK LEVEL EVALUATION MATRIX	24
RISK LEVEL EVALUATION MATRIX	25
EXAMPLES: HOW TO USE RISK LEVEL EVALUATION MATRIX	26
Scenario 1: Resulting from PII Owner Action and/or Personal Use	26
Scenario 2: Valid Need to Know and Authorized User	26
Scenario 3: Authorized User, but One or More Recipients has no Need to Know.....	27

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



Scenario 4: Not Authorized, Greater than 10 PII Fields, and Affecting More than 2500
Individuals 27

APPENDIX C – DELEGATION OF AUTHORITY MEMORANDUM 28

APPENDIX D – FLOWCHART 29

**APPENDIX E – SENIOR AGENCY OFFICIAL FOR PRIVACY/CHIEF PRIVACY
OFFICER AND COMMERCE OPERATING UNIT CIRT REPORTING OFFICES
..... 30**

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



1.0 Introduction

1.1 Purpose

The Department of Commerce (DOC, Commerce, or the Department) has a duty to appropriately safeguard personally identifiable information (PII) in its possession and to prevent its compromise in order to maintain the public's trust. This Breach Response and Notification Plan (the Plan) serves this purpose by informing DOC and its bureaus, employees, and contractors of their obligation to protect PII and by establishing procedures defining how they must prepare for and respond to a PII incident.

The Plan also addresses response and notification procedures for business identifiable information (BII) and Privacy Act (PA) incidents.

1.2 Background

The Office of Management and Budget (OMB) regularly issues memoranda which require agencies to assess and mitigate the risk of harm to individuals potentially affected by a breach and develop guidance on whether and how to provide notification and services to those individuals. This Plan establishes appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records for any individual on whom information is maintained. Further, OMB requires each agency to develop a breach notification policy and plan, and to establish a core management team responsible for responding to the breach of PII/BII.

Pursuant to these OMB requirements, this Plan:

- Outlines procedures for reporting a DOC breach;
- Provides guidance for assessing and mitigating the risk of harm to individuals potentially affected by a breach;
- Delineates the investigation process, notification and remediation plan;
- Identifies applicable privacy compliance documentation;
- Lists the appropriate information sharing when responding to a breach; and
- Establishes the breach response team, called the DOC PII Breach Response Task Force (Task Force).

This Plan supplements current requirements for reporting and handling incidents pursuant to the Federal Information Security Modernization Act (FISMA), National Institute of Standards and Technology (NIST) [Special Publication 800-61](#), Computer Security Incident Handling Guide, and the concept of operations for Department of Homeland Security (DHS), United States



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Computer Emergency Readiness Team (US-CERT). All Bureaus, Operating Units, and contractors are responsible for compliance with this Plan.

1.3 Scope

The DOC PII, BII, and PA Breach Response and Notification Plan applies to all DOC and Bureau personnel including contractors, and to all DOC and Bureau information systems and information in any format (e.g., paper, electronic, etc.).

1.4 Authorities

- The [Privacy Act of 1974, 5 U.S.C. § 552a](#), provides privacy protections for records containing information about individuals (i.e., citizen and legal permanent resident) that are collected and maintained by the federal government and are retrieved by a personal identifier. The Act requires agencies to safeguard information contained in a system of records.
- The [Federal Information Security Modernization Act of 2014, Public Law No. 113-283](#), requires agencies to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of an agency.
- [US-CERT Federal Incident Notification Guidelines](#), effective April 1, 2017, provides guidance for notifying the computer emergency readiness team of any incident that jeopardizes the integrity, confidentiality, or availability of information or an information system.
- [OMB Memorandum M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 \(September 26, 2003\)](#), requires agencies to conduct reviews of how information about individuals is handled when information technology (IT) is used to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information, and to describe how the agency handles information that individuals provide electronically.
- [OMB Memorandum M-06-16, Protection of Sensitive Agency Information \(June 23, 2006\)](#), requires agencies to implement encryption protections for PII being transported and/or stored offsite.
- [OMB Memorandum M-11-02, Sharing Data While Protecting Privacy \(November 3, 2010\)](#), requires agencies to develop and implement solutions that allow data sharing to move forward in a manner that complies with applicable privacy laws, regulations, and policies.
- [OMB Memorandum M-16-04, Cybersecurity Strategy and Implementation Plan \(CSIP\) for the Federal Civilian Government \(October 30, 2015\)](#), requires agencies to take immediate

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



steps to further protect Federal information and assets and improve the resilience of Federal networks.

- [OMB Memorandum M-17-05, Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements \(November 4, 2016\)](#), requires oversight and reporting requirements for Information Security and Privacy Programs and updates major incident definition and US-CERT notification guidelines.
- [OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information \(January 3, 2017\)](#).

2.0 Definitions and Examples

- **Authorized User** - A person or persons granted permission to manage, access or make decisions regarding PII.
- **Breach/Incident** - For the purposes of this document, a PII breach incident includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses sensitive PII, or (2) an authorized user accesses or potentially accesses sensitive PII for other than an authorized purpose. A PII breach incident is not limited to an occurrence where a person other than an authorized user potentially accesses sensitive PII by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A breach incident may also include:
 - The loss or theft of physical documents that include sensitive PII and portable electronic storage media that stores sensitive PII. This could be a laptop or portable storage device storing sensitive PII which is lost or stolen, or a box of documents with sensitive PII which is lost or stolen during shipping;
 - The inadvertent disclosure of sensitive PII. Examples include an email containing PII/BII which is inadvertently sent to the wrong person or sensitive PII that should not be widely disseminated is posted inadvertently on a public website;
 - An employee sending their own sensitive PII via an unencrypted email;
 - An oral disclosure of sensitive PII to a person who is not authorized to receive that information. For example, an unauthorized third party overhears agency employees discussing sensitive PII about an individual seeking employment or Federal benefits;
 - An authorized user accessing sensitive PII for other than an authorized purpose. An example is a user with authorized access to sensitive PII sells it for personal gain or disseminates it to embarrass an individual.



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

- **Business Identifiable Information (BII)** Information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person and privileged or confidential." Commercial or financial information is considered confidential if disclosure is likely to cause substantial harm to the competitive position of the person from whom the information was obtained.
- **Close-out** The process by which the Bureau Privacy Officer (BPO) or BPO designee closes a PII incident report. Close-out is warranted after completion of the investigation of the incident, issuance of external notification if appropriate, and implementation of all suitable privacy and IT security mitigation, corrective, and/or remedial actions. If a portion of one or more of these stages is ongoing, the incident cannot be closed. Written SAOP/CPO concurrence is required for close-out of Moderate and High risk PII incidents.
- **Computer Incident Response Team (CIRT)²** A capability set up for the purpose of assisting in responding to computer security-related incidents. [[NIST SP 800-61](#)]. This capability may include resources, such as staff, tools, monitoring, and intrusion detection/prevention services.
- **Corrective/Remedial Actions** Steps taken to mitigate losses and protect against any further breaches.
- **Enterprise Security Operations Center (ESOC)** – the committee that provides the Department of Commerce with cybersecurity status information and decision-making regarding cyber threat risks of various types.
- **Harm** Any adverse effects that would be experienced by an individual whose sensitive PII was the subject of a breach, as well as any adverse effects experienced by the organization that maintains the PII. Harm to an individual includes any negative or unwanted effects (i.e., anything that may be socially, physically, or financially damaging). Examples of types of harm to individuals include, but are not limited to, the potential for blackmail, identity theft, physical harm, discrimination, or emotional distress. Organizations may also experience harm as a result of a loss of sensitive PII maintained by the organization, including but not limited to administrative burden, financial losses, loss of public reputation and public confidence, and legal liability.

² Throughout the Plan, the term CIRTs refer to both the DOC CIRT and Bureau/Operating Unit (BOU) CIRT, except where otherwise specified.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



[[NIST SP 800-122](#)].

➤ **Major Incident** Incidents requiring a report to Congress no later than seven (7) days after the date on which the Department has considered the totality of circumstances of the affects the risk poses to the Department or Bureau/Operating Unit (BOU) and individuals and concluded a major incident has occurred. Incidents are considered major when:

- The information involved is Classified, Controlled Unclassified Information (CUI), or PII; the incident resulted in the loss of critical service availability for all users or for at least 10,000 users, for eight hours or more; and the potentially compromised information poses a risk of harm to the Department or BOU and individuals.
 - a. The Department CIO shall document a determination that potentially compromised information does not pose a risk of harm to the affected organizations and individuals as well as any risk mitigations in place.

Or

- The information involved is Classified, CUI, or PII; the incident resulted in the unauthorized modification, deletion, exfiltration of, or access to any records:
 - a. Related to 10,000 or more individuals; or
 - b. Compromised or likely to result in a significant impact to Department mission, public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence;and the potentially compromised information poses a risk of harm to the affected organizations and individuals.
 - a. The Department CIO shall document a determination that potentially compromised information does not pose a risk of harm to the Department or BOU and individuals, as well as any risk mitigations in place.

➤ **Need to Know** - Information or data that is restricted due to its sensitive nature and the information is only given when needed or authorized.

➤ **Personally Identifiable Information (PII)** Information that can be used to distinguish or trace an individual's identity, such as name, Social Security number (SSN), biometric records, etc., alone, or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

- Sensitive PII is personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.
- Some forms of PII are sensitive as stand-alone data elements. Examples of such



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

PII include: SSN, driver's license or state identification number, passport number, Alien Registration Number, or financial account number. SSNs including truncated SSNs revealing only the last four digits are considered sensitive PII, both stand-alone and when associated with any other identifiable information.

- Other data elements such as citizenship or immigration status; medical information; ethnic, religious, sexual orientation, or lifestyle information; and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred), are also sensitive PII.
 - Additionally, the context of the PII may determine whether it is sensitive, such as a list of names of employees with poor performance ratings.
- **Privacy Act (PA) Incident** Disclosure of official records containing individually identifiable information that is prohibited by 5 U.S.C. § 552a, or regulations established thereunder. A PA incident occurs when an officer or employee of the Department, who by virtue of employment or official position with possession of, or access to records, discloses the material in any manner to any person or agency not entitled to receive it. NOTE: PA protection is based on how an individual's personal information is maintained by the government. If personal information is maintained by the government in a manner that is searchable by a personal identifier, it is PA information that must be covered under a published System of Records Notice (SORN). Disclosure of a PA record covered by a particular SORN without an identified routine use or another PA exception is considered a PA incident.³
- **Risk** The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. [[NIST FIPS 200](#)].
- **Low** is defined as the loss of confidentiality, integrity, or availability that is expected to have a **limited** adverse effect on organizational operations, organization assets or individuals. Breach incidents resulting from the following may be defined as Low if there was no failure of a Commerce IT security control:
 - a. An individual exposed his/her own sensitive PII.
 - b. A PII incident resulted from personal use of Commerce IT.

³ The twelve exceptions to the “No Disclosure Without Consent Rule” are: 1) “need to know” within agency; 2) required FOIA disclosure; 3) routine uses; 4) Bureau of the Census; 5) statistical research; 6) National Archives and Records Administration; 7) law enforcement request; 8) health or safety of an individual; 9) Congress; 10) General Accountability Office; 11) court order; and 12) Debt Collection Act. Additional information is available on the U.S. Department of Justice website: [Overview of the Privacy Act of 1974](#).

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



- **Moderate** is defined as the loss of confidentiality, integrity, or availability that is expected to have a **serious** adverse effect on organizational operations, organization assets or individuals.
 - **High** is defined as the loss of confidentiality, integrity, or availability that is expected to have a **severe or catastrophic** adverse effect on organizational operations, organization assets or individuals.
- **Security Control** The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [NIST FIPS 200]. For the protection of PII, security controls may include password protection, data encryption, full-disk encryption, or “auto-wipe” and “remote kill” features that provide the ability to protect a lost device by remotely disabling accessibility to data.
 - **Substitute Notification** A supplemental notification of an incident breach which keeps potentially affected individuals informed when there is insufficient contact information or a means by which affected individuals are informed collectively. A substitute notification consists of a conspicuous posting of the notification on the home page of the Department’s website and/or notification to major print and broadcast media, including major media in areas where the potentially affected individuals reside. Substitute notification includes phone numbers and email for affected individuals to use.

3.0 Roles and Responsibilities

3.1 Bureau/Operating Unit CIRT (BOU CIRT)⁴

- Reports all sensitive PII breach incidents within one (1) hour of discovery/detection to the SAOP/CPO, **AND** Enterprise Security Operations Center (ESOC).
- Reports all incidents to the SAOP/CPO at: cpo@doc.gov.
- Reports all incidents to the ESOC at: ESOC@doc.gov or 202-482-4000.
- Provides information on all sensitive PII breach incidents in the initial incident report (or as much of the information as known) in the format provided in [Appendix A](#)
- Ensures an initial risk of harm rating (Low, Moderate, or High) is assigned by the BCPO as part of the initial reporting for each PII incident using [Appendix B](#) - Risk Level Evaluation Matrix.

⁴Throughout this Plan, Bureau/Operating Unit CIRT (BOU CIRT) may refer to the Bureau’s/Operating Unit’s Privacy Office, Information Technology Security Officer (ITSO), or Information System Security Officer (ISSO) as prescribed by the Bureau’s/Operating Unit’s policies/processes, Service Level Agreement (SLA), and/or Memorandum of Understanding (MOU).



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

- Investigates all sensitive PII breach incidents within 48 hours of the incident discovery/detection and provides a follow-up report to the SAOP/CPO, ESOC, and BCPO. Investigates means that the following information has been documented in an incident report and submitted to the ESOC and SAOP/CPO: initial risk rating, mitigation and corrective/remedial actions, and any details/special circumstances missing from the initial report.
- Continues to investigate the incident, as necessary, and follows-up on all open incidents as part of the weekly SAOP/CPO reporting until the incident is closed out.
- Ensures the Privacy Task Force Package is built by the BCPO with coordination of the SAOP/CPO for Moderate and High risk incidents, if required.
- Ensures all applicable compliance documentation is identified, such as SORNs, Privacy Impact Assessments, and privacy notices, when responding to a breach incident.
- For PA and BII incidents involving no breach of sensitive PII, ensures PA incident without PII is turned over to the Bureau Chief Counsel (BCC) for investigation.
- Coordinates with BCPO to consult with the BCC as appropriate on BII incidents without sensitive PII to determine if a Trade Secrets Act violation occurred, dates of referral to the BCC for investigation are documented and sensitive PII portion of breach is closed.
- For PA and BII incidents which do involve breach of sensitive PII, ensures BCC notification of BII/PA aspects of incident, continuation of PII processing noting BII/PA efforts in parallel, and BCC instructions are followed to close BII/PA portion of incident.
- In instances where a PA violation occurs solely because an individual sends PA information via an unencrypted email, the BCPO's investigation clearly indicates that the violation via the unencrypted email was inadvertent, and remedial measures have already been taken to mitigate the PII breach, ensures that the BCPO does not refer the matter to the BCC for further review.
- Ensures the appropriate Property Management Office is notified of the loss when it involves network server, desktop computer, laptop computer, notebook computer, or other media and/or storage equipment, so that appropriate property management controls can be considered.
- Ensures notification to the Office of Inspector General (OIG), when necessary (e.g., intentional acts, criminal acts).
 - The OIG has discretion to contact the Attorney General/Department of Justice.
- Ensures notification to the appropriate law enforcement authorities:
 - Office of Security (OSY) and/or the Bureau-managed police force, when applicable;
 - Local law enforcement (Police Department), if incident involves theft from locations other than the workplace (e.g., laptop stolen from personal or government vehicle, laptop stolen from home); or

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



- Federal Protective Service (FPS), if incident involves theft from workplace locations that include facilities managed by the General Services Administration (GSA).
- Documents completion of all appropriate corrective/remedial actions in the incident report prior to close-out of PII incident.
- Supports and participates in tabletop exercise with the Task Force in order to practice a coordinated response to a breach, assist to refine and validate the Plan, and assist to further identify potential weaknesses in the Department's response capabilities.

3.2 Bureau Chief Privacy Officer (BCPO)⁵

- Ensures effective BOU execution of each breach response.
- Represents BOU in all Commerce Privacy Program meetings/events.
- Ensures all BOU sensitive PII incidents are reported within one (1) hour of discovery/detection to the SAOP/CPO, and ESOC.⁶
- Ensures the BOU PII incident reporting process requires collection of all [Appendix A](#) identified fields of information.
- Evaluates all BOU PII incidents in accordance with [Appendix B](#) Risk Level Evaluation Matrix and assigns a risk of harm rating at initial report, changing as necessary upon completion of the investigation.
- Notifies the appropriate Property Management Office of the loss when it involves network server, desktop computer, laptop computer, notebook computer, or other media and/or storage equipment, so that appropriate property management controls can be considered.
- Notifies the OIG, when necessary (e.g., intentional acts, criminal acts)
 - The OIG has discretion to contact the Attorney General/Department of Justice.
- Notifies to the appropriate law enforcement authorities:
 - Office of Security (OSY) and/or the Bureau-managed police force, when applicable;
 - Local law enforcement (Police Department), if incident involves theft from locations other than the workplace (e.g., laptop stolen from personal or government vehicle, laptop stolen from home); or
 - Federal Protective Service (FPS), if incident involves theft from workplace locations that include facilities managed by the General Services Administration (GSA).
- Ensures all BOU PII incidents are under investigation within 48 hours of the incident discovery/detection and a follow-up report has been submitted to the SAOP/CPO and

⁵ Includes privacy officers in Operating Units.

⁶ As indicated in [OMB Memorandum M-17-05](#), "Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements (November 4, 2016).



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

ESOC. Under investigation means that the following information has been documented in an incident report and submitted to the ESOC and SAOP/CPO: initial risk rating, mitigation and corrective/remedial actions, and any details/special circumstances missing from the initial report.

- Builds the Privacy Task Force Package in coordination with the SAOP/CPO for Moderate and High risk incidents, if required.
- Identifies all applicable compliance documentation, such as SORNs, Privacy Impact Assessments, and privacy notices, when responding to a breach.
- Ensures appropriate management attention is given to repeat offenders.
- Maintains thorough records of PII incidents from the initial report through the completed response.
- Ensures completion of corrective/remedial actions for each PII incident and ensures BOU CIRT has documented completion of these actions in the incident report prior to close-out of PII incident.
- Closes Low risk incidents and provides closure notification to SAOP/CPO and ESOC.
- Sends closure concurrence requests for Moderate and High risk PII incidents to the SAOP/CPO.
- For PA and BII incidents involving no breach of PII, turns over PA incidents without PII to the BCC for investigation, coordinates with BOU CIRT to consult with the BCC as appropriate on BII incidents without PII to determine if a Trade Secrets Act violation occurred, documents dates of referral to the BCC for investigation, and closes PII portion of breach.
- For PA and BII incidents which do involve breach of PII, notifies the BCC of BII/PA aspects of incident, continues PII processing noting BII/PA efforts in parallel, and follows BCC instructions to close BII/PA portion of incident.
 - In instances where a PA violation occurs solely because an individual sends PA information via an unencrypted email, the BCPO's investigation clearly indicates that the violation via the unencrypted email was inadvertent, and remedial measures have already been taken to mitigate the PII breach, the BCPO is not required to refer the matter to the BCC for further review.
- Provides training to BOU personnel regarding the handling of PII breach response, as needed.
- Delegates a BCPO responsibility only to fully qualified individuals and designation is made in writing to the SAOP/CPO (Sample delegation of authority memorandum is provided in [Appendix C](#)).
- Ensures BOU policies and training are updated, as appropriate, in response to problems identified by a specific incident or trends indicated by several incidents.
- Ensures that contract terms necessary for the Department to respond to a breach are included in contracts when a contractor collects or maintains Federal information on

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



behalf of the Department or uses or operates an information system on behalf of the Department.

- Provides reporting to the Bureau Senior Management as necessary.
- Supports and participates in tabletop exercise with the Task Force in order to practice a coordinated response to a breach, assist to refine and validate the Plan, and assist to further identify potential weaknesses in the Department's response capabilities

3.3 Enterprise Security Operations Center (ESOC)

- Reports all cyber PII incidents within one (1) hour of notification to the SAOP/CPO and the US-CERT by completing the US-CERT Incident Reporting System form.
- Ensures all non-cyber PII incidents have been reported to the SAOP/CPO within one (1) hour of notification.
- Requests status updates when needed from the BCPO and/or BOU CIRT.
- Provides closure notification to US-CERT and SAOP/CPO for all cyber low risk PII incidents; provides closure notification to US-CERT for all cyber moderate/high risk PII incidents; and provides closure notification to SAOP/CPO for all non-cyber low risk PII incidents.
- Provides a quarterly report to the SAOP/CPO detailing the status of each breach reported to the ESOC.

3.4 Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)

- Serves as Chair of the Task Force.
- Provides reports about Task Force actions to the Privacy Council, ensuring lessons learned are used to implement preventative actions.
- Convenes mandatory Task Force meetings when a breach constitutes a major incident and determines frequency of all other Task Force meetings.
- Holds a tabletop exercise annually with the Task Force in order to practice a coordinated response to a breach, further refine and validate the Plan, and identify potential weaknesses in the Department's response capabilities.
- Receives reports of all PII incidents at: cpo@doc.gov.
- Ensures effective execution of each breach response.
- Meets regularly with the Privacy Council to ensure effective execution of BOU level breach response.
- Provides closure concurrence for Moderate and High risk PII incident reports.
- Provides quarterly PII metrics.
- Maintains thorough records of PII incidents from the initial report through the completed response.
- Provides training to DOC employees and contractors regarding preparing for and the handling of PII breach response, as needed.
- Reviews the quarterly status report received from the ESOC and validates the reports accurately reflect the status of each reported breach.
- Reviews reports and determines appropriate action, such as developing new policy,



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

- updating existing policies, improving training and awareness, etc.
- Provides reporting to the Secretary, Deputy Secretary, and the Executive Management Team (EMT), as necessary.
- Develops training for individuals with access to Federal information and information systems on how to identify, report, and respond to a breach.
- Ensures routine uses are in all PA System of Records Notices (SORNs) for the disclosure of information necessary to respond to a breach either of the Department's PII or to assist another agency in its response to a breach.

3.5 DOC PII Breach Response Task Force

Consistent with the OMB guidance, the Task Force will consist of the following permanent members (or their designees):

- Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), Chair
- General Counsel (legal counsel)
- Chief Information Officer (CIO) or the CIO's designee
- Senior Agency Information Security Officer (SAISO) or the SAISO's designee
- Chief Financial Officer/Assistant Secretary for Administration
- Assistant Secretary for Legislative and Intergovernmental Affairs (OLIA) (legislative affairs official)
- Chief of Staff, Office of the Secretary
- Director, Office of Public Affairs (OPA) (communication official)
- Director, Office of Policy and Strategic Planning
- Director, Office of Human Resources Management
- Office of Security (OSY), Attends on an as needed basis
- Office of Inspector General (OIG), Advisory Role

Each member shall participate in Task Force meetings when convened by the SAOP/CPO and shall provide his/her expertise as needed to provide the best response and lessons learned for each incident. Decisions and recommendations are made by consensus. In addition, the Task Force members must participate in the tabletop exercise held annually.

The Bureau/Operating Unit (BOU) that initially reported an incident may be asked to attend a Task Force meeting to discuss the specific details of the incident, help to formulate an appropriate response, and assist in executing the breach response.

The Task Force, or a designated representative, may also work closely with other Federal agencies, offices, or teams to share lessons learned or help to develop government-wide guidance for handling PII incidents.

If a breach involves DOC employee PII, then the Task Force has the discretion to notify the relevant and affected senior management while the response is being developed and executed.

As Chair of the Task Force, the CPO shall provide reports to the Privacy Council, as appropriate.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



In order to effectively and efficiently respond to a breach, the breach response team may need to consult with the following personnel:

- Budget and procurement personnel who can provide expertise when a breach involves contractors or an acquisition, or who may help procure services such as computer forensics, cybersecurity experts, services, or call center support;
- Human resources personnel who may assist when employee misconduct results in a breach or when an employee is suspected of intentionally causing a breach or violating agency policy;
- Law enforcement personnel who may assist when a breach involves the violation or suspected violation of law or when a breach is the subject of a law enforcement investigation;
- Physical security personnel who may investigate a breach involving unauthorized physical access to a facility or when additional information regarding physical access to a facility is required; and,
- Other agency personnel who may be necessary according to specific agency missions, authorities, circumstances, and identified risks.

3.6 Office of the Chief Information Officer (OCIO)

- Provides information technology guidance in responding to suspected or known breaches, such as an evaluation of controls or computer forensics investigation and analysis.
- Working with the affected BOU, takes steps to control and contain the breach, such as:
 - Monitor, suspend, or terminate affected accounts;
 - Modify computer access or physical access controls; and
- Takes other necessary and appropriate action without undue delay and consistent with current requirements under FISMA.

3.7 Office of General Counsel (OGC)/Bureau Chief Counsel (BCC)

- Provides legal support and guidance in responding to a PII incident.
- Provides legal review of BII and PA incidents.

3.8 Office of Inspector General (OIG)

- Determines whether to notify the Department of Justice or other law enforcement authorities following a breach.
- Advises the Task Force about ongoing investigations and the timing of external notifications that may affect such investigations.

3.9 Office of Legislative and Intergovernmental Affairs (OLIA)

- Coordinates all communications and meetings with members of Congress and their staff when necessary.
- Ensures major incidents are reported to Congress within the established seven (7) days.



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

3.10 Privacy Council

- Receives reports about the actions of the Task Force.
- Analyzes reports from the Task Force to make recommendations for privacy policy changes.
- Approves changes to this Plan as recommended by the SAOP/CPO.

3.11 Office of Public Affairs (OPA)

- Coordinates notifications to individuals, the media, and other third parties as appropriate.

3.12 Supervisor/Manager

- Ensures compliance to Federal laws, rules, regulations, and Departmental privacy policy.
- Ensures employee/contractor completes training to properly safeguard information.
- Takes steps to prevent a breach from occurring (e.g., ensuring laptops are password protected and encrypted, and providing shredder for staff, etc.).
- Recognizes a privacy incident and upon discovery/detection, immediately reports a suspected or confirmed breach incident to the BCPO and BOU CIRT (NOTE: Supervisor/manager does not forward sensitive PII when reporting incident). Information to report verbally or by email includes:
 - Name
 - Contact information
 - Description of incident
 - Date, time, and place incident occurred
 - Type of media or device involved
 - Any controls enabled to mitigate loss
 - Number of individuals potentially affected
- Maintains or documents records of information and/or actions relevant to the incident.
- Provides advice, expertise, and assistance to the BCPO and/or BOU CIRT, as needed.
- Assists with the investigation and corrective/remedial actions, as needed.
- Ensures appropriate consequences for repeat offenders.

3.13 Employee/Contractor

- Adheres to Federal laws, rules, regulations, and Departmental privacy policy and is aware of the consequences for violating such directives.
- Successfully completes training regarding his/her respective responsibilities relative to safeguarding information.
- Takes steps to prevent a breach from occurring (e.g., encrypting sensitive PII in emails and on mobile computers, media, and devices, destroying paper containing sensitive PII, and locking computer system when leaving it unattended, etc.).
- Recognizes a privacy incident and upon discovery/detection, immediately reports a suspected or confirmed breach incident to his/her supervisor, BCPO, and BOU CIRT

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



(NOTE: Employee/contractor does not forward sensitive PII when reporting incident).
Information to report verbally or by email includes:

- Name
- Contact information
- Description of incident
- Date, time, and place incident occurred
- Type of media or device involved
- Any controls enabled to mitigate loss
- Number of individuals potentially affected
- Maintains or documents records of information and/or actions relevant to the incident.
- Completes corrective/remedial actions, if appropriate.

4.0 DOC PII/BII/PA Incident Response Process

(See [Appendix D](#) for process flowchart)

- A) DOC employee or contractor suspects or becomes aware of a PII/BII/PA incident.
- B) DOC employee or contractor reports the incident immediately to his/her BCPO/BOU CIRT⁷ **AND** to his/her immediate supervisor.
- C) The BCPO/BOU CIRT reports the PII incident to the SAOP/CPO and ESOC within one (1) hour of discovery/detection. Simultaneously the following occurs:
 - 1) The BCPO and BOU CIRT continue to investigate the incident.
 - 2) The BCPO/BOU CIRT determines if the incident is a BII or PA incident.
 - i. If the incident is a BII or PA incident which DOES NOT contain PII
 - (1) BCPO/BOU CIRT turns over the PA incident without PII to the BCC for investigation and consults with the BCC as appropriate on BII incidents without PII to determine if a Trade Secrets Act violation occurred.
 - (2) BCPO/BOU CIRT documents date of referral to BCC for investigation and closes PII portion of the incident.
 - ii. If the incident is BII or PA incident and DOES contain PII
 - (1) BCPO/BOU CIRT continues with PII incident processing **AND**

⁷ Some BOUs report directly to the ESOC (See Appendix E for additional information).



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

- (2) BCPO/BOU CIRT notifies the BCC of the BII/PA aspects of the incident and follows BCC instructions to close BII/PA portion of the incident while proceeding with the PII incident response in parallel.
 - 3) The BCPO uses [Appendix B](#) Risk Level Evaluation Matrix to assign an initial risk of harm rating for the PII incident.
 - 4) The BCPO/BOU CIRT notifies the Property Management Office, OIG, and/or law enforcement, if applicable.
 - 5) The BCPO/BOU CIRT documents planned and completed corrective/remedial actions.
 - 6) The BCPO/BOU CIRT provides a report of the results of the investigation to the SAOP/CPO and the ESOC within 48 hours of initial incident reporting.
 - i. If an incident is handled directly by the ESOC, then the ESOC shall provide the report to the SAOP/CPO.
 - ii. Low risk of harm rated incidents may be closed by the BCPO only after fully documenting the incident in accordance with [Appendix A](#) of this plan and updating the incident report with confirmation that corrective/remedial actions have been completed.
 - iii. Moderate and High risk of harm rated incidents require SAOP/CPO concurrence for closure.
 - iv. All major incidents require SAOP/CPO concurrence for closure.
- D) When reviewing privacy compliance documentation in response to a breach, the SAOP considers the following:
- 1) Which SORNs, PIAs, and privacy notices apply to the potentially compromised information.
 - 2) If PII maintained as part of a system of records needs to be disclosed as part of the breach response, is the disclosure permissible under the Privacy Act and how the Department will account for the disclosure.
 - 3) If additional PII is necessary to contact or verify the identity of individuals potentially affected by the breach, will new or revised SORNs or PIAs be required.
 - 4) Whether all relevant SORNs, PIAs, and privacy notices are accurate and up-to-date.
- E) When determining the potential information sharing that may be required in response to a breach, the SAOP considers the following:
- 1) Is the information sharing consistent with existing agreements;
 - 2) How the PII is transmitted, protected, and retained during this phase; and
 - 3) If the information may be shared with third parties.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



- F) The SAOP/CPO determines whether to convene a meeting of the Task Force for Moderate and High Risk of harm and Major incidents based on several factors, including:
- Risk and type of harm to the affected individuals and/or the DOC
 - Whether the acts leading to the breach were intentional or accidental
 - Number of affected individuals
 - Security controls applied to the affected PII
 - Other factors enumerated in the section entitled “Risk of Harm Analysis Factors and Rating Assignment”
 - Any other basis on which the SAOP/CPO believes the incident warrants attention of the Task Force
- 1) If the SAOP/CPO determines that the Task Force needs to be convened
- i. The BCPO builds a Privacy Task Force Package in coordination with the SAOP/CPO. The Privacy Task Force Package includes:
 - PII summary of incident
 - Notification letter
 - OPA talking points
 - Additional documents as requested
 - ii. The Task Force concurs, modifies, and/or approves corrective/remedial actions to be taken.
 - iii. The BCPO/BOU CIRT confirms and documents completion of corrective/remedial actions directed by the Task Force in close coordination with the SAOP/CPO and submits a request for closure.
 - iv. The SAOP/CPO follows up to ensure that the breach response is carried out effectively and approves closure request.
 - v. The BCPO/BOU CIRT notifies ESOC to close incident.
- 2) If the SAOP/CPO determines that the Task Force DOES NOT need to be convened
- i. The BCPO/BOU CIRT confirms and documents completion of corrective/remedial actions and submits a request for closure to the SAOP/CPO at CPO@doc.gov.
 - ii. The SAOP/CPO follows up to ensure that the breach response is carried out effectively and approves closure request.
 - iii. The BCPO/BOU CIRT notifies ESOC to close incident.

5.0 Risk of Harm Analysis Factors and Rating Assignment

Based on the risk of potential harm and other factors provided in this section, the BCPO shall assign an initial rating level of the risk of harm Low, Moderate, or High for each



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

reported PII incident. The rating level of the risk of harm will be used to assist the SAOP/CPO in making a determination as to whether the Task Force should be convened. The analysis and risk rating should be used by the Task Force to determine the appropriate response.

In assessing the risk of harm, it is important to consider all potential harm to both the affected individuals and the Department.

Potential harm to the individual may include, but is not limited to:

- Identity theft
- Blackmail
- Embarrassment
- Physical harm
- Discrimination
- Emotional distress
- Inappropriate denial of benefits

Potential harm to the Department may include, but is not limited to:

- Administrative burden
- Cost of remediation
- Loss of public trust
- Legal liability

Additional factors the SAOP considers for determining the rating level for the risk of harm include:⁸

- Security controls in place at the time of the breach.
- Type of breach and evaluation of each data element as well as evaluation of the sensitivity of all the data elements combined.
- Number of individuals affected by the breach.
- Sensitivity of the PII and the context in which it was used.
- Likelihood the information is accessible and usable which includes:
 - **Security safeguards** for whether the PII was properly encrypted or rendered partially or completely inaccessible by other means;
 - **Format and media** if the format of the PII makes it difficult and resource-intensive to use;
 - **Duration of exposure** to find out how long the PII was exposed; and
 - **Evidence of misuse** to indicate or confirm that the PII is being misused or never accessed.
- Likelihood that the breach may lead to harm.

⁸ See NIST SP 800-122, [Guide to Protecting the Confidentiality of PII \(Section 3\)](#) for additional information about assessing the impact level for a particular collection of PII.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



- Specific legal obligations to protect the PII or report its loss.
- Whether the acts leading to the breach were intentional or accidental.
- The extent to which the PII identifies or disproportionately impacts a vulnerable population (e.g., children, senior citizens, active duty military, confidential informants, individuals with disabilities, victims, or other populations considered vulnerable).
- The permanence of the breach including the continued relevance and utility of the PII over time and whether it is easily replaced or substituted.

6.0 Breach Notification and Remediation

The appropriate response to a breach of PII may include notification to the affected individuals or third parties, as well as specific corrective/remedial actions. The SAOP/CPO (and/or Task Force, if convened) shall recommend a response plan to mitigate risks to the individual and the Department. The SAOP/CPO and/or Task Force should consider the options available to protect potential victims of identity theft and other harm.

Options may include:

- Providing notice of the breach to affected individuals.
- Engaging a third party to conduct a data breach analysis to determine whether a particular data loss appears to be resulting in identity theft.
- Providing credit monitoring services.⁹
- Referring individuals to websites providing guidance about ID Theft, such as the [Federal Trade Commission Consumer Information](#) site.
- Providing a toll-free hotline or website for affected individuals to obtain additional information.

6.1 Notifying Individuals

The SAOP/CPO (and/or Task Force, if convened) shall determine whether individuals should be notified based on the rating level of the risk of harm, as well as the analysis leading to the assigned rating level. The OIG shall notify the SAOP/CPO and/or Task Force and request a delay if notice to individuals or third parties would compromise an ongoing law enforcement investigation. Unless notification to individuals is delayed or barred for law enforcement or national security reasons, the notice should be provided within 30 days or as expeditiously as practicable and without unreasonable delay.

⁹ If a decision is made to retain monitoring services, the SAOP/CPO and/or Task Force should consult the OMB Memorandum M-07-04, [Use of Commercial Credit Monitoring Services Blanket Purchase Agreements](#), (December 22, 2006).

Department of Commerce PII, BII, and PA Breach Response and Notification Plan

The SAOP/CPO and/or Task Force shall consider the following elements in the notification process:

- Timing of the notice
- Source of the notice
- Contents of the notice
- Method of notification
- Special Considerations
- Preparation for follow-on inquiries

The contents of the notice to individuals shall include:

- A brief description of what happened, including the date(s) of the breach and of its discovery.
- To the extent possible, a description of the types of information involved in the breach.
- A statement of whether the information was encrypted or protected by other means, when it is determined that disclosing such information would be beneficial to the potentially affected individuals and would not compromise the security of the information system.
- A brief description of what the Department is doing to investigate the breach, mitigate losses, and protect against further breaches.
- Contact information for individuals who have questions or need more information, such as a toll-free number, website, or postal address.
- Steps for individuals to undertake in order to protect themselves from the risk of ID theft.
- Information about how to take advantage of credit monitoring or other service(s) that the Department or BOU intends to offer.
- The signature of the relevant senior Department management official (Head of Operating Unit or Secretarial Officer).

6.2 Method of Notification

The SAOP/CPO will determine the method of notification to the potentially affected individuals. The best method for providing notification will be dependent upon the number of individuals affected, available contact information for the potentially affected individuals, and the urgency in which the individuals need to receive the notification. Notification should be provided by:

- First-Class Mail
- Telephone
- Email¹⁰

¹⁰ While email notification may be appropriate, it is not recommended as the primary form of notification.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



- Substitute Notification

6.3 Notification/Reporting Requirements

The SAOP/CPO (and/or Task Force, if convened) shall determine whether notification to any third parties is necessary. Potential third parties may include:

- **Law Enforcement** Local law enforcement or Federal Protective Services; the IG may notify the FBI.
- **Media and the Public** The Director of the Office of Public Affairs, in coordination with the SAOP/CPO and/or Task Force and the affected Bureau public affairs staff, will be responsible for directing all communications with the news media and public. This includes the issuance of press releases and related materials on www.commerce.gov or a BOU website.
- **Financial Institutions** If the breach involves government-authorized credit cards, the DOC must notify the issuing bank promptly.¹¹ The SAOP/CPO and/or Task Force shall coordinate with the Department's Acquisitions Branch regarding such notification and suspension of the account.
- **Appropriate Members of Congress** The Assistant Secretary for Legislative and Intergovernmental Affairs, in consultation with the Task Force, shall be responsible to coordinate all communications and meetings with members of Congress and their staff.
- **Attorney General/Department of Justice** The Inspector General shall determine when to contact the Attorney General.
- **Others** – The SAOP/CPO and/or Task Force shall have the discretion to determine if any additional third parties should be notified.

7.0 Consequences

Employees are expected to familiarize themselves with their responsibilities with respect to the protection of PII, as well as their responsibilities in the event of a breach. Likewise, managers and supervisors should ensure that their employees have access to adequate training with respect to these responsibilities.

Failure to adhere to the requirements of this Plan may result in administrative or disciplinary action, up to and including removal from the Federal service.

¹¹ OMB M-07-16 requires bank notification in the event that PII related to government-authorized credit cards is involved in a breach.



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Appendix A – DOC PII Incident Report Content

The Department requires that the following elements be included in a PII Incident Report:

- Incident number
- Contact Person and Phone number
 - Breach reported by
 - Contact information
 - B/OU
 - Email
 - Phone Number
- Incident date/time
- Major Incident (Yes/No)
- Contractor System (Yes/No)
- Date/Time Reported to BOU-CIRT
- Date/Time Reported to US-CERT
- Date/Time Reported to Law Enforcement
- Repeat Offender (Yes/No) If Yes, include 2nd, 3rd offense
- Region
- Status (Open/Closed)
- Follow-up within 48 Hours (Yes/No)
- Summary of Circumstances Summarize the facts or circumstances of the theft, loss, or compromise of PII as currently known, including:
 - A description of the parties involved in the breach;
 - The physical or electronic storage location of the information at risk;
 - If steps were immediately taken to contain the breach;
 - Whether the breach is an isolated occurrence or a systematic problem;
 - Who conducted the investigations of the breach, if applicable; and
 - Any other pertinent information.
- Type(s) of PII Disclosed or Compromised (e.g., SSN, truncated or partial SSN, DOB, address, driver's license number, passport number, or credit card)
 - Lost information or equipment, (e.g., laptop or table, desktop, smartphone, external storage devices, or paper files).
 - Stolen information or equipment, (e.g., laptop or table, desktop, smartphone, external storage devices, or paper files).
 - Unauthorized equipment (e.g., using an unauthorized personal device server or email account to store PII).
 - Unauthorized disclosure (e.g., email sent to incorrect address, oral or written disclosure to unauthorized person, or disclosing documents publicly with sensitive information not redacted).
 - Unauthorized access (e.g., an unauthorized employee or contractor access information or an information system).
 - Unauthorized use (e.g., employee with agency-authorized access to database or

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



file access and uses information for personal purposes rather than for official purposes).

- Storage Medium (e.g., unencrypted, email, or unsecure website)
- Controls Enabled- Password Protection and/or Encryption
- Number of Individuals Affected (internal or external to DOC)
- FISMA System ID Number(s)
- Identify Relevant Specific PIA or SORNs
- BII or Privacy Act Violation (BII/PA/No)
- Risk Assessment and Employee Making Assessment
- Corrective and Remedial Actions (include status e.g., pending, confirmed)

Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Appendix B – Risk Level Evaluation Matrix

In analyzing a PII incident, the BCPO must consider the following six (6) critical risk of harm factors:

- The nature of the data compromised, level of risk in light of the context of the data, and broad range of potential harm that may result from disclosure;
- Whether the incident occurred during the performance of an official “Commerce work related activity”;
- The likelihood that the PII will be or has been used in an unauthorized manner;
- DOC’s ability to mitigate the risk of harm to affected individuals;
- The likelihood that the breach may lead to harm (e.g., mental or emotional distress, financial harm, embarrassment, harassment or identity theft); and
- The number of individuals affected by the breach.

To address the first of the six (6) critical factors, the BCPO must evaluate whether the type of breached PII data elements constitute the type of information that may pose a risk of identity theft and whether a significant and immediate identity theft risk exists. Examples of data which present an identity theft risk include: (1) SSN, including truncated form; (2) date of birth, place of birth, or mother’s maiden name; (3) passport number, financial account number, credit card number, medical information, or biometric information; (4) potentially sensitive employment information (e.g., personnel ratings, disciplinary actions, and results of background investigations) and criminal history; or (5) any information that may stigmatize or adversely affect an individual. If there is a significant and immediate risk of identity theft, the BCPO must immediately contact the Commerce SAOP/CPO who will determine whether to convene the Privacy Task Force and advise on how to proceed. If no significant and immediate risk of identity theft is implicated, the BCPO will use the Commerce Risk Level Evaluation Matrix to assess the five (5) remaining factors and assign an initial incident risk of harm rating.

Using the Risk Level Evaluation Matrix:

Step 1: From left to right, select the first “Breach Category” section of the Matrix that describes the general fact pattern of the incident.

Step 2: Then, from top to bottom, use the detailed facts of the incident to determine the appropriate response (Y/N/NDF) for each evaluation statement of the Matrix until all answers are documented. NOTE: Y (Yes); N (No); and NDF (Not Determining Factor)

Step 3: Finally, use the “Recommended Initial Risk Rating” row of the appropriate “Breach Category” with Y/N/NDF selections that match those of the incident to determine the risk of harm rating.

The risk of harm rating may be adjusted by the BPO to a higher rating as appropriate to reflect a unique mission impact. However, Commerce CPO concurrence is required prior to lowering an initial risk of harm rating. If PII was encrypted, the incident may be rated a Low risk of harm.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



Risk Level Evaluation Matrix

Critical Factors	Evaluation Statement	Breach Category																				Automatic Moderate Trigger	Automatic High Trigger
		PII Incidents Resulting for PII Owner Action and/or Personal Use						All Recipients Have Valid Need to Know and are Authorized to						All Recipients are Authorized, However One or More Recipient Does NOT have a Need to Know									
Association with an Official Duty	Sent by PII Owner and/or PII Owner is Sender's Family Member	Y	Y	N	N	N	Y														All Incidents with One or More Recipients NOT Authorized	All Incidents with One or More Recipients NOT Authorized Affecting Greater than 2500 Individuals	
	Personal Use (excludes Official Commerce Business)	Y	N	Y	Y	Y	N																
Likelihood PII will be used in Unauthorized Manner	Recipients have Need to Know	NDF	NDF	Y	N	NDF	NDF	YES						NO									
	Recipients are Authorized	NDF	Y	Y	Y	N	N	YES						YES									
Ability to Mitigate Risk of Harm	Exposed Only to DOC Personnel	NDF	Y	NDF	Y	NDF	NDF	Y	N	Y	Y	Y	N	N	Y	N	Y	Y	Y	N			N
	Exposed on Internet, non DOC system, or public/non DOC controlled facility	NDF	NDF	NDF	NDF	NDF	NDF	N	N	N	N	Y	Y	Y	N	N	N	N	Y	Y			Y
Likelihood Incident may lead to Harm	Quantity of PII (# of exposed fields of PII per person)	NDF	NDF	<10	<5	NDF	NDF	<10	>10	NDF	>10	NDF	NDF	<10	<5	>5	<5	>5	NDF	NDF	>3		
	# of Individuals Affected	NDF	NDF	<500	<250	NDF	NDF	<500	NDF	>500	NDF	>500	<500	NDF	<250	<250	>250	<250	>250	>100	NDF		
	Recommended Initial Risk Rating	LOW	LOW	LOW	LOW	MOD	MOD	LOW	LOW	MOD	MOD	MOD	MOD	MOD	LOW	LOW	MOD	MOD	MOD	MOD	MOD	MOD	HIGH

NOTE: If PII was encrypted, the incident may be rated a "Low" risk of harm.
 Y Yes
 N No
 NDF Not Determining Factor



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Examples: How to Use Risk Level Evaluation Matrix

Scenario 1: Resulting from PII Owner Action and/or Personal Use

John Doe, DOC employee, faxed his Form 1040 to the Loan Department at Capitol One Bank without notifying his loan officer to expect the document. Approximately four hours later, the loan officer informed John that he received the form from a contractor who was repairing the shredder in the bank. John was concerned that his identity had the potential of being compromised and notified his supervisor who reported the incident to his bureau CIRT since a DOC fax machine was used.

Analysis:

- Fax sent by PII owner (Y)
- Faxed document for personal use (Y)
- First recipient had need to know (NDF)
- First recipient authorized to receive information (NDF)
- Fax exposed only to DOC personnel (NDF)
- Fax exposed on Internet, non-DOC system, or public/non-DOC controlled facility (NDF)
- Quantity of PII (NDF)
- Number of individuals affected (NDF)

Rating: Low Risk

Scenario 2: Valid Need to Know and Authorized User

A supervisory payroll specialist sent an unencrypted email with attachments to a payroll specialist in the same division to ensure notification letters were sent to certain employees. The attachments contained information regarding child support payments which included sensitive PII (SSN, DOB) of 20 DOC employees.

Analysis:

- Recipient had need to know (Y)
- Recipient authorized to receive information (Y)
- Email exposed only to DOC personnel (Y)
- Email exposed on Internet, non-DOC system, or public/non-DOC controlled facility (N)
- Quantity of PII (<10)
- Number of individuals affected (<500)

Rating: Low Risk

Department of Commerce

Privacy Breach Notification Plan



Scenario 3: Authorized User, but One or More Recipients has no Need to Know

25 supervisors in the Los Angeles Field Office were granted access to the electronic Employee Relations files of 200 employees located in the Denver Field Office. These files contained sensitive PII (SSN, DOB, medical information, performance ratings, performance grievances, and disciplinary actions).

Analysis:

- Recipients had need to know (N)
- Recipients authorized to receive information (Y)
- Exposed only to DOC personnel (Y)
- Exposed on Internet, non-DOC system, or public/non-DOC controlled facility (N)
- Quantity of PII (>5)
- Number of individuals affected (<250)

Rating: Moderate Risk

Scenario 4: Not Authorized, Greater than 10 PII Fields, and Affecting More than 2500 Individuals

An employee incorrectly mailed Standard Form (SF)-85P, Questionnaire for Public Trust Positions, to 10 survey respondents, rather than to employees at the U.S. Office of Personnel Management. Each SF-85P contained SSN, DOB, POB, mother's maiden name, passport number, alien registration number, reason employment ended, police record, illegal drug activity, financial record, and delinquency on loans or financial obligations. 2,842 employees were affected.

Analysis:

- Recipients had need to know (N)
- Recipients authorized to receive information (N)
- Exposed only to DOC personnel (N)
- Exposed on Internet, non-DOC system, or public/non-DOC controlled facility (Y)
- Quantity of PII (>10)
- Number of individuals affected (>2500)

Rating: High Risk



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Appendix C – Delegation of Authority Memorandum

Bureau Chief Privacy Officer (BCPO) Delegation of Authority Memorandum

MEMORANDUM FOR: *(Insert name of current SAOP/CPO)*
Senior Agency Official for Privacy/Chief Privacy Officer

FROM:
(Name of bureau) Bureau Chief Privacy Officer

SUBJECT: Delegation of Privacy Breach Authority for Bureau Chief Privacy Officer

In accordance with the Department of Commerce (DOC) PII, BII, and PA Breach Response and Notification Plan, I hereby appoint *(insert name of employee)* to act on behalf of the Bureau Chief Privacy Officer (BCPO) for privacy breaches. The employee identified above is qualified to manage the daily operations for privacy breaches and hereby delegated authority to *(check all that apply)*:

- Evaluate all Bureau/Operating Unit PII incidents in accordance with the Risk Level Evaluation Matrix and assign a risk of harm rating
- Ensure all Bureau/Operating Unit PII incidents are under investigation within 48 hours of the incident discovery/detection and a follow-up report has been submitted to the SAOP/CPO and ESOC
- Maintain thorough records of Bureau/Operating Unit PII incidents from the initial report through the completed response
- Ensure Bureau/Operating Unit CIRT has documented completion of all appropriate corrective/remedial actions in the incident report prior to close-out of the PII incident
- Close Low risk incidents and send closure concurrence requests for Moderate and High risk PII incidents to the SAOP/CPO

The delegation may be terminated at any time by written notice by the BCPO.

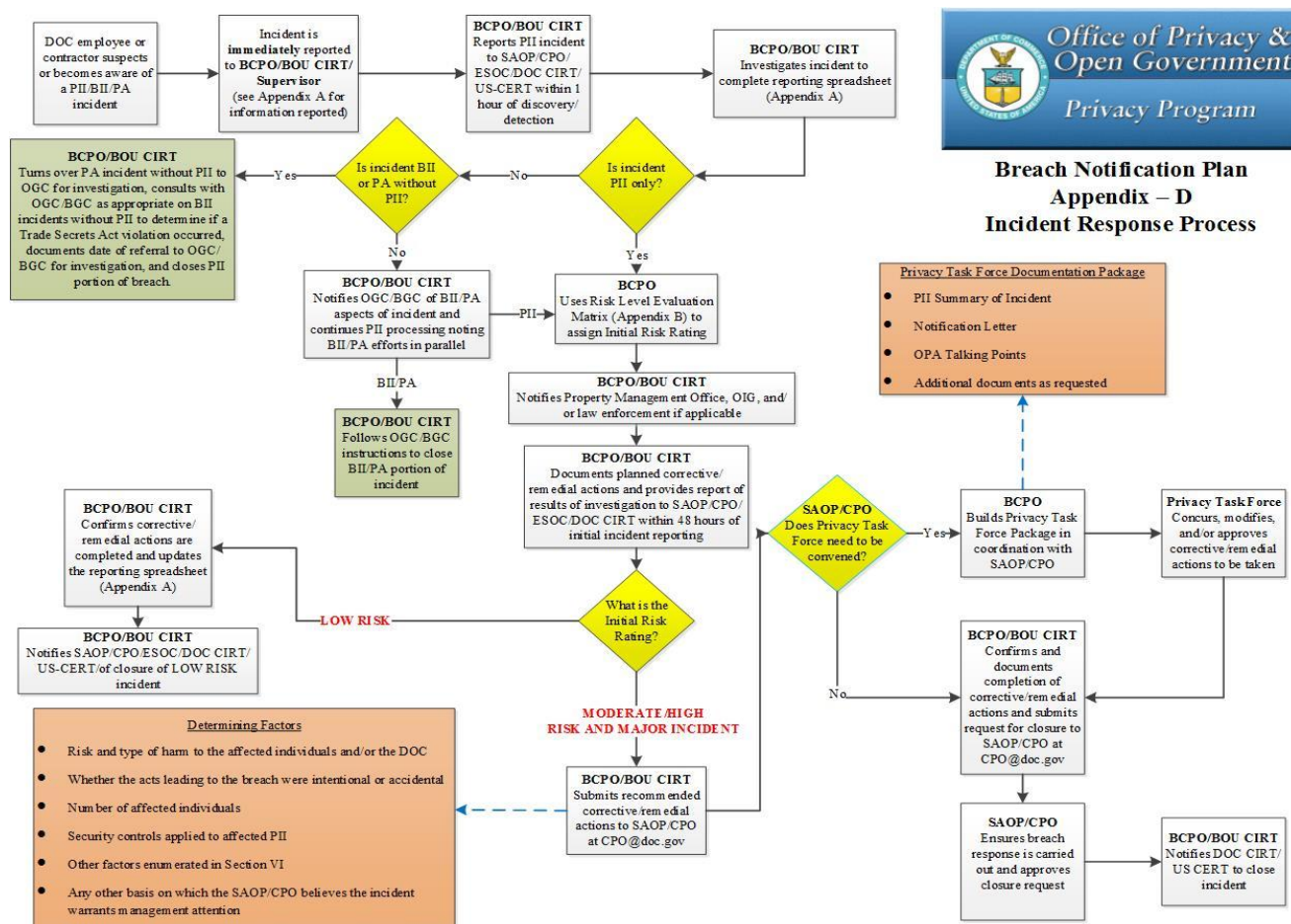
EMPLOYEE SIGNATURE

[Employee signature indicates that he/she has read, understands, and agrees to comply with the BCPO role and responsibilities.]

Department of Commerce PII, BII, and PA Breach Notification Plan



Appendix D Flowchart





Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Appendix E – Senior Agency Official for Privacy/Chief Privacy Officer and Commerce Operating Unit CIRT Reporting Offices

The ESOC and Bureau CIRTs shall report PII incidents directly to the SAOP/CPO.

- **Senior Agency Official for Privacy/Chief Privacy Officer (SAOP/CPO)**
 - cpo@doc.gov
 - (202) 482-1190, for immediate assistance only

- **Enterprise Security Operations Center (ESOC)**
 - ESOC@doc.gov
 - (202) 482-4000
 - <https://connection.commerce.gov/overview/about-doc-cirt>

PII incidents occurring in EDA, ESA, MBDA, NTIA, OIG, and OS shall be reported directly to ESOC.

- **Bureau of Economic Analysis (BEA) CIRT**
 - helpdesk@bea.gov
 - (301) 278-9407

- **Bureau of Industry and Security (BIS) IT Security**
 - BISITSecurity@bis.doc.gov
 - (202) 482-0623 or (202) 482-1188

- **Bureau of the Census (BOC) CIRT**
 - boc.cirt@census.gov
 - (301) 763-3333 or (877) 343-2010 (after hours)

- **International Trade Administration (ITA) CIRT**
 - CSC@trade.gov
 - (202) 482-1955 or (877) 206-0645 (toll free)

- **National Institute of Standards and Technology (NIST) CIRT**
 - itac@nist.gov
 - (301) 975-5375 (Gaithersburg, MD); (303) 497-5375 (Boulder, CO)

- **National Oceanic and Atmospheric Administration (NOAA) CIRT**
 - ncirt@noaa.gov
 - (301) 713-9111

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



- **National Technical Information Service (NTIS) CIRT**
 - secops@ntis.gov
 - (703) 605-6519

- **U.S. Patent and Trademark Office (USPTO) CIRT**
 - CyberSecurityInvestigations@uspto.gov
 - (571) 272-6700



U.S. Department of Commerce
Personally Identifiable Information (PII),
Business Identifiable Information (BII)
and Privacy Act (PA)
Breach Response and Notification Plan

Published July 2017

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Tuesday, February 6, 2018 1:48 PM
To: Mark Graff NOAA Federal
Cc: Tahir Ismail; Mark Deforest; _NMFS InfoSec
Subject: NOAA4100 PTA for review and signature.
Attachments: NOAA4100_PTA_20180206_Ver1.1_kdr (1).pdf

Mark, this is a system that's using Clearwell.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Purvis, Catrina (Federal)

Subject: Privacy Council Face to Face Meeting
Location: Rooms 12015/12017 HCHB

Start: Tuesday, February 6, 2018 8:30 AM
End: Tuesday, February 6, 2018 12:30 PM

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Purvis, Catrina (Federal)

Attachments: Privacy Council F 2 F Agenda 02 06 18.docx; CD 15 Transmittal and Routing Form.pdf; Digital Privacy Report Template.pdf; DIGITAL PRIVACY REPORT.docx; Federal Privacy Updates.docx; GDPR Background 11 17.docx; Guide to Conducting a PII Breach Table Top Exercise.docx; Identity Protection Services from GSA.docx; OMB Memo 16 14 (Identity Protection Services).pdf; SSN Collection and Mailing (002).docx; Upcoming Data Call.docx; The Annual Compliance Review Processes.docx

Sending more documents

Sending attachments

Due to the weather conditions expected tomorrow morning, the Privacy Council meeting is being rescheduled from Tuesday, January 30, 2018, to Tuesday, February 6, 2018, from 8:30 a.m. to 12:30 p.m.

If the Bureau Chief Privacy Officer cannot participate in this meeting, please ensure your bureau/operating unit has representation with the authority to make decisions on your bureau's/operating unit's behalf.

Below is the WebEx Conference/Telecom information for this meeting:

Meeting Number: (b)(6)
Meeting Host: Tahira Murphy

Join instructions for Instant Net Conference:








1. Join the meeting now: **Error! Hyperlink reference not valid.**
2. Enter the required fields
3. Indicate that you have read the Privacy Policy
4. Click on Proceed

Privacy Council Telecom Dial In: (b)(6)
Participant Passcode: (b)(6)






FORM CD-15 (12 6 73) PRESCR. BY TRANSMIT/ROUTE DAO 214 2		U.S. DEPARTMENT OF COMMERCE		DATE 01/24/2018																
NAME	BUILDING, ROOM OR REFERENCE NO.	TAKE ACTION BELOW	INITIALS AND DATE																	
Catrina Purvis	Rm. 52012R	2																		
Lisa Casias	Rm. 58032R	1																		
ACTION ITEMS																				
<table border="0"> <tr> <td>1. APPROVAL/SIGNATURE</td> <td>9. YOUR INFORMATION</td> </tr> <tr> <td>2. CLEARANCE/INITIALS</td> <td>10. PER OUR CONVERSATION</td> </tr> <tr> <td>3. RECOMMENDATION OR COMMENT</td> <td>11. AS REQUESTED</td> </tr> <tr> <td>4. RETURN WITH MORE DETAILS</td> <td>12. NECESSARY ACTION</td> </tr> <tr> <td>5. INVESTIGATE AND REPORT</td> <td>13. CIRCULATE AMONG STAFF</td> </tr> <tr> <td>6. NOTE AND SEE ME</td> <td>14. ANSWER DIRECTLY</td> </tr> <tr> <td>7. NOTE AND RETURN</td> <td>15. PREPARE REPLY FOR SIGNATURE</td> </tr> <tr> <td>8. NOTE AND FILE</td> <td></td> </tr> </table> <p style="text-align: right;">OF: _____</p>					1. APPROVAL/SIGNATURE	9. YOUR INFORMATION	2. CLEARANCE/INITIALS	10. PER OUR CONVERSATION	3. RECOMMENDATION OR COMMENT	11. AS REQUESTED	4. RETURN WITH MORE DETAILS	12. NECESSARY ACTION	5. INVESTIGATE AND REPORT	13. CIRCULATE AMONG STAFF	6. NOTE AND SEE ME	14. ANSWER DIRECTLY	7. NOTE AND RETURN	15. PREPARE REPLY FOR SIGNATURE	8. NOTE AND FILE	
1. APPROVAL/SIGNATURE	9. YOUR INFORMATION																			
2. CLEARANCE/INITIALS	10. PER OUR CONVERSATION																			
3. RECOMMENDATION OR COMMENT	11. AS REQUESTED																			
4. RETURN WITH MORE DETAILS	12. NECESSARY ACTION																			
5. INVESTIGATE AND REPORT	13. CIRCULATE AMONG STAFF																			
6. NOTE AND SEE ME	14. ANSWER DIRECTLY																			
7. NOTE AND RETURN	15. PREPARE REPLY FOR SIGNATURE																			
8. NOTE AND FILE																				
COMMENTS																				
<p>One "Certificate of Appreciation" and four "Certificates of Recognition" to be presented at the Privacy Council meeting on January 30, 2018.</p>																				
<input type="checkbox"/> <i>Continued on reverse</i>																				
FROM (Name)	BUILDING, ROOM OR REF. NO.	CODE AND EXTENSION																		
Lisa Martin	Rm. 52010	x2459																		

Comments (*continued*)









**Policies for Federal Agency Public Websites and Digital Services
OMB MEMO-17-06 - Data Call**

OMB 17-06 Citing	OPOG's Initial Assessment	B/OU's Response	Target for Improvement	Completion Date Given	Analysis Status	Analysis Symbol	Date	
SECTION 6.A PRIVACY PROGRAM PAGE								
Section 6.A	Does your B/OU have a central Privacy Program page? Note: This is not referencing the Privacy Policy page in the footer of the website. Example: www.commerce.gov/privacy	No https://www.XXX.doc.gov/privacy does not work	No, the page renders the XXX Privacy Policy Statement rather than a home page.	Update to point to the Privacy Policy Page. Will point it to the Privacy Program page when it is completed.	7/28/2017	Points to Digital Privacy Policy Page (DPP) https://www.XXX.doc.gov/Privacy		12/22/2017
	If so, is the Privacy page accessible in the "About" Page? (Example: https://www.commerce.gov/about)	No. If XXX will maintain its own Privacy Program page, it needs to be accessible from their About page.	There is no page only a statement	Will develop a privacy home page to link from the "About" page.	7/28/2017	Points to Privacy Policy Program (PPP) page https://www.XXX.doc.gov/XXX/privacy-policy-program		1/10/2018
	Does the website have a Privacy Policy and/or Digital Policy Page? If so, is it accessible throughout the website? (Example: http://www.osce.doc.gov/opog/privacy/digital-policy.html)	Yes, at the bottom of each page is a link. However, the page does not link to any privacy related information https://www.XXX.doc.gov/index.php/p/27 about XXX/174 XXX privacy policy statement.	This page is not working from the home page. It works from other pages on the site.	A new compliant Privacy Policy page will be developed. (Possible consideration: will reference the Departments Digital Policy)	7/28/2017	Points to Digital Privacy Policy Page https://www.XXX.doc.gov/Privacy		1/10/2018
Section 6.A.1.a	Does the website list and provide links to complete, up to date versions of your B/OU's SORNs? (Example: http://www.osce.doc.gov/opog/PrivacyAct/PrivacyAct_SORNs.html)	Unable to determine.	XXX only has 1 SORN. It is not in HTML. A pdf file will appear when the SORN link is selected from the website footer.	XXX has an existing Link to its SORN through the website footer. (May move to privacy home page).	7/28/2017	Link to SORN exists on the footer, DPP, and PPP http://www.osce.doc.gov/opog/PrivacyAct/SORNs/XXX_1.html . Needs to consistent with the link used on the PPP.		1/10/2018
	Does the website provide citations and links to all Federal Register notices that comprise the SORN for each system of records? (Example: http://www.osce.doc.gov/opog/PrivacyAct/SORNs/pat_tm_23.html)	Unable to determine.	The SORN that is being rendered is a PDF of the SORN in the Federal Register. Unsure what citations and notices are required or related.	Decide what SORN specific FR notices need to be included and provide links to them.	7/28/2017	Needs to consistent with the link used on the PPP.		1/10/2018
	For any SORNs that are comprised of multiple Federal Register notices, does the website provide a link to the unofficial consolidated versions of the SORNs that describe the current system of records and allow members of the public to view the SORN in its entirety in a single location?	Unable to determine.	Do not know what citations and notices are relevant, but the full SORN as documented in the Federal Register would be displayed.	If there are any relevant citations and notices, include them and provide links to them.	7/28/2017	Needs to consistent with the link used on the PPP.		1/10/2018
Section 6.A.1.b	Does the website list and provide links to PIAs or compelling justification to decline to post a link to a PIA? Does the B/OU's PIA webpage link to OPOG's website? (Example: http://www.osce.doc.gov/opog/privacy/compliance.html#approvedpias)	Unable to determine.	PIAs are not easily found. A PIA search was conducted on the site and found the XXX PIA document.	A Post and link to PIAs from Privacy Home page will be created.	7/28/2017	Yes, The PIA links, on the PPP, point to the PIA on the DOC/Privacy Page.		1/10/2018





Policies for Federal Agency Public Websites and Digital Services
OMB MEMO-17-06 - Data Call

OMB 17-06 Citing	OPOG's Initial Assessment	B/OU's Response	Target for Improvement	Completion Date Given	Analysis Status	Analysis Symbol	Date
Section 6.A.1.c	Does the website list and provide links to matching notices and agreements for all active matching programs in which the B/OU participates?	B/OU reported there are no matching notices or agreements.	Do not know what citations and notices are relevant.	N/A	N/A	N/A	1/10/2018
Section 6.A.1.d	Does the website have any exemptions to the Privacy Act? If yes, are the citations and links to the final rules published in the Federal Register on the B/OU website?	Did not see any exemptions to the Privacy Act.	Exemptions are listed in the SORN and applicable PIA.	Exemptions are listed in the SORN which is accessible from the website. (May need to be move to a website page)	N/A	Yes, the exemptions are listed on the PPP and points to GPO https://www.gpo.gov/fdsys/pkg/USCODE2015title5/html/USCODE2015title5part1chap5subchapIIsec552.htm .	 1/10/2018
Section 6.A.1.c	Does the website list and provide links to Privacy Act implementation rules promulgated pursuant to 5 U.S.C. § 552a(f)? (Example: http://www.osce.doc.gov/opog/PrivacyAct/PrivacyAct.html)	Unable to determine.	Exists in the SORN	Include Privacy Act implementation rules on the new Privacy Policy Page.	7/28/2017	Yes, Privacy act implementation rules are on the PPP.	 1/10/2018
Section 6.A.1.f	Does the website list and provide links to publicly available agency policies on privacy, including any directives, instructions, handbooks, manuals, or other guidance? If not, please link to OPOG's policy page. (Example: http://www.osce.doc.gov/opog/privacy/laws_and_regs.html)	Unable to determine.	Nothing besides the privacy page.	Determine if any reports exist. If needed update website and provide links on a new Privacy Policy page.	7/28/2017	Unable to determine.	 1/10/2018
Section 6.A.1.g	Does the website list and provide links to publicly available agency reports on privacy? Note: These reports need not include the agency's FISMA reports or reports provided to OMB and Congress.	Unable to determine.	No	Determine if any reports exist. If needed update website and provide links on a new Privacy Policy page.	7/28/2017	N/A	N/A 1/10/2018
Section 6.A.1.h	Does the website provide instructions on submitting a Privacy Act request for individuals who wish to request access to or amendment of their records? If not, please link to OPOG's Privacy Act page. (Example: http://www.osce.doc.gov/opog/PrivacyAct/PrivacyAct_requests.html)	Unable to determine.	No	Determine how requests will be submitted and update Privacy page.	7/28/2017	Yes, XXX links to the Privacy Act instructions on the DOC Privacy page.	 1/10/2018
Section 6.A.1.i	Does the website provide appropriate agency contact information for individuals who wish to submit a privacy related question or complaint? If not, please provide the appropriate privacy contact information.	No	No	Identify designated person and means of contact. Include in Privacy Home Page.	7/28/2017	Yes, XXX provides a link to the XXX Privacy Office and the Department's CPO.	 1/10/2018

**Policies for Federal Agency Public Websites and Digital Services
OMB MEMO-17-06 - Data Call**

OMB 17-06 Citing	OPOG's Initial Assessment	B/OU's Response	Target for Improvement	Completion Date Given	Analysis Status	Analysis Symbol	Date	
Section 6.A.1.j	Does the website list and provide a link to contact information for the Agency's Senior Agency Official for Privacy (SAOP)? If not, please use: www.commerce.gov/saop.	Did not see any links to agency's SAOP. Link to DOC's SAOP	No	Identify designated persons and means of contact. Include in Privacy Home Page.	7/28/2017	Yes, XXX provides an email link to the SAOP via the CPO@doc.gov on the DPP. However, the page does not identify the SAOP.		1/10/2018
	Does the website identify and provide contact information for the BCPO?	Could not easily find the B/OU's Chief Privacy Officer. Include contact information and email address to BCPO.	Yes	Identify designated persons and means of contact. Include in Privacy Home Page.	7/28/2017	Yes, the BCPO is identified on the PPP.		1/10/2018
Section 6.A.2	Does the B/OU maintain a sub agency , component , or program specific privacy program page? If so, the privacy program page must be accessible through www[sub agency, component, or program domain].gov/privacy. (Example: http://www.osec.doc.gov/opog/privacy/digitalpolicy.html#boupriavacy)	No	Agency level.	N/A	N/A	XXX PPP is not linked via www.XXX.doc.gov/privacy. This page is pointed to the DPP and not the PPP. The link needs to be changed to the correct page.		1/10/2018
SECTION 6. B. PRIVACY POLICIES ON AGENCY WEBSITE								
Section 6.B.1.a	Is the website written in plain language and organized in a way that is easy to understand and navigate? (Example: https://www.digitalgov.gov/resources/plainlanguagewebwritingtips/)	Unable to determine.	Yes	Will review to ensure plain language and organization (usability).	7/28/2017	The PPP is accessible via the About page; otherwise it is not easily found unless searching for it.		1/10/2018
Section 6.B.1.b	Does the Privacy Policy provide useful information that the public would need to make an informed decision about whether and how to interact with your agency? (This should include website, FAQs and other types of feedback loops.) (Example: https://www.digitalgov.gov/resources/plainlanguagewebwritingtips/)	Unable to determine.	No, current link renders an error	Will include FAQ section.	7/28/2017	Had to search to find FAQ but could not find any on Privacy, Privacy Act, SORN, etc.		1/10/2018
Section 6.B.1.c	Is the Privacy Policy updated whenever the agency makes a substantive change to the practices it describes?	Unable to determine.	Yes	OA should review Privacy Policy Content and provide OCIO with page updates when changes are made.	7/28/2017	Maintenance of Privacy Policy changes are not sent to the CPO@doc.gov.		1/10/2018
Section 6.B.1.d	Does the Privacy Policy include a time/date stamp to inform users of the last time the agency made a substantive change to the practices the privacy policy describes? Note: Must be included on every page.	Unable to determine.	No	Privacy Policy page does have an updated date and time stamp.	N/A	Not all pages contain date stamps. DPP does but the PPP does not.		1/10/2018
Section 6.B.1.e	Does the Privacy Policy adhere to all other applicable OMB requirements?	Unable to determine.	Yes	Will review to ensure all applicable OMB requirements are included.	7/28/2017	The PPP contains links to policies and a link to the policies on the DOC Privacy page.		1/10/2018

**Policies for Federal Agency Public Websites and Digital Services
OMB MEMO-17-06 - Data Call**

OMB 17-06 Citing	OPOG's Initial Assessment	B/OU's Response	Target for Improvement	Completion Date Given	Analysis Status	Analysis Symbol	Date	
Section 6.B.1.f	Does the Privacy Policy include a link to the agency's Privacy Program Page? If you do not have a page, please link to the OPOG webpage. (Example: www.commerce.gov/privacy)	Unable to determine.	No	Create link to the OPOG privacy program page.	7/28/2017	Could not find a link to the XXX or the Department's PPP on the DPP.		1/10/2018
Section 6.B.2	Does the Privacy Policy include content on the Children's Online Privacy Protection Act? If you do not have a page, please link to the OPOG webpage. (Example: http://www.oscc.doc.gov/opog/privacy/digitalpolicy.html#coppa)	Unable to determine.	No.	Will review Privacy Policy and update as required.	7/28/2017	Yes, the DPP contains a statement about COPPA and a link to the ftc.gov page https://www.ftc.gov/tips/advice/businesscenter/privacyandsecurity/children%27sprivacy .		1/10/2018
SECTION 6. C. PRIVACY ACT STATEMENTS FOR ONLINE COLLECTIONS OF INFORMATION								
Section 6.C	Does the website provide a Privacy Act statement for collecting information using an online interface?	Unable to determine.	Not on main website page. Its on the applications at the point of data collection.	Not on main website page. Its on the applications at the point of data collection. Will need to be included on Privacy Home Page (link)	7/28/2017	Could not find a link to the Privacy Act statement for collecting information using an online interface or the Department's PPP on the DPP.		1/10/2018
	Does the website provide a privacy notice to cover when a Privacy Act is not required but the public still has a possibility to provide PII to the agency using an online interface anyway?	Unable to determine.	Not on main website page.	Not on main website page. Will include as necessary.	7/28/2017	Unable to find.		1/10/2018
SECTION 10. COMPLY WITH 3RD PARTY WEBSITE AND APPLICATION REQUIREMENTS								
Section 10.C	Does the B/OU use third party websites and applications? If so, do they comply with all relevant privacy protection requirements and a careful analysis of privacy implications as specified in OMB Memorandum M 10 23, Guidance for Agency Use of Third Party Websites?	No	No	N/A	N/A	N/A	N/A	1/10/2018

DIGITAL PRIVACY REPORT

- The policies for Federal Agency Public Websites and Digital Services (OMB Memorandum 17-06) will be used as the template for the analysis.
- The BCPO will be consulted for clarification.
- The report will be provided to the CPO.
- The follow icons will be used to notate the following:



- - Update is in progress



- - Update is complete



- - Indication of update was not found



- - Indication of new update is forthcoming

Federal Privacy Updates

2017 Federal Privacy Summit

The Federal Privacy Summit was held on December 12, 2017 in which there were more than 400 attendees. The keynote address was provided by Neomi Rao, Administrator of the Office of Information and Regulatory Affairs. In addition to networking session which gave attendees the opportunity to interact with Senior Agency Officials for Privacy and the Privacy Council's Committees and Working Groups, there were 16 breakout sessions on a wide variety of topics, such as shared services, privacy compliance reviews, the Paperwork Reduction Act, authentication, identifying and managing risk, and biometrics.

Updated Directive on Border Search of Electronic Devices (CBP Directive No. 3340-049A)

This directive enhances the transparency, accountability, and oversight of electronic device border searches performed by the U.S. Customs and Border Protection (CBP). The purpose of this directive is to provide guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers, tablets, removable media, disks, drives, tapes, mobile phones, cameras, music and other media players, and any other communication, electronic, or digital devices subject to inbound and outbound border searches by the CBP.

Upcoming Event

Tech Tuesday

Tuesday, February 13, 2018

Time: 1:00 p.m. 2:30 p.m.

GSA HQ 1800 F St NW

Washington DC, 20420

Room 1408

Dial-in (b)(6)

Adobe Connect (b)(6)

(b) (5)

(b) (5)

(b) (5)

Guide to Conducting a PII Breach Table Top Exercise (TTX)

Prior to Conducting this TTX

1. Review the DOC PA, PII, and BII Breach Response Plan.
2. Review OMB Memorandum 17 12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.

Breach Response Team Members

1. Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)
2. General Counsel (legal counsel)
3. Chief Information Officer (CIO) or the CIO's designee
4. Senior Agency Information Security Officer (SAISO) or the SAISO's designee
5. Chief Financial Officer/Assistant Secretary for Administration
6. Assistant Secretary for Legislative and Intergovernmental Affairs (OLIA) (legislative affairs official)
7. Chief of Staff, Office of the Secretary
8. Director, Office of Public Affairs (OPA) (communication official)
9. Director, Office of Policy and Strategic Planning
10. Director, Office of Human Resources Management
11. Office of Security (OSY), Attends on an as needed basis
12. Office of Inspector General (OIG), Advisory Role
13. Bureau Chief Privacy Officers
14. Privacy Act Officers
15. Deputy Director for Departmental Privacy Operations
16. Departmental FOIA/PA Officer

Planning

1. Establish the objectives of the TTX. Some of your objectives may be:
 - a. Improve the understanding of the DOC Breach Response Plan.
 - b. Identify opportunities to improve the DOC Breach Response Plan and the Department's preparedness.
 - c. Identify interdependencies among agency organizations and third party service providers.
2. Plan the TTX logistics.
 - a. Determine the date.
 - b. Reserve a space with an appropriate clearance level, as well as any materials or multimedia support you may need, such as computer and display, whiteboard and markers, butcher block paper, handouts, and dial in capabilities.
 - c. Set a time limit for the TTX. This will help you choose an appropriate scenario and focus the conversation appropriately during the TTX.
 - d. Assign support staff roles.

- i. Determine what role you want your privacy program to play in the exercise. Individuals who are deeply involved in planning the TTX may need to take a step back during the exercise to avoid accidentally influencing the course of the exercise. In a TTX, privacy office representatives often act in an advisor or consultant role, responding to questions from other participants, rather than the active leaders they often are in an actual breach.
- ii. Identify a facilitator (Consider using a neutral facilitator). The facilitator has the primary responsibility for exercise conduct. This includes introducing and providing scenario updates, moderating the discussions to ensure players address exercise objectives and core capabilities, and ensuring everyone contributes to the discussion and relevant issues are explored as thoroughly as possible within the allotted time.
- iii. In addition to a facilitator, you will also need staff dedicated to:
 - 1. Taking notes. These notes will form the basis of the after action report.
 - 2. Tracking “parking lot” issues.
 - 3. Documenting when Breach Response Plan steps are completed.
- e. Create a participant roster to track attendance at the TTX.
- f. Consider what role you want Senior Executive Service (SES) members and other senior leaders to play. SES member participation may stifle the conversation. Consider using SES members or other senior leaders as floaters who give out real time feedback.

A sample agenda is below:

Time	Activity
[Month Day, Year]	
0000 - 0000	Registration
0000 - 0000	Welcome and Introductions
0000 - 0000	Exercise Overview
0000 - 0000	Module 1: Initial Response – Scenario Background
0000 - 0000	Break
0000 - 0000	Module 2: Response
0000 - 0000	Module 3: Recovery
0000 - 0000	Break
0000 - 0000	Hot Wash

Time	Activity
0000 - 0000	Closing Comments
0000 - 0000	Debrief (Facilitators and Evaluators only)

3. Develop a realistic breach scenario.

a. Choosing a scenario.

- i. Consider which high value assets, applications, or processes you may want to include in the scenario.
 1. You do not have to limit yourself to high value assets, but you want to make sure the scenario has stakes. A high profile system or program, or a scenario that involves risks to the reputation or operations of the agency may be more engaging and offer more avenues for the participants to explore.
- ii. Look at the Department's recent breaches, as well as any major breaches, for ideas.
- iii. Review the Department's breach metrics to see where there are trends that may indicate a weakness or identify an issue about which you receive questions or complaints and consider developing a scenario around those fact patterns.
- iv. Consider breaches that will engage all of the participants. For example, a loss of hardcopy documents may not effectively engage a participant from the cybersecurity team. A scenario that requires cross functional collaboration (e.g., between staff supporting Freedom of Information Act (FOIA), privacy, cybersecurity, and human resources) is often a more effective TTX.
- v. Balance the complexity of the TTX with the knowledge and experience the BRT members have with handling a breach. A too simple scenario may not be an effective use of this training and awareness opportunity; a too complex scenario may make it difficult for participants to engage in the TTX.

b. Refining the scenario.

- i. After you have chosen the breach you would like to test, speak with the relevant program office and/or system owners to ensure that you understand their data and processes. The scenario should be grounded in reality.
- i. Create a scenario that evolves over time. Create injects that complicate the scenario by adding additional facts. Provide a realistic timestamp for each update to help participants track their compliance with reporting requirements and understand how long actual breach response activities may take.
- ii. You should be able to map the DOC Breach Response Plan steps to the steps in your TTX; this will help you ensure that you have not forgotten any aspects of the DOC Breach Response Plan in the development of the scenario. Consider creating a table or grid citing back to the plan to ensure you know each BRT member's role and responsibility.
- iii. Try to make the TTX as interactive as possible. Break the scenario into modules with injects to keep participant attention and focus the discussion.

4. Create supporting artifacts, such as breach reports, supplemental reports, and after action reports.

- a. Use the Department’s breach reporting forms, including supplemental reports and after action reports, for the exercise. Using existing artifacts may highlight areas that need clarification or improvement.
 - b. You may want to create additional artifacts, such as dummy data file examples and external press reports.
 - c. Be sure to label all documents created for the TTX with “For exercise purposes only.”
 - d. It can be helpful to have packets available to the participants that include your agency’s breach response policy, the initial scenario, the injects, and any other supporting materials. The participants should not view the injects until they are directed to by the facilitator.
5. Provide an executive summary of the goals of the breach response program, its importance, and the goals and relevance of the TTX for senior leadership prior to TTX.

Execution

1. Share the TTX ground rules with the participants.
 - a. Stress that this is a learning exercise and that participants should feel comfortable asking questions or throwing out ideas. There are no wrong answers and everyone’s opinion will be considered.
 - b. Emphasize that participants should not “fight the scenario.” Every effort will have been made to ensure that the scenario is realistic and reflects actual practices.

Examples of TTX Ground Rules
<ul style="list-style-type: none"> Silence cell phones and other mobile devices during the exercise. Accept that the circumstances surrounding the event are real. This is a “no-fault” environment where varying viewpoints and disagreements are to be expected. There are no wrong answers.

2. Present the initial facts of the scenario to the participants. Use prompts to encourage interaction if the conversation is slow to start.
3. Participants should begin to identify immediate actions that should be taken, including establishing a communications plan and, if appropriate, Congressional notification plan.

Examples of Questions the BRT Should Consider
<ul style="list-style-type: none"> Is there a SORN or PIA? What other agency stakeholders or partners should be made aware of the breach? Who reports the breach to Congress? Who will need to approve any notices, notifications, and other communications? Who would be the source of the notification? Is any official designation required? How and who will fund identity protection services (IPS)? Does the CFO need to be engaged before securing IPS? Is there a vendor engaged for call center and IPS?

4. Start to provide injects to the scenario that reflect the types of information you would learn from a breach investigation.
 - a. With each inject, participants should identify the actions that should be taken based on the updated information.
 - b. You can also ask questions that explore other potential aspects of the breach. For example, if your breach involves information about members of the public only, you can ask them whether they would do anything differently if employee information was included.
5. Have participants complete a post TTX survey before leaving to get their input on the quality and strengths of the TTX, suggestions for improvement, and recommendations for future TTX scenarios.

Close-out

1. Develop an after action report/improvement plan that documents lessons learned and follow up actions for strengthening the DOC breach response process and/or the system, program, or processes that were tested in the TTX. The report/plan must provide timelines for improvement recommendation implementation and assignment to responsible parties.
 - a. Also document lessons learned for the next tabletop exercise. You can include these in the same report or a separate document.
 - b. Share the report with the BRT.
2. Review the DOC Breach Response Plan for any needed changes based on the lessons learned from the TTX.
3. If appropriate, conduct an out brief for senior leadership. The briefing should identify any unresolved issues to allow leadership to determine if any unmitigated risks are within the Department's risk tolerance.

Identity Protection Services (IPS) Multiple Award Blanket Purchase Agreement (BPA)

To best ensure federal customers have access to a pool of well qualified contractors capable of providing identity protection services to include data breach response and protection identity monitoring, GSA now offers government-wide Federal Supply Schedule (FSS), Blanket Purchase Agreements (BPAs), to provide these services.

Under the BPAs, which are in effect for the next five years, federal agencies have access to a variety of identity protection services covering both routine protection services that include:

- Consumer credit reports, address verification reports, and credit risk assessments; and
- Recovery services involving suspected or actual breaches of sensitive personally identifiable information.

Specifically, this government-wide multiple award BPA provides identity monitoring data breach response and protection services for the federal government including:

- Business information services;
- Credit monitoring services;
- Identity monitoring services;
- Identity theft insurance;
- Identity restoration services;
- Website services; and
- Call center services (related to these requirements).

Tiers of Experience

Two tiers of contractors are available under the BPAs:

- Tier 1: Is awarded only to Contractors with experience in responding to data breaches impacting populations of significant size (benchmark of 21.5 million); and
- Tier 2: Includes Contractors with general experience in providing routine data breach responses.

Tier 1 Contractors are included in Tier 2. Ordering Contracting Officers have the discretion to compete task orders (TO) at either Tier regardless of the impacted population size.

During the performance period of the BPAs, Tier 2 Contractors not selected as Tier 1 service providers can provide to the BPA Contracting Officer evidence of their experience in responding to data breaches impacting populations of significant size and based on that documentation, may be added to Tier 1.

For smaller numbers of individuals, it is recommended to use credit monitoring services under Tier 2 on the website. If the total cost of credit monitoring services falls under the purchase card threshold of \$2,500, you can contact any one of the three contractors directly, ask for a quote based on "BPA CLIN 0003A," (CLIN stands for Contract Line Item Number), and place the order directly with the contractor you choose.

Authorized Users

Any warranted Contracting Officer from authorized users of the Schedules program, within the scope of their delegated procurement authorities, may place orders against the BPA(s).

IPS BPA Ordering Period

Five years from September 01, 2015, through August 31, 2020. Orders (including order options) have their own period of performance. Any orders placed during the BPA ordering period may extend beyond that period (including the right to exercise order options) and be completed in accordance with the Contractor's FSS FAR clause 52.216-22 paragraph (d).

Order Dollar Value Limitations

Unlike most ID/IQ Contracts, BPAs do not have a dollar value ceiling. Thus there is no dollar value limitation on the size of an order.

Small Business Credit

Agencies will receive small business credit when issuing orders to small business BPA holders. For BPAs based on a Contractor Teaming Arrangement (CTA), a small business team member may be designated as the CTA lead for any task order as applicable. Hence, all CTA members have been assigned BPA numbers for this purpose. Agencies are also authorized if applicable to set-aside orders for small business. See ordering procedures for further details.

IPS BPA Award Information

Collect estimates from each contractor. POCs are listed on the contract. If the quote is under \$2,500, you may use the government purchase card.

In November 2017, three contractors offered BPA CLIN 0003A credit monitoring services. The following are the estimates received at that time based upon approximately 10 individuals for one year. You will need to call each contractor and get an estimate based upon your breach, i.e., the number of individuals required services and the duration of the service. You also will need to obtain a description of the specific services offered with the cost estimate.

Contactor	Cost Per Person Per Year	Phone	Website and Email
ID EXPERTS	\$51.58	(866) 726-4271	http://www.idexpertsCorp.com/ mailto:government@idexpertsCorp.com
IdentityForce	High Risk \$49.66 Low Risk \$15.17 Package 3 \$10.18	(508) 210-4414	http://www.identityforce.com/ mailto:sbrown@identityforce.com
LADLAS PRINCE LLC	\$38.50	(248) 875-3409	http://www.ladlasprince.com/ mailto:Amos.O.Ajani@ladlasprince.com

Contact

Email Professional Services at professionalservices@gsa.gov.

Additional information can be found at: www.gsa.gov/ipsbpa.

Government/GSA POC:

Kenny Yiu
Senior Contracting Officer
GSA, FAS, PSHC
400 15th Street SW
Auburn, WA 98001
kenny.yiu@gsa.gov
253-931-7915



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

July 1, 2016

M-16-14

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

FROM: Anne E. Rung 
United States Chief Acquisition Officer

SUBJECT: **Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response**

This memorandum updates a longstanding Office of Management and Budget (OMB) policy, first implemented in 2006, to maximize federal agency use of a government-wide solution for acquiring identity protection services when needed. This memorandum requires, with limited exceptions, that when agencies need identity protection services, agencies address their requirements by using the government-wide blanket purchase agreements (BPAs) for Identity Monitoring Data Breach Response and Protection Services awarded by the General Services Administration (GSA), referred to below as the “IPS BPAs.”

For the past decade, GSA has offered commercial credit monitoring services through government-wide BPAs established under its Federal Supply Schedules (FSS) Program. When the BPAs were launched, OMB instructed agencies to review the pricing and terms and conditions of the BPAs in addition to any other credit monitoring services they may be considering in their market research and notify OMB prior to making an award outside of the BPAs.¹

Last year, GSA partnered with other agencies on requirements for new BPAs to ensure that all agencies have access to a pool of best qualified contractors capable of providing a comprehensive range of identity protection services, including credit monitoring. For details on the IPS BPAs, including task order instructions, offered services, authorized users, order dollar value limitations, the inclusion of agency specific terms, and ordering periods, visit www.gsa.gov/ipsbpa.

Taking advantage of the IPS BPAs ensures agencies can meet their needs for expeditious delivery of best-in-class solutions from pre-approved and vetted companies at competitive pricing and reduced administrative costs. For these reasons, the IPS BPAs shall be treated as a preferred source for Federal agencies when agencies have a need for credit monitoring, breach response, and identity protection services. Consistent with category management principles, GSA, as the contract manager, will work with an interagency team to periodically review and refresh, as appropriate, the contract terms and requirements to ensure the BPAs continue to reflect the best identity protection practices and agencies’ needs.

¹ See OMB Memorandum M-07-04, *Use of Commercial Credit Monitoring Services Blanket Purchase Agreements*.

The following steps, which are effective immediately, are designed to ensure agency use of the IPS BPAs to the maximum extent practicable:

1. **Review the range of services offered under the IPS BPAs:** If the agency has an existing vehicle that overlaps with the BPAs and is planning to exercise an option, or is planning to issue a new contract that could overlap with the BPAs, take the additional steps described below.

2. **Existing contracts:**

a) **Analysis of alternatives:** As part of deciding whether to exercise an option under an existing agency contract, and in accordance with Federal Acquisition Regulation (FAR) 17.207, the agency shall analyze terms/conditions, pricing, performance, fees and savings under the agency contract relative to the IPS BPAs. The agency may also consider the impact on an incumbent small business contractor.

b) **Sharing of final analysis:** If the agency exercises the option, it shall provide the final analysis to GSA and OMB at the following URL:
<https://community.max.gov/x/CoELQ>.

c) **Agency approvals:** If an agency proceeds with exercising an option under an existing agency contract, the agency shall ensure the final analysis has been approved by the Senior Agency Official for Privacy (SAOP) and any other officials as identified by internal agency policies.

d) **Sharing of prices paid and other contract information:** If the agency exercises the option, it shall submit, using the URL provided above:

(i) a copy of the option and underlying contract vehicle and,

(ii) at the end of the option period, prices paid under the option.

3. **Planned procurements:**

a) **Analysis of alternatives:** Agencies that are considering a different vehicle to provide identity protection services shall develop an analysis of alternatives that compares the planned vehicle to the IPS BPAs in terms of: scope, period of performance, terms and conditions, pricing, performance, administrative costs (cost of full-time equivalent employees supporting award and administration of the vehicle vs. the fees that would be paid to use the IPS BPAs) customer satisfaction (if the organization has previously managed a similar vehicle), and small business impact, if any. The analysis should also highlight any unique features and/or requirements. Finally, if the agency is planning an inter-agency

contract, its evaluation should include a market analysis and a description of the agency's suitability for managing the vehicle.

- b) Sharing of analysis: If the agency proceeds with its own vehicle, it shall:
 - (i) provide the final analysis to GSA and OMB at the URL identified above; and
 - (ii) if the anticipated value of the vehicle exceeds the simplified acquisition threshold (SAT), the agency shall share a draft of the analysis with the Category Manager for Professional Services and OMB at <https://community.max.gov/x/CoELQ> for a five (5) business day review period to offer input on the analysis.
- c) Agency approvals: If, after considering any input from the Category Manager, the agency decides to proceed with its own vehicle, it shall ensure the final analysis has been approved in accordance with internal agency policies. At a minimum, the analysis shall be approved by the SAOP and, if the vehicle has an anticipated value above the SAT, by the agency's Senior Procurement Executive.
- d) Sharing of prices paid and other contract information: If the agency proceeds with its own vehicle, the agency shall submit using the URL provided above:
 - (i) a copy of the contract vehicle; and,
 - (ii) at the end of the base and each option period, prices paid under the contract vehicle.

Agencies that require contractors to provide identity protection services, or a subset thereof, as part of the security or safeguarding requirements in their contract are exempt from this guidance. However, pursuant to FAR Part 51.1 Contractor Use of Government Supply Sources, agencies may at their discretion authorize government contractors under cost-reimbursement contracts and fixed price contracts for protection of security classified information and related security equipment to use GSA sources, including the IPS BPAs, when determined to be in the best interest of the government. Additionally, agencies may seek a deviation pursuant to FAR Subpart 1.4 to address other situations where contractor access to the IPS BPAs would be beneficial.

By implementing the process described above, the government will serve the needs of impacted individuals, programs, and operations by leveraging the government's robust buying power abilities to provide cost-effective, best-in-class solutions. Agencies are encouraged to contact GSA and OMB with any potential questions or concerns regarding the implementation of included instructions.

For further questions regarding this memorandum, please contact Iulia Manolache in the OMB's Office of Federal Procurement Policy at imanolache@omb.eop.gov or (202) 395-7318.

Privacy Council Face-to-Face Meeting Agenda – February 6, 2018

Time	Topic	Presenter
08:00 – 08:30	Arrival	
08:30 – 08:40	Welcome and Introductions	Lisa Martin
08:40 – 08:50	Action Item Updates	Catrina Purvis
08:50 – 09:20	Privacy Program Coordinator Updates <ul style="list-style-type: none"> • PII Incident Metrics • PIA Compliance Metrics 	Tahira Murphy/Nate Thweatt Kathy Gioffre
09:20 – 09:30	Federal Privacy Updates <ul style="list-style-type: none"> • Federal Privacy Summit • Updated Directive on Border Search of Electronic Devices • EU General Data Protection Regulation (GDPR) • Upcoming Events 	Lisa Martin/Catrina Purvis
09:30 – 10:00	Privacy Program Highlights <ol style="list-style-type: none"> 1. Privacy Act Officer Updates 2. SSN Fraud Prevention Act Update 3. Credit Monitoring 4. DOC Website Reviews 	Michael Toland Lisa Martin/Michael Toland Lisa Martin Tahira Murphy
10:00 – 10:15	BREAK	
10:15 – 11:15	Privacy Program Improvement/Policy Reviews <ol style="list-style-type: none"> 5. FY18 PII Breach Table Top Exercise Planning 	
11:15 – 11:45	BOU Member Time <ul style="list-style-type: none"> • SharePoint Privacy Warning Banner when Logging In 	Byron Crenshaw
11:45 – 12:00	Round Table	Catrina Purvis
12:00 – 12:30	Year-End Assessment	Lisa Casias

(b) (5)

The Annual Compliance Review Processes Compliance Review Board (CRB) and the Certification Process

Two options are available to complete the annual system review requirement, the Compliance Review Board (CRB) and the Certification process. Most of you are all familiar with the CRB, but the Certification Process is relatively new. As a matter of practice, we will continue to schedule all systems for a CRB. If you plan to use the Certification Process, notify us as soon as possible. If we do not receive your Certification package with two weeks of the schedule CRB, we will expect you to attend the CRB.

I. The Certification Process

- You are eligible to use the Certification Process, if:
 - The system has gone through the CRB process and received a SAOP-approved PIA within the last three years.
 - No changes have occurred in the system that would create new privacy risks, i.e., you are able to check the third option in the Question 1.1 of the PIA.
- The certification package needs to be complete and consists of three documents:
 - Certification Form
 - Last SAOP-approved PIA with updated ATO, current signatures, and any updated information that does not create new privacy risks.
 - PTA with new signatures and updates as needed.
- Certification Form is complete when:
 - All the blanks need to be completed.
 - The form is signed by:
 - The IT System/Program Owner or ISSO,
 - Privacy Act Officer, and
 - Bureau Chief Privacy Officer (BCPO)
- The Certification package is submitted to the CPO mailbox at CPO@doc.gov with two weeks of the scheduled CRB.
- The transmittal email states:
 - No changes have been made to the last SAOP-approved PIA, other than an updated ATO date and current signatures, and/or
 - If applicable, identify where any minor changes or clarifications have been made, e.g., Question 1.1, 12.2, 12.3. Remember, if the changes create new privacy risks, you may not use this process.
 - Submissions are subject to periodic or random reviews.

II. The Compliance Review Board Process

- All new PIAs and PTAs must be submitted on the new templates, Version Number 01-2017.
- All PIA and PTAs must be submitted 60 days prior to expiration of the system's ATO. This will now be tracked.
- Currently, the DOC OCIO participates in the CRB. However, the authority to assess system controls will be delegated by DOC OCIO to the BOUs effective in February. We are waiting for the delegation memo to be distributed.

- The BOU system owner, ISSO and/or BCPO will be asked to confirm the following has been completed:
 - A crosswalk review of the NIST SP 800-122 Privacy Controls has been conducted and the risks are found to be acceptable.
 - A review of the NIST SP 800-53, Revision 4 Privacy Overlays Security and Privacy Controls. This document is comprised of four Privacy Overlays that identify security and privacy control specifications required to protect personally identifiable information (PII) at various levels of PII sensitivity.

Upcoming Data Call:

- Privacy Review of Forms

Upcoming Request for Comments:

- Delegation of the Departmental OCIO Review of Security Controls

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Tuesday, February 6, 2018 4:09 PM
To: Jean Apedo NOAA Federal
Cc: Anne Lynch; Mark Graff NOAA Federal
Subject: Re: re NOAA0900 certification in place of new PIA
Attachments: NOAA0900 PTA 2018.docx

Here is the PTA completed by me and ready for signatures.

On Tue, Feb 6, 2018 at 3:39 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
Forgot to say that DOC has scheduled the CRB, IF we were submitting a revised PIA, for 2 22 17. At the very least, they would want a certification ASAP, and the other two docs could follow. So would it be possible for you to sign the ISSO slot on the certification and return to me today or tomorrow?

thx Sarah

On Tue, Feb 6, 2018 at 3:27 PM, Jean Apedo NOAA Federal <jean.apedo@noaa.gov> wrote:
Hi Sarah,
I will follow up with the team and get back to you.
Thank you.

On Tue, Feb 6, 2018 at 3:25 PM Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
Jean I discussed this with Anne. We don't know who the new SO is, but Anne thought you could sign the last PIA and a new PTA as both the ISSO and ITSO? Or what about James Jones for one of them? We don't know what happened to SK Bhachech but my email to him was returned.

Attached is the last approved PIA with new ato date for you to sign, but the PTA is in a new template. I'll take a stab at it it has a new list of questions in the system description and send to you.

Also attached is the certification. We need to figure out who will sign no ITSO signature required, but maybe you can sign as the ISSO? And the date of last CRB was 6 15 17.

I am right down the hall this pm and most of tomorrow!

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)

Ce (b)(6)

Jean Apedo, CISSP, CAP
ITSO/OCIO
[1315 East West Highway](#) SSMC3
Silver Spring, Maryland 20910
Tel: [\(301\) 628-5730](#)

"Cogito ergo sum" R. Descartes

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](#)
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Wednesday, February 7, 2018 10:16 AM
To: Mark Graff NOAA Federal
Subject: NOAA2220 PIA and PTA for your signature
Attachments: NOAA2220_PIA_020718 for MHG signature.pdf; NOAA2220
PTA_01_23_2018_final_v2_requires_signatures_itso_isso_AO.pdf

Mark, I had not asked Sean to do a PTA in the new template, but I can still do after the fact if you think best.

I did one already for NOAA0900.

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751

Ce (b)(6)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Mark Graff - NOAA Federal

From: Mark Graff NOAA Federal
Sent: Wednesday, February 7, 2018 11:14 AM
To: Sarah Brabson NOAA Federal
Subject: Fwd: NOAA2220 PIA and PTA for your signature
Attachments: NOAA2220 PTA_01_23_2018_final_v2_requires_signatures_itso_isso_AO mhg.pdf;
NOAA2220_PIA_020718 for MHG signature mhg.pdf

Signed and attached to accompany the re certification. Great news on the elimination of SSNs from the collections referenced in Sec. 12. I wouldn't worry about the new PTA template unless DOC mentions it. I think their push is on the PIAs since those will be forward facing. Where the PTA answer is "yes, we need a new PIA", a new template has no substantive bearing on the outcome.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

Forwarded message

From: Sarah Brabson - NOAA Federal <sarah.brabson@noaa.gov>
Date: Wed, Feb 7, 2018 at 10:16 AM
Subject: NOAA2220 PIA and PTA for your signature
To: Mark Graff NOAA Federal <mark.graff@noaa.gov>

Mark, I had not asked Sean to do a PTA in the new template, but I can still do after the fact if you think best.

I did one already for NOAA0900.

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

**U.S. Department of Commerce
NOAA**



**Privacy Threshold Analysis
for the
Ships Fleet Support System (SFSS) NOAA2220**

**U.S. Department of Commerce Privacy Threshold Analysis
NOAA Ship Fleet Support System**

Unique Project Identifier: 006-48-01-15-02-3601-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *NOAA2220 is an amalgamation of sixteen ships with similar general functions and operating characteristics, security needs, and operating environments. Common functions of all of the ship backbone subsystems are to provide network connectivity, domain authentication, internet connectivity and general business support services. While each ship has common (or class similar) configurations, mission requirements require each to have a unique configuration.*

The NOAA fleet of ships are managed, operated and maintained by NOAA's Office of Marine and Aviation Operations (OMAO), Marine operations centers (MOC), located in Norfolk, Virginia and Newport, Oregon. Additional ship specific support is provided through port office facilities in Woods Hole, Massachusetts; Charleston, South Carolina; Pascagoula, Mississippi; Davisville RI, and Ford Island, Hawaii. Ships are also maintained pier side in Newport, RI and Kodiak, Alaska.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

This is a new information system. *Continue to answer questions and complete certification.*

This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

This is an existing information system in which changes do not create new privacy risks. *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *Please describe the activities which may raise privacy concerns.*

- NOAA2220 ships have a Closed Circuit Television (CCTV) system that is used to record video throughout the ship for the purpose of safety. Ships personnel are notified by signs located throughout the ship that state that these premises are under video surveillance and cameras in use.
- NOAA2220 Aircraft record Crew Members and Scientific Partners names that participate in the flight and publish those names on the internet with the data for the flight in which they participated in.

No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.).”

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

X No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PIA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

 X I certify the criteria implied by one or more of the questions above **apply** to the Ship Fleet Support System and as a consequence of this applicability, I will perform and document a PIA for this IT system.

 I certify the criteria implied by the questions above **do not apply** to the Ships Fleet Support System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Sean T. McMillan

Signature of ISSO or SO: MCMILLAN.SEAN.T. 1185814382 Digitally signed by MCMILLAN.SEAN.T.1185814382 Date: 2018.01.31 12:52:47 -05'00' Date: 24 Jan 2018

Name of Information Technology Security Officer (ITSO): James Jones IV, LCDR, USPHS

Signature of ITSO: JONES.JAMES.IV.1049453465 Digitally signed by JONES.JAMES.IV.1049453465 Date: 2018.01.29 12:16:39 -05'00' Date: _____

Name of Authorizing Official (AO): Joseph Baczkowski, CDR, USPHS

Signature of AO: BACZKOWSKI.JOSEPH.PADES.1167987300 Digitally signed by BACZKOWSKI.JOSEPH.PADES.1167987300 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USPHS, cn=BACZKOWSKI.JOSEPH.PADES.1167987300 Date: 2018.02.06 16:52:33 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): MARK GRAFF

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.02.07 11:02:05'00' Date: _____

**U.S. Department of Commerce
National Oceanographic and Atmospheric
Administration (NOAA)**



**Privacy Impact Assessment
for the
NOAA Ship Fleet Support System (NOAA2220)**

Reviewed by: _____, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment

NOAA OMAO Ship Fleet Support System

Unique Project Identifier: 006-48-01-15-02-3601-00

Introduction: System Description

The NOAA2220 System consists of ships, aircraft and land based ground support systems. Many of these systems have similar general functions and operating characteristics, security needs, and operating environments, and shore-based applications that support the ship missions. Common shipboard IT infrastructure functions include network connectivity, domain authentication, internet connectivity, and general business support services, such as file and print services. Ships are configured with satellite communication systems, such as Inmarsat and VSAT, and connect to NOAA networks and the internet via contract satellite service providers. While each ship has common (or class similar) configurations, mission requirements require each to have a unique configuration. To facilitate their inclusion in a consolidated System Security Plan (SSP), each ship and subsystem is described in the System Security Plan.

The NOAA fleet of ships are managed, operated and maintained by NOAA's Office of Marine and Aviation Operations (OMAO), Marine operations centers (MOCs), located in Norfolk, Virginia; Honolulu, Hawaii; and Newport, Oregon. Additional ship-specific support is provided through port office facilities in Woods Hole, Massachusetts; Davisville, Rhode Island; Charleston, South Carolina; Pascagoula, Mississippi; San Diego, California; and Ford Island, Hawaii. Limited pier-side support is also provided to ships in Newport, Rhode Island and Kodiak, Alaska.

Typical PII transactions in the NOAA2220 system consist of transmitting information to and from NOAA Workforce Management Office, to facilitate Human Resources (HR) processes, processing of benefits for wage mariners, and continuation of medical care for sick and injured mariners, and as required by other government agencies and industry.

For HR processes and processing of wages, NOAA2220 collects: name, work and home addresses, telephone numbers and email addresses; and passport number for travel purposes. This data is secured through physical controls for facilities and encryption at rest for soft copies.

Currently NOAA2220 stores Health Insurance Portability and Accountability Act (HIPAA) information in a secure manner at Marine Operation Center-Atlantic (MOC-A), Marine Operation Center Pacific (MOC-P), and HQ: hard copies are secured by physical controls implemented at each facility that meets NIST SP 800-53 rev.4 requirements; and soft copies data is encrypted at rest. The HIPAA information consists of medical information for NOAA employees and guests who sail on a NOAA vessel, as well as for contractors who will be on board for more than 24 hours. This information is transmitted as needed via secure means by Accellion, secure e-mail, or fax (with notification to the recipient so he/she will be standing at

the fax machine). There are multiple medical officers who share responsibility for collecting and transmitting HIPAA information. Any medical officer who has this responsibility is trained and aware of how to handle such information.

NOAA2220 collects two forms of identification (Commerce ID, Driver's license number and/or passport number) in order to issue a CAC or Alt tokens. The system also collects user-id and date-time access information for federal employees and contractors with a valid CAC cards at MOC-P and MOC-A. The form used to collect this information is DD-2841. These forms are stored on NOAA1200 on a file server once received by Local Registration Authority (LRA).

Information is shared on an as-needed basis after both authorization and need to know have been determined. Most information that needs to be shared is collected and sent to the NOAA Workforce Management Office for dissemination. There are some instances where NOAA employees' PII will be sent to other Department of Commerce (DOC) agencies and to other federal agencies if the employees are detailed temporary or permanently.

The Aircraft Fleet Support System (AFSS) includes two primary networking segments, the Aircraft Computing Systems (ACS) and the Ground-based Support Network (GSN), and an alternate site located at the National Weather Service Facility in Ruskin, FL. These segments provide critical services during mission operations. The alternate site provides critical application and storage redundancy.

The network segment that encompasses the NOAA aircraft fleet is identified as the AFSS Aircraft Computing Systems (AFSS/ACS). All aircraft have common IT functions that can provide network connectivity, Internet connectivity, and general business support services. In addition to common IT functions, each aircraft is required to support scientific data collection and distribution of data to onboard systems and to ground-based systems during flight. The IT equipment and network configurations on the aircraft are unique due to the regularly changing project and mission requirements.

The ground-based network segment is identified as the AFSS Ground Support Network (AFSS/GSN). The GSN is a multi-segmented system that uses a single firewall/gateway device to apply a separation of network resources that restricts access to and from internal resources and public servers. The GSN permits public access to organizational web servers and FTP servers, supports ACS-to-ground data-flow applications, and hosts data processing and development systems.

The aircraft collect various raw data through a suite of sensors outside the aircraft and in expendable drop sensors. Certain data points are immediately transmitted from the aircraft to the ground stations, while the remaining raw data set is stored on the aircraft until it returns to ground. At the end of the mission the entire data set is transferred to ground servers for processing.

The raw data set is publically available on the public web server. Pertinent data set is directly transmitted to the National Weather Service telecommunication gateway while the aircraft are on mission and in the air.

Legal authorities to collect PII and/or BII:

NOAA2220's legal authorities to collect PII are:

Title 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.C. 3101, 3309, Title 29 U.S.C 651-78, Title 28 U.S.C. 2671-2680, Executive Order 12196, Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966, Title 33 U.S.C. 853i; 853j; 853j-1; 853t; 854; 854a-1; 857-5, 857a, 855, Title 37 U.S.C; Executive Order 10450, Title 16 U.S.C. 143, and Executive Order 11222.

NOAA2200 is a FIPS 199 moderate level system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

This is a new information system.

This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging	X*	g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

This is an existing system with no changes that create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (Check all that apply.)

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License	x	j. Financial Account	
c. Employer ID	x	g. Passport	x	k. Financial Transaction	
d. Employee ID	x	h. Alien Registration		l. Vehicle Identifier	

m. Other identifying numbers (specify): HR and Medical Files/Records are stored in NOAA2220 on file servers that have least-privilege functions enforced on them and only authorized personnel can view them; and these records are transmitted via fax or Accellion to service entities. DOB, HIPAA information, and other PII are collected only when needed by the requesting staff office in order to provide continuity of care, maintain official records (personnel records/officer records), and HR Processes including hiring, travel and performance appraisals.

General Personal Data (GPD)

a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name	X	h. Place of Birth	X	n. Financial Information	
c. Alias	X	i. Home Address	X	o. Medical Information	X
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education	X	r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)

a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Medical records regarding injuries and sickness acquired while underway as necessary to facilitate care when at sea and ashore.					

Distinguishing Features/Biometrics (DFB)

a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)

a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

--

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify) Sometimes we have NOAA employees who transfer within DOC to other offices such as DOC Office of the Inspector General (OIG) and we are required to transfer PII information. Whenever PII is transmitted to DOC or other federal agencies, it is done via fax or Accellion.					

Non-government Sources					
Public Organizations		Private Sector	X*	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

*Private medical office

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)					
Smart Cards				Biometrics	
Caller-ID				Personal Identity Verification (PIV) Cards	
Other (specify):					

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
---	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities					
Audio recordings				Building entry readers	
Video surveillance	X*			Electronic purchase transactions	

Other (specify):

*NOAA2220 ships have a Closed Circuit Television (CCTV) system that is used to record video throughout the ship for the purpose of safety. Ships' personnel are notified by signs located throughout the ship that state that these premises are under video surveillance and cameras in use. Least privileges are enforced for access to the video surveillance data. Only authorized personnel will have access. The NOAA2220 System Owner will be responsible for granting access and controlling who has access to this information. The orientation packet given to those traveling on the ships includes a vessel orientation and a statement about safety compliance.

There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.
(Check all that apply.)

Purpose			
To determine eligibility		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Medical care NOAA2220 ships have a Closed Circuit Television (CCTV) system that is used to record video throughout the ship for the purpose of safety. The orientation packet given to those traveling on the ships includes a vessel orientation and a statement about safety compliance.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

NOAA2220 gathers PII as necessary and requested in order to facilitate the HR processes, provide continuity of medical care to injured and sick wage mariners/NOAA Corp Officers/Visitors riding NOAA vessels, and perform administrative functions such as the training and relocation of employees (Federal employees/contractors).

For HR processes and processing of mariner wages, we collect: name, work and home addresses, telephone numbers and email addresses and passport number for travel purposes. This information is collected through hiring processes, mid-term and annual evaluation periods, and awards. This information is stored on a file server and encrypted at rest

NOAA2220 collects Health Insurance Portability and Accountability Act (HIPAA) information which consist of medical information (health examination information) for OMAO employees. All of OMAO employees are federal employees; however there may be times when a LO may send a contractor to a ship for over a period of 24 hours and thus a medical evaluation will be conducted. In addition, any person becoming injured or ill on a ship would be treated, and the treatment would become part of the person's medical record. This applies to guests on the ships, also (Federal employees, contractors, members of the public).

NOAA2220 collects information only at the behest of other primary care providers and line offices. Requests for information can come from Veterans Administration, Primary Care Providers, Workforce Management or other line offices as they staff personnel for shipboard research objectives. Medical records will be shared as needed with an individual's primary care physician.

Whenever an NOAA/OMAO employee transfers to another DOC or federal agency or to a private physician, we are required to transmit those individuals' PII (Medical information and additional PII, along with a signed consent form). PII is transmitted via Accellion.

NOAA2220 collects two forms of identification (Commerce ID, Driver's license number and/or passport number) in order to issue a CAC or Alt tokens. The system also collects user-id and date-time access information for federal employees and contractors with a valid CAC cards at MOC-P and MOC-A. The form used to collect this information is DD-2841. These forms are stored on NOAA1200 on a file server once received by Local Registration Authority (LRA).

For some aircraft missions a log is hand written during the course of the mission. Comments from the crew member and or scientists are written on the log and the last name and/or name of the commenter is noted. The log is scanned and uploaded to the applicable data directory.

The crew member is typically a Commissioned Officer and or a Civil Servant. The scientist can be a federal employee/contractor, member of the public, foreign national, and or a visitor.

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov't agencies			
Public			X**
Private sector	X*		
Foreign governments			
Foreign entities			
Other (specify):			

** This only applies to the aircraft mission log. No other PII.

*To new private physician

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	-----------------------------------------------

- 6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input type="checkbox"/>	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

- 6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	X*	Government Employees	X
Contractors	X		
Other (specify):			

* This only applies to the aircraft mission log. No other PII.

Section 7: Notice and Consent

- 7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and
---	------------------------------------------------------------------------------------------------------

	discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. There is Public Health Services Privacy Act statement in the medical release form.. It is included in this PIA, just before the signature page. There is also a PAS in the hard copy policy and guidance document given to flight registrants.	
X	Yes, notice is provided by other means.	<p>Specify how: The line office provides notice to the employee/contractor on medical-related forms that have the privacy act statement included.</p> <p>Medical information is taken (by medical staff) with the sick/injured person on site and is conveyed strictly for continuity of care. This information is only available within OMAO by qualified medical personnel. A release of information form must be submitted in order for this information to be disseminated outside of the line office and signed by the individual whose information is being released.</p> <p>Performance plans provide notice as part of the forms, but no privacy act statement is included. For the PII on the aircraft log (passengers name), the Flight Director provides notice to the passengers during the preflight brief.</p> <p>For video surveillance captured onboard ships the ships personnel are notified by signs located throughout the ship that state that these premises are under video surveillance and cameras in use.</p>
	No, notice is not provided.	

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	<p>Specify how:</p> <p>A release of information form MUST be signed by the patient prior to information being released by or to OMAO. If this document is not signed, medical staff does not release the information. This medical information is used <i>only</i> to determine the level of care/intervention needed for a patient. The release is only for medical information, as stated on the privacy act statement.</p> <p>For administrative functions: Certain users (Privileged Users) may decline to provide PII info on a DD-2841 form; however, this will prevent them from receiving a Alt Token and that will prevent them from being HSPD-12 compliant. NOAA/OMAO employees may decline to provide PII information on performance evaluations.</p>
	No, individuals do not have an opportunity to decline to provide PII/BII.	

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	<p>Specify how:</p> <p>A release of information form MUST be signed by the patient prior to information being released by or to OMAO. If this document is not signed, medical staff does not release the information. This medical information is used <i>only</i> to determine the level of care/intervention needed for a patient. The release is only for medical information.</p> <p>For administrative functions: Employees are able to consent to particular uses of their PII. Whenever information is requested from an employee for a particular use within the office or bureau, their signature is required or it will not be released.</p>
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	<p>Specify how:</p> <p>Medical information is updated as new injuries/sicknesses occur to the patient. This information requires a release form to be signed by the patient in order for it to be released. All individuals are made aware of the opportunity to update PII during their employment process and at each annual, bi-annual, or every five year requirement for physicals.</p> <p>For administrative functions, individuals have an opportunity to update their information by contacting the servicing line office in writing to update/review PII pertaining to them in accordance with their guidelines. Otherwise, during each evaluation period each employee will have an opportunity to update their PII before signing their evaluation form.</p>
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. (*Check all that apply.*)

x	All users signed a confidentiality agreement or non-disclosure agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: NOAA2220 has security controls in place to audit user activities to network share drives where PII/BII is stored.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 4/24/2017 <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
x	Contractors that have access to the system are subject to information and privacy security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

NOAA2220 employs hard drive encryption for the laptops that OMAO medical staff uses to store employees PII. This encryption is FIPS 140-2 validated.

For HR information, NOAA2220 employs Virtual Local Area Networks (VLANs)*, and all data is behind firewalls for protection from outside adversaries.

* A VLAN is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).

** The web server that stores the mission logs is open to the general public. The server itself is secured, scanned, and backed up on a regular basis.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number (<i>list all that apply</i>): NOAA-10, NOAA Diving Program File; DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons, DEPT-7, Employee Accident Records, DEPT-18, Employees Information Not Covered by of Other Agencies and NOAA-22, NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSD). Also, OPM/GOVT-1, General Personnel Records, OPM-2, Employees Performance File Records apply.
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. (*Check all that apply.*)

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Management Office requires medical records be handled in accordance with (IAW) Record Schedule 311-02. When applicable all other PII is handled in accordance with NOAA and DOC record schedules: 1700, 200, 600, or other applicable Records Management Schedules. NOAA2220 relies on the servicing staff office to maintain these documents in accordance with the NOAA defined records schedule.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. (*Check all that apply.*)

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X
Other (specify): When a NOAA2220/OMAO medical staff employee departs and returns their laptop to NOAA2220 IT staff the machine is sanitized in accordance with NIST SP 800-88 requirements. The same is conducted for servers within the NOAA2220 boundary that stores HR information on employees.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels.
(Check all that apply.)

x	Identifiability	Provide explanation: The information directly identifies a large amount of individuals using names, phone numbers, address, HIPAA information. For the aircraft mission logs the PII is a scanned copy of hand written flight-log which contains a historical details about the flight-mission which includes the (passengers names) that where on the flight but no other PII.
x	Quantity of PII	Provide explanation: There is a significant amount of PII.
x	Data Field Sensitivity	Provide explanation: There is sensitive data entered in the system is entered on forms and is stored in a secure manner, accessible by only approved individuals and saved in .pdf form to limit any alteration.
x	Context of Use	Provide explanation: The release of this information could cause moderate harm to the individuals due to the sensitivity of the PII being collected and in some case released. For the aircraft mission logs, the information is accessible to the public and the release of the information, modification of the content and denial of availability would have no adverse effect on organizational operations, organizational assets, or individuals.
x	Obligation to Protect Confidentiality	Provide explanation: NOAA2220 is obligated under the Health Insurance Portability and Accountability Act (HPAA) to protect the confidentiality of the PII is process, stores, or transmits and does so by encrypting data at rest and using access controls.
x	Access to and Location of PII	Provide explanation: The information is accessed by Medical staff and Supervisors only with the need to know. Although in some cases the medical staff and supervisor may have laptops they don't store any PII on them and in the case that they may all laptops are encrypted.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: We are reevaluating what PII we collect for new employees and employee evaluations. For example, SSN is no longer collected on any forms that are stored, processed, and transmitted within NOAA2220. Also a Privacy Act Statement has been added to the policy and guidance given to flight registrants.
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

National Oceanic and Atmospheric Administration

U.S. Public Health Service

PRIVACY ACT STATEMENT FOR CLIENTS

Authorities: Privacy Act of 1974, 5 CFR Part 293, Personnel Records and Part 297, Privacy Procedures for Personnel Records; Occupational Safety and Health Administration, 29 CFR 1910 Occupational Safety and Health Standards, Health Insurance Portability and Accountability Act, Pub. L. 104-191.

Purposes: The health services you receive through this program result in the gathering and recording of information that is personal and confidential. Your employing agency serves as a custodian of your records. Upon termination of employment the original documents or copies of your records will be transferred to your Employee Medical Folder (EMF) in the agency's Employee Medical File System (EMFS). These records are stored as a distinct and separate part of your Official Personnel Folder. **Your records are collected and maintained for a variety of purposes, including:**

- (a) to meet the mandates of law, Executive order, or regulations;
- (b) to provide data necessary for proper medical evaluations, treatment for the continuity of medical care;
- (c) to provide an accurate medical history and treatment and/or hazard exposures and health monitoring;
- (d) to enable the planning for further care;
- (e) to provide a record of communications among members of the health care team;
- (f) to provide a legal document describing the health care administered and exposure incidents;
- (g) to provide a method of evaluating the quality of health care rendered as required by professional standards and legislative authority;
- (h) to ensure that all relevant, necessary, accurate, and timely data are available to support any medically-related employment decisions;
- (i) to document claims filed with and the decisions reached in OWCP cases;
- (j) to document employee's reporting of occupational injuries, unhealthy and/or unsafe working conditions;
- (k) to ensure proper and accurate operation of the agency's employee drug testing program under Executive Order 12564.

Routine Uses:

Information is collected to manage medical care and to maintain accurate and current medical records on employees. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a), to be shared with applicable entities related to the purposes described above. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice, [COMMERCE/NOAA-22](#), NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSD).

Disclosure: Collection of this information is voluntary. If you do not wish to participate in these services, or to provide the requested information, you are not required to do so. However, if you decline the health services required for job-related clearances, the absence of documented medical clearances will impact your employer's authority to permit you to perform certain functions of your position. You should consult with your supervisor in this matter.

Employee Signature

Date

Points of Contact and Signatures

<p>Information System Security Officer or System Owner Name: Sean T. McMillan, ISSO Office: OMAO Phone: 863-500-3924 Email: sean.t.mcmillan@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: center;">MCMILLAN.SE Digitally signed by MCMILLAN.SEAN.T.11858 14382 Date: 2018.01.31 12:54:11 05'00'</p> <p>Signature: AN.T.1185814 382 Date signed:</p>	<p>Information Technology Security Officer Name: LCDR James Jones IV Office: OMAO Phone: 301-713-7663 Email: james.jones@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: center;">JONES.JAMES.IV Digitally signed by JONES.JAMES.IV.1049453465 Date: 2018.01.29 12:16:00 05'00'</p> <p>Signature: V.1049453465 Date signed:</p>
<p>Authorizing Official Name: CDR Joseph Baczkowski Office: OMAO Phone: 240-393-0905 Email: joseph.baczkowski@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: center;">BACZKOWSKI Digitally signed by BACZKOWSKI.JOSEPH.PADES.1167 987300 DN: c US, o U.S. Government, ou DoD, ou PKI, ou USPHS, cn BACZKOWSKI.JOSEPH.PADES.1 167987300 Date: 2018.02.06 16:51:28 -05'00'</p> <p>Signature: JOSEPH.PADES.1167987300 Date signed:</p>	<p>Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p style="text-align: center;">GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447 892 Date: 2018.02.07 11:10:43 -05'00'</p> <p>Signature: HYRUM.1514447892 Date signed: 47892</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Wednesday, February 7, 2018 11:22 AM
To: Gioffre, Kathy (Federal); CPO
Cc: Mark Graff NOAA Federal; Sean Mcmillan NOAA Federal; James Jones NOAA Affiliate
Subject: NOAA2220 PIA and PTA for certification; re sending certification so all in one email
Attachments: NOAA2220 PTA_01_23_2018_final_v2_requires_signatures_itso_isso_AO mhg.pdf; NOAA2220 Annual Review Certification Form _BCPO signature required mhg.pdf; NOAA2220_PIA_020718 for MHG signature mhg.pdf

Kathy, please see the attached. No changes to PIA except the ATO date and changing "new privacy risks" to "no new privacy risks".

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: Ships Fleet Support System (SFSS) NOAA2220

FISMA Name/ID (if different): NOAA2220

Name of IT System/ Program Owner: CDR Ieshia k. Jones

Name of Information System Security Officer: Sean T. McMillan

Name of Authorizing Official(s): CDR Joseph Baczkowski

Date of Last PIA Compliance Review Board (CRB): 15 April 2017
(This date must be within three (3) years.)

Date of PIA Review: 24 January 2018

Name of Reviewer: Sean T. McMillan, ISSO

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: MCMILLAN.SEAN.T.1185814382 Digitally signed by MCMILLAN.SEAN.T.1185814382
Date: 2018.01.24 13:53:11 05'00'

Date of Privacy Act (PA) Review: 1/24/2018

Name of Reviewer: Sarah Brabson

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Digitally signed by BRABSON SARAH 1365710488
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER,
cn=BRABSON SARAH 1365710488
Date: 2018.02.02 10:31:29 05'00'

Date of BCPO Review: 2/6/18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark H. Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: GRAFF.MARK.HYRU M.1514447892

Digitally signed by GRAFF MARK HYRUM 1514447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=OTHER, cn=GRAFF MARK HYRUM 1514447892
Date: 2018.02.06 17:01:38 -0500

**U.S. Department of Commerce
NOAA**



**Privacy Threshold Analysis
for the
Ships Fleet Support System (SFSS) NOAA2220**

**U.S. Department of Commerce Privacy Threshold Analysis
NOAA Ship Fleet Support System**

Unique Project Identifier: 006-48-01-15-02-3601-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *NOAA2220 is an amalgamation of sixteen ships with similar general functions and operating characteristics, security needs, and operating environments. Common functions of all of the ship backbone subsystems are to provide network connectivity, domain authentication, internet connectivity and general business support services. While each ship has common (or class similar) configurations, mission requirements require each to have a unique configuration.*

The NOAA fleet of ships are managed, operated and maintained by NOAA's Office of Marine and Aviation Operations (OMAO), Marine operations centers (MOC), located in Norfolk, Virginia and Newport, Oregon. Additional ship specific support is provided through port office facilities in Woods Hole, Massachusetts; Charleston, South Carolina; Pascagoula, Mississippi; Davisville RI, and Ford Island, Hawaii. Ships are also maintained pier side in Newport, RI and Kodiak, Alaska.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

 This is a new information system. *Continue to answer questions and complete certification.*

 This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

 X This is an existing information system in which changes do not create new privacy risks. *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

 X Yes. *Please describe the activities which may raise privacy concerns.*

- NOAA2220 ships have a Closed Circuit Television (CCTV) system that is used to record video throughout the ship for the purpose of safety. Ships personnel are notified by signs located throughout the ship that state that these premises are under video surveillance and cameras in use.
- NOAA2220 Aircraft record Crew Members and Scientific Partners names that participate in the flight and publish those names on the internet with the data for the flight in which they participated in.

 No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.).”

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

X No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

 X I certify the criteria implied by one or more of the questions above **apply** to the Ship Fleet Support System and as a consequence of this applicability, I will perform and document a PIA for this IT system.

 I certify the criteria implied by the questions above **do not apply** to the Ships Fleet Support System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Sean T. McMillan

Signature of ISSO or SO: MCMILLAN.SEAN.T. 1185814382 Digitally signed by MCMILLAN.SEAN.T.1185814382 Date: 2018.01.31 12:52:47 -05'00' Date: 24 Jan 2018

Name of Information Technology Security Officer (ITSO): James Jones IV, LCDR, USPHS

Signature of ITSO: JONES.JAMES.IV.1049453465 Digitally signed by JONES.JAMES.IV.1049453465 Date: 2018.01.29 12:16:39 -05'00' Date: _____

Name of Authorizing Official (AO): Joseph Baczkowski, CDR, USPHS

Signature of AO: BACZKOWSKI.JOSEPH.PADES.1167987300 Digitally signed by BACZKOWSKI.JOSEPH.PADES.1167987300 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USPHS, cn=BACZKOWSKI.JOSEPH.PADES.1167987300 Date: 2018.02.06 16:52:33 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): MARK GRAFF

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.02.07 11:02:05'00' Date: _____

**U.S. Department of Commerce
National Oceanographic and Atmospheric
Administration (NOAA)**



**Privacy Impact Assessment
for the
NOAA Ship Fleet Support System (NOAA2220)**

Reviewed by: _____, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment

NOAA OMAO Ship Fleet Support System

Unique Project Identifier: 006-48-01-15-02-3601-00

Introduction: System Description

The NOAA2220 System consists of ships, aircraft and land based ground support systems. Many of these systems have similar general functions and operating characteristics, security needs, and operating environments, and shore-based applications that support the ship missions. Common shipboard IT infrastructure functions include network connectivity, domain authentication, internet connectivity, and general business support services, such as file and print services. Ships are configured with satellite communication systems, such as Inmarsat and VSAT, and connect to NOAA networks and the internet via contract satellite service providers. While each ship has common (or class similar) configurations, mission requirements require each to have a unique configuration. To facilitate their inclusion in a consolidated System Security Plan (SSP), each ship and subsystem is described in the System Security Plan.

The NOAA fleet of ships are managed, operated and maintained by NOAA's Office of Marine and Aviation Operations (OMAO), Marine operations centers (MOCs), located in Norfolk, Virginia; Honolulu, Hawaii; and Newport, Oregon. Additional ship-specific support is provided through port office facilities in Woods Hole, Massachusetts; Davisville, Rhode Island; Charleston, South Carolina; Pascagoula, Mississippi; San Diego, California; and Ford Island, Hawaii. Limited pier-side support is also provided to ships in Newport, Rhode Island and Kodiak, Alaska.

Typical PII transactions in the NOAA2220 system consist of transmitting information to and from NOAA Workforce Management Office, to facilitate Human Resources (HR) processes, processing of benefits for wage mariners, and continuation of medical care for sick and injured mariners, and as required by other government agencies and industry.

For HR processes and processing of wages, NOAA2220 collects: name, work and home addresses, telephone numbers and email addresses; and passport number for travel purposes. This data is secured through physical controls for facilities and encryption at rest for soft copies.

Currently NOAA2220 stores Health Insurance Portability and Accountability Act (HIPAA) information in a secure manner at Marine Operation Center-Atlantic (MOC-A), Marine Operation Center Pacific (MOC-P), and HQ: hard copies are secured by physical controls implemented at each facility that meets NIST SP 800-53 rev.4 requirements; and soft copies data is encrypted at rest. The HIPAA information consists of medical information for NOAA employees and guests who sail on a NOAA vessel, as well as for contractors who will be on board for more than 24 hours. This information is transmitted as needed via secure means by Accellion, secure e-mail, or fax (with notification to the recipient so he/she will be standing at

the fax machine). There are multiple medical officers who share responsibility for collecting and transmitting HIPAA information. Any medical officer who has this responsibility is trained and aware of how to handle such information.

NOAA2220 collects two forms of identification (Commerce ID, Driver's license number and/or passport number) in order to issue a CAC or Alt tokens. The system also collects user-id and date-time access information for federal employees and contractors with a valid CAC cards at MOC-P and MOC-A. The form used to collect this information is DD-2841. These forms are stored on NOAA1200 on a file server once received by Local Registration Authority (LRA).

Information is shared on an as-needed basis after both authorization and need to know have been determined. Most information that needs to be shared is collected and sent to the NOAA Workforce Management Office for dissemination. There are some instances where NOAA employees' PII will be sent to other Department of Commerce (DOC) agencies and to other federal agencies if the employees are detailed temporary or permanently.

The Aircraft Fleet Support System (AFSS) includes two primary networking segments, the Aircraft Computing Systems (ACS) and the Ground-based Support Network (GSN), and an alternate site located at the National Weather Service Facility in Ruskin, FL. These segments provide critical services during mission operations. The alternate site provides critical application and storage redundancy.

The network segment that encompasses the NOAA aircraft fleet is identified as the AFSS Aircraft Computing Systems (AFSS/ACS). All aircraft have common IT functions that can provide network connectivity, Internet connectivity, and general business support services. In addition to common IT functions, each aircraft is required to support scientific data collection and distribution of data to onboard systems and to ground-based systems during flight. The IT equipment and network configurations on the aircraft are unique due to the regularly changing project and mission requirements.

The ground-based network segment is identified as the AFSS Ground Support Network (AFSS/GSN). The GSN is a multi-segmented system that uses a single firewall/gateway device to apply a separation of network resources that restricts access to and from internal resources and public servers. The GSN permits public access to organizational web servers and FTP servers, supports ACS-to-ground data-flow applications, and hosts data processing and development systems.

The aircraft collect various raw data through a suite of sensors outside the aircraft and in expendable drop sensors. Certain data points are immediately transmitted from the aircraft to the ground stations, while the remaining raw data set is stored on the aircraft until it returns to ground. At the end of the mission the entire data set is transferred to ground servers for processing.

The raw data set is publically available on the public web server. Pertinent data set is directly transmitted to the National Weather Service telecommunication gateway while the aircraft are on mission and in the air.

Legal authorities to collect PII and/or BII:

NOAA2220's legal authorities to collect PII are:

Title 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.C. 3101, 3309, Title 29 U.S.C 651-78, Title 28 U.S.C. 2671-2680, Executive Order 12196, Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966, Title 33 U.S.C. 853i; 853j; 853j-1; 853t; 854; 854a-1; 857-5, 857a, 855, Title 37 U.S.C; Executive Order 10450, Title 16 U.S.C. 143, and Executive Order 11222.

NOAA2200 is a FIPS 199 moderate level system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

This is a new information system.

This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging	X*	g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

This is an existing system with no changes that create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (Check all that apply.)

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License	x	j. Financial Account	
c. Employer ID	x	g. Passport	x	k. Financial Transaction	
d. Employee ID	x	h. Alien Registration		l. Vehicle Identifier	

m. Other identifying numbers (specify): HR and Medical Files/Records are stored in NOAA2220 on file servers that have least-privilege functions enforced on them and only authorized personnel can view them; and these records are transmitted via fax or Accellion to service entities. DOB, HIPAA information, and other PII are collected only when needed by the requesting staff office in order to provide continuity of care, maintain official records (personnel records/officer records), and HR Processes including hiring, travel and performance appraisals.

General Personal Data (GPD)

a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name	X	h. Place of Birth	X	n. Financial Information	
c. Alias	X	i. Home Address	X	o. Medical Information	X
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education	X	r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)

a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Medical records regarding injuries and sickness acquired while underway as necessary to facilitate care when at sea and ashore.					

Distinguishing Features/Biometrics (DFB)

a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)

a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

--

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify) Sometimes we have NOAA employees who transfer within DOC to other offices such as DOC Office of the Inspector General (OIG) and we are required to transfer PII information. Whenever PII is transmitted to DOC or other federal agencies, it is done via fax or Accellion.					

Non-government Sources					
Public Organizations		Private Sector	X*	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

*Private medical office

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)					
Smart Cards				Biometrics	
Caller-ID				Personal Identity Verification (PIV) Cards	
Other (specify):					

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
---	----------------------------------------------------------------------------------------------------------

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities					
Audio recordings				Building entry readers	
Video surveillance	X*			Electronic purchase transactions	

Other (specify):

*NOAA2220 ships have a Closed Circuit Television (CCTV) system that is used to record video throughout the ship for the purpose of safety. Ships’ personnel are notified by signs located throughout the ship that state that these premises are under video surveillance and cameras in use. Least privileges are enforced for access to the video surveillance data. Only authorized personnel will have access. The NOAA2220 System Owner will be responsible for granting access and controlling who has access to this information. The orientation packet given to those traveling on the ships includes a vessel orientation and a statement about safety compliance.

There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Medical care NOAA2220 ships have a Closed Circuit Television (CCTV) system that is used to record video throughout the ship for the purpose of safety. The orientation packet given to those traveling on the ships includes a vessel orientation and a statement about safety compliance.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

NOAA2220 gathers PII as necessary and requested in order to facilitate the HR processes, provide continuity of medical care to injured and sick wage mariners/NOAA Corp Officers/Visitors riding NOAA vessels, and perform administrative functions such as the training and relocation of employees (Federal employees/contractors).

For HR processes and processing of mariner wages, we collect: name, work and home addresses, telephone numbers and email addresses and passport number for travel purposes. This information is collected through hiring processes, mid-term and annual evaluation periods, and awards. This information is stored on a file server and encrypted at rest

NOAA2220 collects Health Insurance Portability and Accountability Act (HIPAA) information which consist of medical information (health examination information) for OMAO employees. All of OMAO employees are federal employees; however there may be times when a LO may send a contractor to a ship for over a period of 24 hours and thus a medical evaluation will be conducted. In addition, any person becoming injured or ill on a ship would be treated, and the treatment would become part of the person's medical record. This applies to guests on the ships, also (Federal employees, contractors, members of the public).

NOAA2220 collects information only at the behest of other primary care providers and line offices. Requests for information can come from Veterans Administration, Primary Care Providers, Workforce Management or other line offices as they staff personnel for shipboard research objectives. Medical records will be shared as needed with an individual's primary care physician.

Whenever an NOAA/OMAO employee transfers to another DOC or federal agency or to a private physician, we are required to transmit those individuals' PII (Medical information and additional PII, along with a signed consent form). PII is transmitted via Accellion.

NOAA2220 collects two forms of identification (Commerce ID, Driver's license number and/or passport number) in order to issue a CAC or Alt tokens. The system also collects user-id and date-time access information for federal employees and contractors with a valid CAC cards at MOC-P and MOC-A. The form used to collect this information is DD-2841. These forms are stored on NOAA1200 on a file server once received by Local Registration Authority (LRA).

For some aircraft missions a log is hand written during the course of the mission. Comments from the crew member and or scientists are written on the log and the last name and/or name of the commenter is noted. The log is scanned and uploaded to the applicable data directory.

The crew member is typically a Commissioned Officer and or a Civil Servant. The scientist can be a federal employee/contractor, member of the public, foreign national, and or a visitor.

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov't agencies			
Public			X**
Private sector	X*		
Foreign governments			
Foreign entities			
Other (specify):			

** This only applies to the aircraft mission log. No other PII.

*To new private physician

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	-----------------------------------------------

- 6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input type="checkbox"/>	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

- 6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	X*	Government Employees	X
Contractors	X		
Other (specify):			

* This only applies to the aircraft mission log. No other PII.

Section 7: Notice and Consent

- 7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and
---	------------------------------------------------------------------------------------------------------

	discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. There is Public Health Services Privacy Act statement in the medical release form.. It is included in this PIA, just before the signature page. There is also a PAS in the hard copy policy and guidance document given to flight registrants.	
X	Yes, notice is provided by other means.	<p>Specify how: The line office provides notice to the employee/contractor on medical-related forms that have the privacy act statement included.</p> <p>Medical information is taken (by medical staff) with the sick/injured person on site and is conveyed strictly for continuity of care. This information is only available within OMAO by qualified medical personnel. A release of information form must be submitted in order for this information to be disseminated outside of the line office and signed by the individual whose information is being released.</p> <p>Performance plans provide notice as part of the forms, but no privacy act statement is included. For the PII on the aircraft log (passengers name), the Flight Director provides notice to the passengers during the preflight brief.</p> <p>For video surveillance captured onboard ships the ships personnel are notified by signs located throughout the ship that state that these premises are under video surveillance and cameras in use.</p>
	No, notice is not provided.	

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	<p>Specify how:</p> <p>A release of information form MUST be signed by the patient prior to information being released by or to OMAO. If this document is not signed, medical staff does not release the information. This medical information is used <i>only</i> to determine the level of care/intervention needed for a patient. The release is only for medical information, as stated on the privacy act statement.</p> <p>For administrative functions: Certain users (Privileged Users) may decline to provide PII info on a DD-2841 form; however, this will prevent them from receiving a Alt Token and that will prevent them from being HSPD-12 compliant. NOAA/OMAO employees may decline to provide PII information on performance evaluations.</p>
	No, individuals do not have an opportunity to decline to provide PII/BII.	

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	<p>Specify how:</p> <p>A release of information form MUST be signed by the patient prior to information being released by or to OMAO. If this document is not signed, medical staff does not release the information. This medical information is used <i>only</i> to determine the level of care/intervention needed for a patient. The release is only for medical information.</p> <p>For administrative functions: Employees are able to consent to particular uses of their PII. Whenever information is requested from an employee for a particular use within the office or bureau, their signature is required or it will not be released.</p>
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	<p>Specify how:</p> <p>Medical information is updated as new injuries/sicknesses occur to the patient. This information requires a release form to be signed by the patient in order for it to be released. All individuals are made aware of the opportunity to update PII during their employment process and at each annual, bi-annual, or every five year requirement for physicals.</p> <p>For administrative functions, individuals have an opportunity to update their information by contacting the servicing line office in writing to update/review PII pertaining to them in accordance with their guidelines. Otherwise, during each evaluation period each employee will have an opportunity to update their PII before signing their evaluation form.</p>
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. (*Check all that apply.*)

x	All users signed a confidentiality agreement or non-disclosure agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: NOAA2220 has security controls in place to audit user activities to network share drives where PII/BII is stored.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 4/24/2017 <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
x	Contractors that have access to the system are subject to information and privacy security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

NOAA2220 employs hard drive encryption for the laptops that OMAO medical staff uses to store employees PII. This encryption is FIPS 140-2 validated.

For HR information, NOAA2220 employs Virtual Local Area Networks (VLANs)*, and all data is behind firewalls for protection from outside adversaries.

* A VLAN is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).

** The web server that stores the mission logs is open to the general public. The server itself is secured, scanned, and backed up on a regular basis.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number (<i>list all that apply</i>): NOAA-10, NOAA Diving Program File; DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons, DEPT-7, Employee Accident Records, DEPT-18, Employees Information Not Covered by of Other Agencies and NOAA-22, NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSD). Also, OPM/GOVT-1, General Personnel Records, OPM-2, Employees Performance File Records apply.
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. (*Check all that apply.*)

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Management Office requires medical records be handled in accordance with (IAW) Record Schedule 311-02. When applicable all other PII is handled in accordance with NOAA and DOC record schedules: 1700, 200, 600, or other applicable Records Management Schedules. NOAA2220 relies on the servicing staff office to maintain these documents in accordance with the NOAA defined records schedule.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. (*Check all that apply.*)

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X
Other (specify): When a NOAA2220/OMAO medical staff employee departs and returns their laptop to NOAA2220 IT staff the machine is sanitized in accordance with NIST SP 800-88 requirements. The same is conducted for servers within the NOAA2220 boundary that stores HR information on employees.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels.
(Check all that apply.)

x	Identifiability	Provide explanation: The information directly identifies a large amount of individuals using names, phone numbers, address, HIPAA information. For the aircraft mission logs the PII is a scanned copy of hand written flight-log which contains a historical details about the flight-mission which includes the (passengers names) that where on the flight but no other PII.
x	Quantity of PII	Provide explanation: There is a significant amount of PII.
x	Data Field Sensitivity	Provide explanation: There is sensitive data entered in the system is entered on forms and is stored in a secure manner, accessible by only approved individuals and saved in .pdf form to limit any alteration.
x	Context of Use	Provide explanation: The release of this information could cause moderate harm to the individuals due to the sensitivity of the PII being collected and in some case released. For the aircraft mission logs, the information is accessible to the public and the release of the information, modification of the content and denial of availability would have no adverse effect on organizational operations, organizational assets, or individuals.
x	Obligation to Protect Confidentiality	Provide explanation: NOAA2220 is obligated under the Health Insurance Portability and Accountability Act (HPAA) to protect the confidentiality of the PII is process, stores, or transmits and does so by encrypting data at rest and using access controls.
x	Access to and Location of PII	Provide explanation: The information is accessed by Medical staff and Supervisors only with the need to know. Although in some cases the medical staff and supervisor may have laptops they don't store any PII on them and in the case that they may all laptops are encrypted.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: We are reevaluating what PII we collect for new employees and employee evaluations. For example, SSN is no longer collected on any forms that are stored, processed, and transmitted within NOAA2220. Also a Privacy Act Statement has been added to the policy and guidance given to flight registrants.
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

National Oceanic and Atmospheric Administration

U.S. Public Health Service

PRIVACY ACT STATEMENT FOR CLIENTS

Authorities: Privacy Act of 1974, 5 CFR Part 293, Personnel Records and Part 297, Privacy Procedures for Personnel Records; Occupational Safety and Health Administration, 29 CFR 1910 Occupational Safety and Health Standards, Health Insurance Portability and Accountability Act, Pub. L. 104-191.

Purposes: The health services you receive through this program result in the gathering and recording of information that is personal and confidential. Your employing agency serves as a custodian of your records. Upon termination of employment the original documents or copies of your records will be transferred to your Employee Medical Folder (EMF) in the agency's Employee Medical File System (EMFS). These records are stored as a distinct and separate part of your Official Personnel Folder. **Your records are collected and maintained for a variety of purposes, including:**

- (a) to meet the mandates of law, Executive order, or regulations;
- (b) to provide data necessary for proper medical evaluations, treatment for the continuity of medical care;
- (c) to provide an accurate medical history and treatment and/or hazard exposures and health monitoring;
- (d) to enable the planning for further care;
- (e) to provide a record of communications among members of the health care team;
- (f) to provide a legal document describing the health care administered and exposure incidents;
- (g) to provide a method of evaluating the quality of health care rendered as required by professional standards and legislative authority;
- (h) to ensure that all relevant, necessary, accurate, and timely data are available to support any medically-related employment decisions;
- (i) to document claims filed with and the decisions reached in OWCP cases;
- (j) to document employee's reporting of occupational injuries, unhealthy and/or unsafe working conditions;
- (k) to ensure proper and accurate operation of the agency's employee drug testing program under Executive Order 12564.

Routine Uses:

Information is collected to manage medical care and to maintain accurate and current medical records on employees. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a), to be shared with applicable entities related to the purposes described above. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice, [COMMERCE/NOAA-22](#), NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSD).

Disclosure: Collection of this information is voluntary. If you do not wish to participate in these services, or to provide the requested information, you are not required to do so. However, if you decline the health services required for job-related clearances, the absence of documented medical clearances will impact your employer's authority to permit you to perform certain functions of your position. You should consult with your supervisor in this matter.

Employee Signature

Date

Points of Contact and Signatures

<p>Information System Security Officer or System Owner Name: Sean T. McMillan, ISSO Office: OMAO Phone: 863-500-3924 Email: sean.t.mcmillan@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: center;">MCMILLAN.SE Digitally signed by MCMILLAN.SEAN.T.11858 14382 Date: 2018.01.31 12:54:11 05'00'</p> <p>Signature: AN.T.1185814 382 Date signed:</p>	<p>Information Technology Security Officer Name: LCDR James Jones IV Office: OMAO Phone: 301-713-7663 Email: james.jones@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: center;">JONES.JAMES.IV Digitally signed by JONES.JAMES.IV.1049453465 Date: 2018.01.29 12:16:00 05'00'</p> <p>Signature: V.1049453465 Date signed:</p>
<p>Authorizing Official Name: CDR Joseph Baczkowski Office: OMAO Phone: 240-393-0905 Email: joseph.baczkowski@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: center;">BACZKOWSKI Digitally signed by BACZKOWSKI.JOSEPH.PADES.1167 987300 DN: c US, o U.S. Government, ou DoD, ou PKI, ou USPHS, cn BACZKOWSKI.JOSEPH.PADES.1 167987300 Date: 2018.02.06 16:51:28 -05'00'</p> <p>Signature: JOSEPH.PADES.1167987300 Date signed:</p>	<p>Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p style="text-align: center;">GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447 892 Date: 2018.02.07 11:10:43 -05'00'</p> <p>Signature: HYRUM.1514447892 Date signed: 47892</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

Mark Graff - NOAA Federal

From: Mark Graff NOAA Federal
Sent: Wednesday, February 7, 2018 2:13 PM
To: Robert Swisher NOAA Federal; Ed Kearns NOAA Federal; Dennis Morgan NOAA Federal
Cc: Eric Williams NOAA Affiliate; Sarah Brabson NOAA Federal
Subject: Draft Monthly Privacy Report
Attachments: SORN_DEPT 29_draft_(2017 07 03) mhg.docx; DOC SORN Status Sheet_NOAA as of 020618.xlsx; PTA PIA Management Report (18).xlsx

Hey Guys,

Can you guys take a look below and let me know if the monthly Privacy report is good to send out?

Good Afternoon,

This is a report regarding the activities of the NOAA Privacy Program from January 1-January 31, 2017. Attached are two spreadsheets outlining the status of SORNs, PIAs, and PTAs within NOAA.

Some of highlights of the Program's activities for the month include:

- DOC has submitted COMMERCE/DEPT-29 SORN, Unmanned Aircraft Systems, to the *Federal Register* for publication, authorizing certain collection, storage, and retrieval of PII through the use of Unmanned Aircraft. The SORN will be published within two business days, and has been highly anticipated within OMAO and NOS. A copy of the draft SORN is attached for your reference.
- DOC reiterated at the Privacy Council that all Bureaus are required to submit their PIA documentation within 60 days of the scheduled ATO date in order to have a CRB scheduled in time. Please coordinate the PIA preparation time within the existing A&A process so that a finalized PIA can be submitted to the Department by this time. In instances where new PII is discovered on a system, or there is change impacting privacy, such as merger or new PII dataset within the FISMA System Accreditation boundaries within this time window, an expedited review request, signed by the NOAA CIO, can be submitted.

NOAA, along with OIG, BIS, and OIS, presented the parameters for the DOC Privacy Incident Tabletop Exercise (TTX) during the Quarterly Privacy Council. This exercise will test the compliance of all DOC bureaus on incident response under the DOC Breach Response Notification Plan. In the coming two weeks, DOC will issue a request for volunteers to participate in the Privacy TTX and outline the parameters of the exercise simulating a "High" incident response scenario. The DOC Response Team, consisting of DOC Senior Management, will be assembled by DOC/OPOG to receive and review the TTX responses by the bureaus and carry out their roles as they would have in a legitimate major Privacy Incident.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

STATUS OF NOAA SYSTEMS OF RECORD NOTICES (SORN)

SORN	Title/Purpose	Date SORN Previously Published	Date Sent to DOC
NOAA 1	Applications for NOAA Corps	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 3	Commissioned Officer Official Personnel Folders	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 5	Fisheries Law Enforcement Cases (Address Update)	8/10/2007 (72 FR 45009)	5/30/2013

NOAA 6	Fishermen's Statistical Data	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 10	NOAA Diving Program	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 11	Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.	NA	5/30/2013
NOAA 12	Marine Mammals, Endangered and Threatened Species, Permits and Exemptions (Amendment)	8/10/2007 (72 FR 45009)	2008
NOAA 13	Records of the Regional Fishery Management Councils	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 14	Dr. Nancy Foster Scholarship Program	2005	8/22/2014
NOAA 15	Observation Privacy Act System of Records Notice 2	10/17/2002 (67 FR 64086)	5/30/2013
NOAA 16	Economic Data Reports for Alaska Federally Regulated Fisheries off the coast of Alaska (first published as Crab Economic Data Report for Bering Sea/Aleutian Islands Management Area (BSAI) off the coast of Alaska, now including two newer economic data report collections)	3 3 2005 (70 FR 10360)	5/30/2013

NOAA 19	Permits and Registrations for United States Federally Regulated Fisheries	4 17 2008/73 FR 20914	5/30/2013
NOAA 20	SARSAT	4 17 2008/73 FR 20914	5/5/2016
NEW NOAA 21	Fisheries Finance Program	NA	2008
NEW NOAA 22	NOAA Health Service Questionnaire	NA	2008
NEW NOAA 23	West Coast Region Economic Data Reports	NA	12/23/2014

TOTAL: 16

2015-16 status at DOC
Published 11/25/15; effective 1/19/16
Published 5/5/16; effective 6/14/16
Added missing info and returned to DOC 3 8 16. 4 13 16, DOC decided that it should be a complete update. OLE completed updates 6 16 16; I cleaned up and sent 2 outstanding minor questions, 6 17 16. At one time it had been thought to separate out GC files into another SORN, but it was decided not to. To DOC 6 20 16. Responded to edits and comments rec'd 6 29 16, on 6 30 16, and added the new volunteer routine use. 6 30 17: now at Assistant General Counsel for Legislation, Regulation, and Oversight

MHG completed review 5 22 17; few edits, added volunteer routine use and put in new template, 5 25 17; sent to DOC same day. In new template to DOC 10 14 17
To DOC 12 13 16
Published 10/9/15; effective 11/23/15. Second amended version published 1-12-17. Another amended version to OPOG 6 26 17
Published July 8, 2016. Became effective August 17, 2016.
Published 9/17/15; effective 10/28/15
Published 7/31/2014; effective 09/02/2014
Published 10/9/15; effective 11/23/15

Published 8/7/2015. effective 9/15/15
Amended SORN published 1-12-17
Published July 8, 2016. Became effective August 17, 2016.
Published 1/19/16; effective 3/1/2016
Published 8-7-15; effective 9/15/15

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Dennis Morgan - NOAA Federal

From: Dennis Morgan NOAA Federal
Sent: Wednesday, February 7, 2018 4:12 PM
To: Mark Graff NOAA Federal; Sarah Brabson NOAA Federal
Cc: Robert Swisher NOAA Federal; Ed Kearns NOAA Federal; Eric Williams NOAA Affiliate
Subject: Re: Draft Monthly Privacy Report
Attachments: SORN_DEPT 29_draft_(2017 07 03) mhg.docx; DOC SORN Status Sheet_NOAA as of 020618.xlsx; PTA PIA Management Report (18).xlsx

Mark: Looks good to me.

Sarah: Any criticism to offer?

On Wed, Feb 7, 2018 at 2:12 PM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:

Hey Guys,

Can you guys take a look below and let me know if the monthly Privacy report is good to send out?

Good Afternoon,

This is a report regarding the activities of the NOAA Privacy Program from January 1-January 31, 2017. Attached are two spreadsheets outlining the status of SORNs, PIAs, and PTAs within NOAA.

Some of highlights of the Program's activities for the month include:

- DOC has submitted COMMERCE/DEPT-29 SORN, Unmanned Aircraft Systems, to the *Federal Register* for publication, authorizing certain collection, storage, and retrieval of PII through the use of Unmanned Aircraft. The SORN will be published within two business days, and has been highly anticipated within OMAO and NOS. A copy of the draft SORN is attached for your reference.
- DOC reiterated at the Privacy Council that all Bureaus are required to submit their PIA documentation within 60 days of the scheduled ATO date in order to have a CRB scheduled in time. Please coordinate the PIA preparation time within the existing A&A process so that a finalized PIA can be submitted to the Department by this time. In instances where new PII is discovered on a system, or there is change impacting privacy, such as merger or new PII dataset within the FISMA System Accreditation boundaries within this time window, an expedited review request, signed by the NOAA CIO, can be submitted.

NOAA, along with OIG, BIS, and OIS, presented the parameters for the DOC Privacy Incident Tabletop Exercise (TTX) during the Quarterly Privacy Council. This exercise will test the compliance of all DOC bureaus on incident response under the DOC Breach Response Notification Plan. In the coming two weeks, DOC will issue a request for volunteers to participate in the Privacy TTX and outline the parameters of the exercise simulating a "High" incident response scenario. The DOC Response Team, consisting of DOC Senior Management, will be assembled by DOC/OPOG to receive and review the TTX responses by the bureaus and carry out their roles as they would have in a legitimate major Privacy Incident.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration

[\(301\) 628 5658](tel:(301)6285658) (O)

(b)(6) (C)

attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

STATUS OF NOAA SYSTEMS OF RECORD NOTICES (SORN)

SORN	Title/Purpose	Date SORN Previously Published	Date Sent to DOC
NOAA 1	Applications for NOAA Corps	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 3	Commissioned Officer Official Personnel Folders	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 5	Fisheries Law Enforcement Cases (Address Update)	8/10/2007 (72 FR 45009)	5/30/2013

NOAA 6	Fishermen's Statistical Data	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 10	NOAA Diving Program	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 11	Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.	NA	5/30/2013
NOAA 12	Marine Mammals, Endangered and Threatened Species, Permits and Exemptions (Amendment)	8/10/2007 (72 FR 45009)	2008
NOAA 13	Records of the Regional Fishery Management Councils	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 14	Dr. Nancy Foster Scholarship Program	2005	8/22/2014
NOAA 15	Observation Privacy Act System of Records Notice 2	10/17/2002 (67 FR 64086)	5/30/2013
NOAA 16	Economic Data Reports for Alaska Federally Regulated Fisheries off the coast of Alaska (first published as Crab Economic Data Report for Bering Sea/Aleutian Islands Management Area (BSAI) off the coast of Alaska, now including two newer economic data report collections)	3 3 2005 (70 FR 10360)	5/30/2013

NOAA 19	Permits and Registrations for United States Federally Regulated Fisheries	4 17 2008/73 FR 20914	5/30/2013
NOAA 20	SARSAT	4 17 2008/73 FR 20914	5/5/2016
NEW NOAA 21	Fisheries Finance Program	NA	2008
NEW NOAA 22	NOAA Health Service Questionnaire	NA	2008
NEW NOAA 23	West Coast Region Economic Data Reports	NA	12/23/2014

TOTAL: 16

2015-16 status at DOC
Published 11/25/15; effective 1/19/16
Published 5/5/16; effective 6/14/16
Added missing info and returned to DOC 3 8 16. 4 13 16, DOC decided that it should be a complete update. OLE completed updates 6 16 16; I cleaned up and sent 2 outstanding minor questions, 6 17 16. At one time it had been thought to separate out GC files into another SORN, but it was decided not to. To DOC 6 20 16. Responded to edits and comments rec'd 6 29 16, on 6 30 16, and added the new volunteer routine use. 6 30 17: now at Assistant General Counsel for Legislation, Regulation, and Oversight

MHG completed review 5 22 17; few edits, added volunteer routine use and put in new template, 5 25 17; sent to DOC same day. In new template to DOC 10 14 17
To DOC 12 13 16
Published 10/9/15; effective 11/23/15. Second amended version published 1-12-17. Another amended version to OPOG 6 26 17
Published July 8, 2016. Became effective August 17, 2016.
Published 9/17/15; effective 10/28/15
Published 7/31/2014; effective 09/02/2014
Published 10/9/15;effective 11/23/15

Published 8/7/2015. effective 9/15/15
Amended SORN published 1-12-17
Published July 8, 2016. Became effective August 17, 2016.
Published 1/19/16; effective 3/1/2016
Published 8-7-15; effective 9/15/15

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Mark Graff - NOAA Federal

From: Mark Graff NOAA Federal
Sent: Wednesday, February 7, 2018 5:40 PM
To: Catherine Amores NOAA Federal; Mary Wohlgemuth NOAA Federal; Wendy Holmes NOAA Affiliate; Anthony Hammond NOAA Affiliate; Scott Leonard NOAA Federal; Albert McMath NOAA Federal; Joe Maniscalco NOAA Federal; Thomas Heinrichs NOAA Federal; Juanita Sandidge NOAA Federal; Joe Brust; Thomas Renkevans NOAA Federal; Ron Mahmot NOAA Federal; John Clark NOAA Federal; Alan Hall NOAA Federal; Ajay Mehta NOAA Federal; Andre Hammond NOAA Federal; Chris Sisko NOAA Federal; Marc Moser NOAA Federal; Larry Ledlow NOAA Federal; Marge Ripley NOAA Federal; James Valenti NOAA Federal; Victor Kalu NOAA Federal; Thomas Narow NOAA Affiliate; David Garcia NOAA Affiliate; Shawnn Shears NOAA Federal; James Schreiber NOAA Federal; Charles Obenschain NOAA Federal; Brian Little NOAA Federal; Scott Koger NOAA Affiliate; Isaac Sanvee NOAA Affiliate; Jeffrey VanDam NOAA Affiliate; John Sanns NOAA Federal; Mark Hall NOAA Federal; Kenneth Haywood NOAA Federal; Kris Tai NOAA Affiliate; Matthew Jochum NOAA Federal; Marcus Ertle NOAA Federal; William Wooten Janney NOAA Affiliate; Sherry Goynes NOAA Affiliate; Jason Symonds NOAA Federal; Ericka EvansSterling NOAA Affiliate; Mark Paese NOAA Federal; Vanessa Griffin NOAA Federal; Steven Cooper NOAA Federal; Juliana Blackwell NOAA Federal; Larry Tyminski NOAA Federal; Bill Lapenta NOAA Federal; Richard Varn NOAA Federal; Mark Strom; Christopher Strager; Christopher Cartwright NOAA Federal; Grant Cooper NOAA Federal; Carven Scott NOAA Federal; Daniel Morris NOAA Federal; Kristen Koch NOAA Federal; David Michaud NOAA Federal; Margarita Gregg NOAA Federal; Thomas Graziano NOAA Federal; Deborah Lee NOAA Federal; Chris Sabine NOAA Federal; Dave Westerholm NOAA Federal; Richard Ullman NOAA Federal; Scott Rumsey NOAA Federal; Harry Cikanek NOAA Federal; _NOAA ITSOs; Ken Van Langen NOAA Federal; Steven Freeman NOAA Federal; Wilbert Francis NOAA Affiliate; Michael McCully NOAA Federal; Cynthia Bridgett NOAA Federal; Tina Williams NOAA Affiliate; Mark Deforest NOAA Federal; Brian McGovern NOAA Federal; Eric Barton NOAA Federal; Barry Harrell NOAA Federal; Nick Tenney NOAA Federal; Rick Miner NOAA Federal; Rich Cosgrove NOAA Federal; Rossyn Tasaka NOAA Federal; Barbara Von mettenheim NOAA Affiliate; Chuck Baxley NOAA Federal; Maurice Mcleod NOAA Federal; Linda Matthews NOAA Federal; Giovanni Sella NOAA Federal; MaryLouise Kurchock NOAA Federal; James Cooperman NOAA Affiliate; Dana Larson NOAA Federal; Russell Worman NOAA Federal; Christina Horvat NOAA Federal; Arthur Yo NOAA Federal; Joseph Devost NOAA Federal; Patrick Quigley NOAA Federal; Jennifer Dover NOAA Federal; Julie Rough NOAA Federal; Blanche Marshall NOAA Federal; Timothy Wugofski NOAA Federal; Steve Michnick NOAA Federal; Mark Dorosh NOAA Affiliate; Chris Ortiz NOAA Federal; Joy Baker NOAA Federal; Sallie Ahlert NOAA Federal; Phil Mieczynski NOAA Federal; Adam Van Meter NOAA Federal; Nicholas Rappold NOAA Federal; Peter Thoenen NOAA Federal; Gary Petroski NOAA Federal; Chris Hornbrook NOAA Federal; James Brown NOAA Federal; John McKeever NOAA Federal; Rene Rodriguez NOAA Federal; Rick Jiang NOAA Federal; Jeff Flick NOAA Federal; Jeff Horn NOAA Federal; Russell Richards NOAA Federal; John Parker NOAA Federal; Timothy O'Brien NOAA Affiliate; Ali Darab NOAA Affiliate; David Skiffington NOAA

Affiliate; Robert Lai NOAA Affiliate; John Shore NOAA Affiliate; Frank Hughes NOAA Affiliate; James Jones NOAA Federal; John Hill NOAA Federal; _NOAA Assistant CIOs; Zachary Goldstein NOAA Federal; Michelle Reed NOAA Federal; Douglas Perry NOAA Federal; Benjamin Friedman NOAA Federal; Karl Mueller NOAA Federal; John D. Parker NOAA Federal

Cc: Robert Swisher NOAA Federal; Dennis Morgan NOAA Federal; Sarah Brabson NOAA Federal; John Almeida NOAA Federal; Cc: OCIO/OPPA; Bogomolny, Michael (Federal); Eric Williams NOAA Affiliate; Robert Hogan; Ed Kearns NOAA Federal; _OCIO GPD

Subject: January Monthly Privacy Report

Attachments: PTA PIA Management Report (18).xlsx; SORN_DEPT 29_draft_(2017 07 03) mhg.docx; DOC SORN Status Sheet_NOAA as of 020618.xlsx

Good Afternoon,

This is a report regarding the activities of the NOAA Privacy Program from January 1-January 31, 2018. Attached are two spreadsheets outlining the status of SORNs, PIAs, and PTAs within NOAA.

Some of highlights of the Program's activities for the month include:

- DOC has submitted COMMERCE/DEPT-29 SORN, Unmanned Aircraft Systems, to the *Federal Register* for publication, authorizing certain collection, storage, and retrieval of PII through the use of Unmanned Aircraft. The SORN will be published within two business days, and has been highly anticipated within OMAO and NOS. A copy of the draft SORN is attached for your reference.
- DOC reiterated at the Privacy Council that all Bureaus are required to submit their PIA documentation at least 60 days in advance of the scheduled ATO date in order to have a CRB scheduled in time. Please coordinate the PIA preparation time within the existing A&A process so that a finalized PIA can be submitted to the Department by this time. In instances where new PII is discovered on a system, or there is a change impacting privacy, such as a merger or a new PII dataset within the FISMA System Accreditation boundaries within this time window, an expedited review request, signed by the NOAA CIO, can be submitted.

NOAA, along with OIG, BIS, and OIS, presented the parameters for the DOC Privacy Incident Tabletop Exercise (TTX) during the Quarterly Privacy Council. This exercise will test the compliance of all DOC bureaus on incident response under the DOC Breach Response Notification Plan. In the coming two weeks, DOC will issue a request for volunteers to participate in the Privacy TTX and outline the parameters of the exercise simulating a "High" incident response scenario. The DOC Response Task Force, consisting of DOC Senior Management, will be assembled by DOC/OPOG to receive and review the TTX responses by the bureaus and carry out their roles as they would have in a legitimate major Privacy Incident.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

STATUS OF NOAA SYSTEMS OF RECORD NOTICES (SORN)

SORN	Title/Purpose	Date SORN Previously Published	Date Sent to DOC
NOAA 1	Applications for NOAA Corps	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 3	Commissioned Officer Official Personnel Folders	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 5	Fisheries Law Enforcement Cases (Address Update)	8/10/2007 (72 FR 45009)	5/30/2013

NOAA 6	Fishermen's Statistical Data	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 10	NOAA Diving Program	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 11	Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.	NA	5/30/2013
NOAA 12	Marine Mammals, Endangered and Threatened Species, Permits and Exemptions (Amendment)	8/10/2007 (72 FR 45009)	2008
NOAA 13	Records of the Regional Fishery Management Councils	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 14	Dr. Nancy Foster Scholarship Program	2005	8/22/2014
NOAA 15	Observation Privacy Act System of Records Notice 2	10/17/2002 (67 FR 64086)	5/30/2013
NOAA 16	Economic Data Reports for Alaska Federally Regulated Fisheries off the coast of Alaska (first published as Crab Economic Data Report for Bering Sea/Aleutian Islands Management Area (BSAI) off the coast of Alaska, now including two newer economic data report collections)	3 3 2005 (70 FR 10360)	5/30/2013

NOAA 19	Permits and Registrations for United States Federally Regulated Fisheries	4 17 2008/73 FR 20914	5/30/2013
NOAA 20	SARSAT	4 17 2008/73 FR 20914	5/5/2016
NEW NOAA 21	Fisheries Finance Program	NA	2008
NEW NOAA 22	NOAA Health Service Questionnaire	NA	2008
NEW NOAA 23	West Coast Region Economic Data Reports	NA	12/23/2014

TOTAL: 16

2015-16 status at DOC
Published 11/25/15; effective 1/19/16
Published 5/5/16; effective 6/14/16
Added missing info and returned to DOC 3 8 16. 4 13 16, DOC decided that it should be a complete update. OLE completed updates 6 16 16; I cleaned up and sent 2 outstanding minor questions, 6 17 16. At one time it had been thought to separate out GC files into another SORN, but it was decided not to. To DOC 6 20 16. Responded to edits and comments rec'd 6 29 16, on 6 30 16, and added the new volunteer routine use. 6 30 17: now at Assistant General Counsel for Legislation, Regulation, and Oversight

MHG completed review 5 22 17; few edits, added volunteer routine use and put in new template, 5 25 17; sent to DOC same day. In new template to DOC 10 14 17
To DOC 12 13 16
Published 10/9/15; effective 11/23/15. Second amended version published 1-12-17. Another amended version to OPOG 6 26 17
Published July 8, 2016. Became effective August 17, 2016.
Published 9/17/15; effective 10/28/15
Published 7/31/2014; effective 09/02/2014
Published 10/9/15; effective 11/23/15

Published 8/7/2015. effective 9/15/15
Amended SORN published 1-12-17
Published July 8, 2016. Became effective August 17, 2016.
Published 1/19/16; effective 3/1/2016
Published 8-7-15; effective 9/15/15

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Jean Apedo - NOAA Federal

From: Jean Apedo NOAA Federal
Sent: Thursday, February 8, 2018 9:00 AM
To: Ann Madden NOAA Federal; Douglas.A.Perry@noaa.gov
Cc: Sarah Brabson NOAA Federal; Mark.Graff@noaa.gov
Subject: RE: Completed: Signed by ISSO: NOAA0900 2018 PIA and PTA
Attachments: NOAA0900 052317 for new signatures_2018 certification.pdf; NOAA0900 PTA 2018.docx.pdf

Good morning Doug,
Attached are NIOAA0900 PTA and PIA for your review.
Thank you.

From: Ann Madden NOAA Federal [mailto:ann.madden@noaa.gov]
Sent: Thursday, February 08, 2018 8:34 AM
To: Jean Apedo NOAA Federal
Cc: Sarah Brabson
Subject: Fwd: Completed: Signed by ISSO: NOAA0900 2018 PIA and PTA

Jean-

Can you please review and sign? I can get them to Doug next.

Thanks

Ann

----- Forwarded message -----

From: Sarah Brabson - NOAA Federal <sarah.brabson@noaa.gov>
Date: Wed, Feb 7, 2018 at 10:50 AM
Subject: Fwd: Completed: Signed by ISSO: NOAA0900 2018 PIA and PTA
To: Ann Rivers <Ann.Madden@noaa.gov>

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

James Cooperman - NOAA Affiliate

From: James Cooperman NOAA Affiliate
Sent: Thursday, February 8, 2018 11:27 AM
To: Sarah Brabson NOAA Federal
Cc: John D. Parker NOAA Federal; Mark Graff NOAA Federal; _NOS IT Security Program; Jonathan Gordon NOAA Federal
Subject: Re: NOAA6602 SORN
Attachments: NOAA6602 PIA_V1 02 2018.docx; NOAA6602 PTA_V1 02 2018.docx

Good Morning Sarah

I'm attaching the Draft PTA and PIA for the Office of National Marine Sanctuaries NOAA6602. I have left them in draft format in case any updates are required.

NOAA6602 underwent 2 major changes just prior to the FY2018 assessment that started in September of 2017 (b)(5)

[Redacted text block]

Jim Cooperman

James Cooperman CTR
Information System Security Office
Office of National Marine Sanctuaries
Desk [240-533-0680](tel:240-533-0680)
Cell (b)(6)



On Thu, Feb 8, 2018 at 9:32 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
Thanks!

On Thu, Feb 8, 2018 at 9:31 AM, John D. Parker NOAA Federal <john.d.parker@noaa.gov> wrote:
I provided the ones off of the PIA web site (both PTA/PIA).

--

John D. Parker, CISSP, CISA <John.D.Parker@noaa.gov>
NOS IT Security Officer
DOC/NOAA/NOS IMO240-533-0832 (office) (b)(6) (mobile)
Email NOS IT security inquires: NOS.ITSP@noaa.gov

On 2/8/2018 9:29 AM, Sarah Brabson NOAA Federal wrote:

Okay, please note that we have new DOC templates for both PIA and PTA. They are labeled 1 17 in upper right corner. thx

http://www.cio.noaa.gov/services_programs/privacy.html

On Thu, Feb 8, 2018 at 9:27 AM, John D. Parker NOAA Federal <john.d.parker@noaa.gov> wrote:

Jim will have to answer that since I have not seen the PTA or PIA update.

--

John D. Parker, CISSP, CISA <John.D.Parker@noaa.gov>
NOS IT Security Officer
DOC/NOAA/NOS IMO240-533-0832 (office) (b)(6) (mobile)
Email NOS IT security inquires: NOS.ITSP@noaa.gov

On 2/8/2018 9:26 AM, Sarah Brabson NOAA Federal wrote:

Is the PII more than user id? If not, no PIA needed.

On Thu, Feb 8, 2018 at 9:14 AM, John D. Parker NOAA Federal <john.d.parker@noaa.gov> wrote:

I will leave that up to you.

--

John D. Parker, CISSP, CISA <John.D.Parker@noaa.gov>
NOS IT Security Officer
DOC/NOAA/NOS IMO240-533-0832 (office) (b)(6) (mobile)
Email NOS IT security inquires: NOS.ITSP@noaa.gov

On 2/8/2018 9:12 AM, Mark Graff NOAA Federal wrote:

Understood thanks John. We should probably mention it on the call today with OPOG to give them a heads up.

Mark H. Graff

FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration

[\(301\) 628 5658](tel:3016285658) (O)

(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Thu, Feb 8, 2018 at 9:11 AM, John D. Parker NOAA Federal
<john.d.parker@noaa.gov> wrote:

Hi Mark,

I just spoke with Jim and he will be submitting his update draft
PTA and PIA today that identifies PII/BII in the system.

The NOAA6602 ATO expiration is March 16, 2018, and will need
to be expedited.

John

--

John D. Parker, CISSP, CISA <John.D.Parker@noaa.gov>
NOS IT Security Officer
DOC/NOAA/NOS IMO [240-533-0832](tel:240-533-0832) (office) (b)(6) (m
obile)
Email NOS IT security inquires: NOS.ITSP@noaa.gov

On 2/8/2018 9:07 AM, Mark Graff NOAA Federal wrote:

Hi James

(Adding Sarah Brabson)

I'm thinking you're referring to whether there is a
PIA for NOAA6602 under OMB A 108, where PIAs
are FISMA system specific. SORNs are collection
specific (such as HR data, or UAS data), but the PIA
has to be done on a system by system basis when
the FISMA system collects PII. What is the PII
contained within NOAA6602 that requires a PIA?
Ordinarily if PII were in the System, it would be
reflected in the PTA, and the last one completed for
NOAA6602 indicated that all PII was removed from
the system in 11/2015. Has PII been re introduced
to the system?

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
[\(301\) 628 5658](tel:3016285658) (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Thu, Feb 8, 2018 at 8:59 AM, James Cooperman
NOAA Affiliate <james.cooperman@noaa.gov>
wrote:

Good Morning Mark

I am trying to determine if a SORN exists for NOAA6602. NOS ITSP recommended that I contact you to see if one had been completed previously and to determine what steps need to be taken to update an existing SORN or create a new one.

Thank You

Jim Cooperman

James Cooperman CTR
Information System Security Office
Office of National Marine Sanctuaries
Desk [240-533-0680](tel:2405330680)
Cell (b)(6)



Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Monday, February 12, 2018 9:53 AM
To: Sally Bibb NOAA Federal
Cc: Mark Graff NOAA Federal
Subject: Re: DRAFT Suggested edits to SORN 19
Attachments: Privacy Act NOAA 19 PA SORN (2015 07 23) akr bibb_sb.docx

Sally, I went over this again and thought that since in the other routine uses we do not go into nearly as much detail, I made an edit using track changes. I also didn't know that we make applications available to the public.

Please see attached.

On Fri, Feb 9, 2018 at 9:18 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
Looks good. Since this is a NOAA wide routine use, I had already involved Mark Graff, our NOAA Privacy and FOIA Officer. But why not an Alaska person as well? We don't usually put this much detail into a routine use, but I started to do so with my first draft.

On Fri, Feb 9, 2018 at 9:01 PM, Sally Bibb NOAA Federal <sally.bibb@noaa.gov> wrote:
Hi Sarah I took a stab at editing the routine use statement for the things that we release to the public on web sites or in response to ad hoc requests for information.

(b)(5) [Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]. What do you think about that

addition?

Mainly wanted your general review to see if the things I added to the routine use paragraph seemed appropriate.

PRA Clearance Officer

Governance and Portfolio Division

Office [301 628 5751](tel:3016285751)

Ce (b)(6)

Sarah D. Brabson

IT Infrastructure Investment Program Manager

PRA Clearance Officer

Governance and Portfolio Division

Office 301 628 5751

Ce (b)(6)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Monday, February 12, 2018 1:06 PM
To: Gioffre, Kathy (Federal); CPO; Murphy, Tahira; Purvis, Katrina
Cc: Mark Graff NOAA Federal; Giovanni Sella
Subject: NOAA Privacy Policy signed by Zach Goldstein 5 17 17
Attachments: NOAAPrivacyPolicy_Final_May2017.pdf

I'm pretty sure Mark sent this to Katrina at some point, but one of our ISSOs noticed it's not posted in that section of your Web pages.

Could you please post? It's posted on our Privacy page of course.

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Cell (b)(6)



NOAA Privacy Policy

Table of Contents

- [I. Background](#)
- [II. Purpose](#)
- [III. Scope](#)
- [IV. References](#)
- [V. Policy](#)
- [VI. Responsibilities](#)
- [VII. Management and Ownership](#)
- [VIII. Intended Audience](#)
- [IX. Implementation Date](#)
- [X. Grandfather Exemption and Waiver Options](#)
- [XI. Performance Objectives and Measurements](#)
- [XII. Definitions](#)
- [XIII. Approval](#)
- [Appendix I: Data Protection and Privacy](#)
- [Appendix II: NOAA's Privacy Principles](#)

I. Background

NOAA is committed to fulfilling its obligations in safeguarding the Personally Identifiable Information (PII) and Business Identifiable Information (BII) entrusted to it by the public. In carrying out this important responsibility, NOAA takes seriously its role in properly collecting, storing, and transmitting the PII within its information systems. Each of these actions are carried out only to further NOAA's mission, and the PII with which NOAA is entrusted is only viewed by those who have proper authorization to view that material on a need-to-know basis for carrying out their work responsibilities. In order to ensure proper handling, storage, and transmission of this sensitive information, NOAA has created this Privacy Policy for those within NOAA entrusted with this important role.

II. Purpose

The purpose of this policy is to explain how we handle information we collect during your visit to NOAA websites. This includes information collected through NOAA forms that are posted on NOAA websites. This policy does not apply to third-party websites that you are able to access from our websites.

We do not collect personally identifiable information (name, address, e-mail address, social security number, or other personal unique identifiers) or business identifiable information on our websites unless we specifically advise you that we are doing so.

Information on the handling of PII and BII under the Privacy Act and the Freedom of Information Act

(FOIA) can be found at the Department of Justice website. (<https://www.justice.gov/oip>). The restrictions on the unencrypted transmission of Sensitive PII under the DOC Transmission of PII Policy apply also to the transmission of BII. BII constitutes information that could qualify for withholding under Exemption 4 of the FOIA¹.

This policy is updated when the NOAA makes relevant technology improvements.

III. Scope

This applies to all NOAA Staff and Line Offices collecting PII or BII, including through the use of online forms collecting that information, on behalf of NOAA, or with NOAA sponsorship, whether NOAA, contractor, or grantee owned. This policy applies to all NOAA activities that include the transmission, storage, use, sharing, or access of PII collected by NOAA.

IV. References

1. DOC list of privacy-related governance:
http://www.osec.doc.gov/opog/Privacy/laws_and_regs.html
2. DOC policy, Electronic Transmission of Personally Identifiable Information:
http://osec.doc.gov/opog/privacy/Privacy_Brochure_2016.pdf
3. DOC Privacy Policy: <https://www.commerce.gov/page/privacy-policy>
4. The Privacy Act of 1974 (referred to as § 552a. Records maintained on individuals), as amended:
<https://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf>
5. OMB M-17-5:
<https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-05.pdf>

V. Policy

Compliance with this policy is mandatory. NOAA will enforce the following obligations to achieve the objectives above:

[01] Web Measurement and Customization Technologies

We use web measurement and customization technologies, including cookies, to optimize your experience during your visit to our websites and to provide information about how you use our web site. Technologies commonly known as “cookies,” may include the use of session or persistent cookies. Cookies are a small amount of data generated by a website and saved by your computer to enhance your online interactions and preferences. NOAA only uses cookies that do not collect PII. These cookies are deleted when your web browser is closed.

There are three “tiers” of these web measurement and customization technologies, as established by the Office of Management and Budget (OMB)²:

Tier 1 - Single Session

This technology tracks the user’s online interactions within a single session or visit to a single

¹ 5 U.S.C. § 552(b)(4).

² See, <https://connection.commerce.gov/policy/20160705/web-measurement-and-customization-tech-policy>; see also <https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-06.pdf>.

web site. Any information related to a particular visit to the web site is deleted from the user's computer immediately after the session ends.

Tier 2 - Multi Session without Personally Identifiable Information

This technology notices when a user returns to a web site and "remembers" his or her online interactions and preferences across multiple sessions, typically for the purpose of statistics on web usage, but also for customizing people's online experience. Google Analytics uses cookies to see if the visitor is a repeat visitor, or a returning visitor. Some GIS sites use cookies so that visitors do not lose context when they go from page to page, and can return to pages they have created before.

Tier 3 - Multi Session with Personally Identifiable Information

This tier encompasses any use of multi-session web measurement and customization technologies when PII and BII is collected (including when the agency is able to identify an individual as a result of its use of such technologies). NOAA does not use Tier 3 technologies. The following sections include information describing the use of these tiers when you visit NOAA websites.

[02] Tiers Accessed When You Visit Our Websites

When you visit our websites to read pages or download information, Tier 1 or Tier 2 technology may be used. We automatically collect and store the following non-personally identifying information:

- The Internet protocol (IP) address from which you access our web site. An IP address is a unique number that is automatically assigned to the computer you are using whenever you are surfing the web. This is used for basic transactions of returning information to the user's machine, and for our own Internet security protocols to help protect the security of NOAA's IT systems and your data.
- The type of browser and operating system used to access our site, to optimize your web page experience.
- The date and time our web site is accessed, for the purpose of monitoring demand.
- The pages visited, for the purpose of improving the usefulness of our web site by providing helpful links and removing pages that are not read.

Visitor logs may contain the URL of the last website you visited, if that web site contains a link to a NOAA web page, which indicates how you found this web site.

The information we retain does not include personally identifying information. The above information is maintained in our system logs for analytical purposes to improve our web pages. The logs may be kept indefinitely and used at any time and in any way necessary to secure our systems and ensure the integrity of the data on our servers.

When you make use of NOAA Websites, Tier 1 and Tier 2 technology may be used, so these cookies will not collect personally identifiable information to be permanently retained by NOAA on either the users' or NOAA's computers. When you order products, database records track your order through the process.

Any data that NOAA may collect is protected under the Privacy Act, FOIA, and other applicable laws.

When you respond to a collection form via the Internet, you may voluntarily include personally identifiable information (PII) or business identifiable information (BII). For each collection and form, we provide an explanation about the laws that apply to the handling of the data that respondents provide.

When you provide PII or BII in response to a collections form through a NOAA web site, Tier 1 technology may be used, but the only PII or BII to be collected is what you voluntarily enter into the form. Once you access an online collection or form, we may collect information about how long it took you to complete the collection or form, which questions you answered, and how many times you logged into the collection or form. In addition, we collect data on navigation of the collection or form, which includes mouse clicks and any data entered onto the collection or form, whether or not the collection or form is completed and submitted. These data are used in aggregate to assess the usability of the collection or form, or for other authorized statistical purposes. If these data are associated with your responses, they may be protected under the Privacy Act, the FOIA, or other applicable law.

Questions concerning this policy may be addressed to: http://www.cio.noaa.gov/contact_us.html.

[03] Blocking the use of Cookies (Opt Out)

The technologies we describe in this policy are the default settings. However, you can remove or block the use of web cookies by changing the setting of your browser as described at http://www.usa.gov/optout_instructions.shtml.

Should you choose to remove or block the use of web cookies, we will provide you with alternatives for acquiring comparable information or services.

[04] Other Information We Collect From E-Mail and Other Online Forms

When you send us personally identifiable information or business identifiable information over e-mail, we only use the information we need in order to respond. When you send us personally identifiable information or business identifiable information on online collection forms (e.g. conference registrations, contact lists, etc.), we only use the information for the stated purposes (shown either on the form or on a corresponding Privacy Act Statement). All information our web site visitors submit via e-mail or an online form is voluntary. Submitting voluntary information constitutes your consent to the use of the submitted information for the stated purpose.

We may contact you by email to invite you to participate in a collection or form, but we will not ask you to provide responses via email.

[05] Data Retention

We retain questions and comments only if required by law, or for a specific program need, as specified by the National Archives and Records Administration's General Records Schedule (GRS) 20, Electronic Records or other approved records schedule as applicable.

[06] Document Accessibility

NOAA is committed to making online forms and other public documents on its Internet server accessible to all. We continuously update our websites and make modifications to those pages, including those which are not in compliance with the Americans with Disabilities Act. We use Hypertext Markup Language (HTML) to create pages that are generally accessible to persons using screen-reading devices, and we are careful in our construction of HTML documents to ensure maximum accessibility. We include

alternate text describing graphics.

Many NOAA Internet documents are in ASCII or HTML formats. These documents are accessible to persons using screen-reading software. We also have a large number of documents in Adobe Acrobat PDF (Portable Document Format) files. Currently, many people using screen-reading devices cannot read documents in PDF format, specifically those that were created from a scanned hard copy.

Adobe Systems, Inc. is producing various products designed to make Adobe Acrobat documents accessible to persons using screen-reading software. Adobe's accessibility web pages describe their efforts.

To allow us to better serve those with visual disabilities who are having difficulty accessing PDF documents, you may contact us directly for further assistance at http://www.cio.noaa.gov/contact_us.html.

[07] Third Party websites and Applications

NOAA has a presence on several social media/Web 2.0 platforms (Facebook, YouTube, Twitter and Flickr, and other third-party services)). Each of these websites provides NOAA unique ways of sharing information. It also allows visitors with a way to communicate with the agency. Some may allow visitors to log in, create profiles and save information in those profiles. We do not collect or use any of the personally identifiable information you may have entered on these social media sites. Further, NOAA has no control over the third-party's use of this information and bears no responsibility for the third-party's handling of your information. These websites have their own privacy, security and accessibility policies.

NOAA may also use a third-party web site or application (hosted service) to conduct customer satisfaction collections and/or feedback forms. These collections and/or feedback forms may collect your name and email address for processing purposes. The results from these collections or forms are used to conduct primary research into the quality of NOAA programs and products. The results collected will be used strictly for internal program management purposes to assess staff work, material design and development and to enhance planning efforts for current and future collections and forms. In addition, other third-party websites or applications may be used to host NOAA data products to be used by the public. These websites do not require the use of personally identifiable information or business identifiable information.

[08] Security and Third Party Links

To ensure that computer service remains available to all users, this government IT system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage to our computer system. websites identified as representing an actual or potential security threat to NOAA information and/or information resources are blocked. Further, websites that are known to violate NOAA, Department of Commerce, and/or Federal guidelines regarding access to certain types of websites and/or content are blocked, for example:

- websites hosting malware/spam
- websites involved in the compromise of other government agencies
- Adult content websites
- On-line storage and file sharing web site
- Freeware/Shareware websites
- websites attacking NOAA systems (attempting to identify and exploit vulnerabilities in Internet facing systems)

Some of our website contains links to other federal agencies, international agencies, and private organizations. Once you link to another web site, you are subject to the policies of the new web site. Our linking to non-government websites does not constitute an endorsement of any products, services or the information found on them.

[09] Mobile Applications

Mobile Applications will comply with all provisions the Privacy Act, and are subject to the same requirements of a Privacy Act Statement (PAS) as outlined in 5 U.S.C. 552a(e)(3). Each Mobile Application will clearly identify if it is a NOAA Application, and if it is a NOAA Application, the PAS, data characterization, notice, consent, privacy controls, authority, and data sharing provisions will be clearly identified in the Privacy Impact Assessment (PIA) associated with the information system to which that mobile application pertains.

VI. Responsibilities

This Policy requires that all NOAA collection of PII and BII is conducted consistent with applicable law, governing OMB Memoranda, and DOC Privacy Policies. The Offices below have the following responsibilities to ensure compliance with this Policy:

[01] The Associate Administrator for each Line Office shall:

Ensure individual privacy protections in compliance with applicable laws, regulations, and policies.

[02] The NOAA Office of the Chief Information Officer (OCIO) has:

Overall responsibility for promulgation and oversight of NOAA-wide information management policies, guidelines and procedures to Line and Staff Offices for their implementation to ensure compliance with relevant Federal laws, regulations and policies. Such policies, guidelines and procedures include, but are not limited to, addressing requirements associated with privacy, IT security, and records management.

[03] The NOAA Staff and Line Offices are:

Responsible for implementing and executing NOAA policies, procedures, and protections consistent with applicable law, Executive Orders, regulations, policies and standards.

VII. Management and Ownership

The NOAA Chief Information Officer establishes the objectives and terms of use for the collection, use, storage, and transmission of PII.

VIII. Intended Audience

The intended audience is the public, and the policy governs NOAA employees and affiliates operating NOAA systems that may collect, store, or transmit PII.

IX. Implementation Date

This procedure is effective immediately upon approval by the NOAA CIO.

X. Grandfather Exemption and Waiver Option

None.

XI. Performance Objectives and Measurements

[01] Training curriculum and objectives

Following adoption of the Policy, NOAA will prepare a training guide and curriculum for adoption to train prospective NOAA users for role-based privacy training within one year.

[02] Review of the Privacy Policy

NOAA will review this Privacy Policy with the passage of subsequent statutes impacting Privacy, OMB Memoranda, Department guidance, and technical advancements that have an impact on Privacy practices. NOAA will also review, no later than once every year, all of the NOAA information systems that contain PII consistent with OMB Memorandum A-130³. This will include a substantive review of individual Privacy policies associated with the staff and line offices. If, in conducting these reviews, substantive changes are necessary, this Policy will be updated pursuant to OMB M-17-06.

XII. Definitions

Business Identifiable Information (BII) Information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person and privileged or confidential.”

Personally Identifiable Information (PII) Information that can be used to distinguish or trace an individual’s identity, such as name, Social Security number (SSN), biometric records, etc., alone, or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. [OMB M-07-16].

Sensitive Personally Identifiable Information (Sensitive PII) Sensitive PII is defined as PII which, when disclosed, could result in harm to the individual whose name or identity is linked to the information. Further, in determining what PII is sensitive, the context in which the PII is used must be considered. For example, a list of people subscribing to a government newsletter is not sensitive PII; a list of people receiving treatment for substance abuse is sensitive PII. As well as context, the association of two or more non-sensitive PII elements may result in sensitive PII. For instance, the name of an individual would be sensitive when grouped with place and date of birth and/or mother’s maiden name, but each of these elements would not be sensitive independent of one another. [DOC Electronic Transmission of PII Policy].

Senior Agency Official For Privacy (SAOP) - The designated Senior Agency Official for Privacy currently serving as the Chief Privacy Officer for the Department of Commerce.

XIII. Approval

GOLDSTEIN.ZACHARY.G.1228698985

Digitally signed by GOLDSTEIN.ZACHARY.G.1228698985
DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER,
cn GOLDSTEIN.ZACHARY.G.1228698985
Date: 2017.05.30 12:05:18 -04'00'

Zachary Goldstein, NOAA CIO

Date

³ <http://www.osec.doc.gov/opog/privacy/Circular%20A-130%20FINAL.pdf>

APPENDIX I

[01] Data Protection and Privacy

How We Protect Your Information

NOAA has an obligation to produce accurate, relevant information on weather, oceanographic data, satellite datasets, records regarding the Nation's Fisheries, but we recognize that in some instances it is your information that we collect to produce these datasets.

We depend on your cooperation and trust, and promise to protect the confidentiality of your information.

[02] Protecting Your Information

Federal law protects your information, and we have developed policies and statistical safeguards to help us follow the law and to protect your information as permitted under applicable law.

[03] Confidentiality of Magnuson-Stevens Act Information

The Magnuson Stevens Act requires that NMFS maintain the confidentiality of information submitted in compliance with any requirement or regulation under the Act.

[04] Privacy Principles

Our Privacy Principles are guidelines that cover all of our activities. These principles encompass both our responsibilities to protect your information and your rights as a respondent. They apply to the information we collect and the information we publish.

[05] Data Stewardship

Data Stewardship is the formal process we use to ensure that your information is protected to the extent authorized by law.

We recognize the value of your trust, and we believe that when you provide information to NOAA we must serve as caretakers of your information. If you would like to learn more about how we fulfill this responsibility, please visit our NOAA Privacy pages.

Appendix II

[01] NOAA's Privacy Principles

We depend on your cooperation and trust, and we promise to protect your information consistent with applicable law.

NOAA's Privacy Principles remind us of this commitment and help ensure the protection of your information throughout all of our activities.

The Privacy Principles are our guidelines. They help us as we design collections of information to consider respondents' rights and concerns. Every principle embodies a promise to you, the respondent. **Necessity:** Do we need to ask this question? Do we need to collect this information?

Every time we prepare to ask a question, we determine whether the information is truly necessary. All of the information we collect is used for a lawful purpose, with proper notice, consent, and information sharing requirements.

- We commit to collect only information necessary for each collection and form.
- It is our commitment to use collected information only as indicated on the collection form and in our Privacy Act Statement, System of Records Notice, and or Privacy Impact Assessment, all of which are made publicly available.

[02] Openness: Do you know why we are collecting your information?

We collect information only for mission-related purposes, and it is only used to identify individuals when authorized by law. Before providing PII, you have the right to know why we are collecting the information, the purposes for which the information will be used, what the result would be for refusing to provide the requested information, and our authority to ask for the information in question.

- It is our commitment to inform you of each of these factors every time PII is requested from you

[03] Respectful Treatment of Users: Are our efforts reasonable and did we treat you with respect?

- We commit to minimizing the effort and time it takes for you to participate in the information collection by efficient designs.
- We commit to using only legal, ethical and professionally accepted practices in collecting information.

[04] How do we protect your information?

In addition to removing personally identifiable information, such as names, telephone numbers, and addresses, from our files insomuch as possible while still serving mission objectives, we use various approaches to protect your personal information; including computer technologies and security procedures.

Our security measures ensure that only a restricted number of authorized people have access to private information and that access is only granted to conduct our work and for no other purposes.

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Tuesday, February 13, 2018 11:20 AM
To: Mark Graff NOAA Federal
Subject: Fwd: NOAA4100 PTA for review and signature.
Attachments: NOAA4100_PTA_20180206_Ver1.1_kdr (1).pdf

Mark Tahir asked me and I realized I hadn't heard back from you. In new template, all correct.

thx Sarah

Forwarded message

From: Sarah Brabson - NOAA Federal <sarah.brabson@noaa.gov>
Date: Tue, Feb 6, 2018 at 1:48 PM
Subject: NOAA4100 PTA for review and signature.
To: Mark Graff NOAA Federal <mark.graff@noaa.gov>
Cc: Tahir Ismail <tahir.ismail@noaa.gov>, Mark Deforest <mark.deforest@noaa.gov>, _NMFS InfoSec <NMFS.InfoSec@noaa.gov>

Mark, this is a system that's using Clearwell.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Mark Graff - NOAA Federal

From: Mark Graff NOAA Federal
Sent: Tuesday, February 13, 2018 3:12 PM
To: Sarah Brabson NOAA Federal
Subject: Re: NOAA4100 PTA for review and signature.
Attachments: NOAA4100_PTA_20180206_Ver1.1_kdr (1) mhg.pdf

Got it signed and attached.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Tue, Feb 13, 2018 at 11:20 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
Mark Tahir asked me and I realized I hadn't heard back from you. In new template, all correct.

thx Sarah

Forwarded message

From: Sarah Brabson - NOAA Federal <sarah.brabson@noaa.gov>
Date: Tue, Feb 6, 2018 at 1:48 PM
Subject: NOAA4100 PTA for review and signature.
To: Mark Graff NOAA Federal <mark.graff@noaa.gov>
Cc: Tahir Ismail <tahir.ismail@noaa.gov>, Mark Deforest <mark.deforest@noaa.gov>, _NMFS InfoSec <NMFS.InfoSec@noaa.gov>

Mark, this is a system that's using Clearwell.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division

Office [301 628 5751](tel:3016285751)

Ce (b)(6)

**U.S. Department of Commerce
NOAA NMFS**



**Privacy Threshold Analysis
for the
NOAA4100 - Greater Atlantic Regional Office (GARFO) Network**

U.S. Department of Commerce Privacy Threshold Analysis

NOAA4100 - Greater Atlantic Regional Office (GARFO) Network

Unique Project Identifier: NOAA4100

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

- a) ***Whether it is a general support system, major application, or other type of system:***
NOAA4100 is a general support system.

- b) ***System location:*** Gloucester, Massachusetts

- c) ***Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects):*** NOAA4100 is part of the larger NOAA4000 network; it has interconnections between other NMFS entities including New England Fisheries Science Center, NMFS Headquarters, and with the Atlantic Coastal Cooperative Statistics Program (ACCSPP). All these connections are 24/7 connected using secure protocols.

- d) ***The purpose that the system is designed to serve:*** NOAA4100 maintains several NMFS main host applications and web servers. The computer systems within NOAA4100 provide service to our ultimate end beneficiaries, the habitat, the fish, and the environment; and to the biologists, scientists, statisticians, and economists within the region and nation; and all fishers who depend on our data.

- e) ***The way the system operates to achieve the purpose:*** NOAA 4100 Achieves this purpose by using the system in the analyzing, collection and collaboration of data. Through management of the data and the application of it in governing fisheries.

- f) ***A general description of the type of information collected, maintained, use, or disseminated by the system:*** NOAA4100 collects maintains and disseminates information used for identifying fisheries related organizations and individuals, FOIA requests. Fisheries specific data such as landing data from fish dealers and catch based allocation data.

- g) ***Identify individuals who have access to information on the system:*** Due to the varying sensitivity of NOAA4100's data, the individuals that have access to our data range from the public to only those who have been authorized by the data owner. NOAA4100 data is shared with a variety of organizations. This includes other federal agencies, state and local agencies, fisheries management organizations, fish dealers, educational entities, vessel owners and the public.

- h) ***How information in the system is retrieved by the user:*** Information retrieval on NOAA4100 is done securely in a variety of ways. The majority of access is through the Greater Atlantic Regions website, the information that is shared and collaborated with other organizations is done securely through hardwired interconnections and though the NOAA4000 controlled non-permanent VPN.

- i) ***How information is transmitted to and from the system:*** Information is transmitted from NOAA4100 through secure web based connections, using SSL. Through secure hardwired connections, or though secure VPN connections.

Questionnaire:

1. What is the status of this information system?

This is a new information system. *Continue to answer questions and complete certification.*

This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify): Handling and Processing FOIA Data and Requests.			

This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Continue to answer questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *Please describe the activities which may raise privacy concerns.*

No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the

submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

- Companies
- Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- DOC employees
- Contractors working on behalf of DOC
- Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

 X I certify the criteria implied by one or more of the questions above **apply** to the NOAA4100 and as a consequence of this applicability, I will perform and document a PIA for this IT system.

 I certify the criteria implied by the questions above **do not apply** to the NOAA4100 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Peter Couture

Signature of ISSO or SO: COUTURE.PETE R.L.1365711158 Digitally signed by COUTURE.PETER.L.1365711158 Date: 2018.02.06 08:28:10 05'00' Date: 2/6/2018

Name of Information Technology Security Officer (ITSO): Catherine Amores

Signature of ITSO: AMORES.CATHERINE.SO LEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2018.02.06 11:31:28 05'00' Date: _____

Name of Authorizing Official (AO): Kimberly Damon-Randall

Signature of AO: DAMON RANDALL.KIMBERLY.B.1365821093 Digitally signed by DAMON RANDALL.KIMBERLY.B.1365821093 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=DAMON RANDALL.KIMBERLY B.1365821093 Date: 2018.02.06 08:50:30 05'00' Date: 2/6/2018

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.02.13 15:11:28 05'00' Date: _____

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Wednesday, February 14, 2018 2:33 PM
To: Gioffre, Kathy (Federal); CPO
Cc: Mark Graff NOAA Federal
Subject: NOAA4011 certification, PIA and PTA
Attachments: NOAA4011 PIA resigned for certification 021418 mhg.pdf;
NOAA4011_PIA_Annual_Review_Certification_Form_with_PA_Officer_Final_2017110
1_(ISSO) mhg.pdf; NOAA4011_PTA_FINAL_20170901 mhg.pdf

ATO date will be 9 25 18.

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751

Ce (b)(6)

U.S. Department of Commerce
NOAA



Privacy Impact Assessment
for the
Permits and Registrations for National Marine Fisheries Service Commercial
and Recreational Fisheries

Reviewed by: Mark Graff, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment National Fishing Permit and Landings Reporting System

Unique Project Identifier: 006-000351100 00-48-02-00-01-00

Introduction: System Description

- The National Fishing Permit and Landings Reporting System (NFPLRS) allows members of the recreational and commercial fishing communities to acquire permits for certain species of fish, renew those permits, report catch/landings, and access a library of related information (e.g., online brochures). The system also provides an information source to NMFS through realtime reports accessible via web browsers.
- The secondary function in the system is Electronic Monitoring (EM). EM consists of monitoring catch/landings via video footage. The EM services support catch/landings data retrieval, catch/landings data analysis/review, and on-land data storage in order to support a program for approximately 135 vessels.

The system is part of the Office of Sustainable Fisheries and we coordinate as needed with the Office of Law Enforcement, and the Office of Financial Services, which calculates applicable permit fees.

- Users include the general public, NMFS staff and customer service staff.
- Supported applications include excel spreadsheets, PDF files, database development and management, electronic mail, and web server applications.

The major functions the system provides are:

- Allow constituents to apply for and renew permits for Highly Migratory Species, Swordfish, and/or Atlantic tunas
- Accept reports of bluefin tuna, swordfish, and billfish landings
- Provide the public timely information regarding fisheries regulations
- Provide the public documents and forms related to fisheries activities and permitting
- Provide NMFS staff and customer service staff administrative access to permits
- Provide NMFS staff access to update information on the NFPLRS website.
- Provide Enforcement agents access to permit status
- Provide NMFS staff with statistical reports on permit holdings and landings
- Provide users access to EM catch/landing footage and data
- Support fee collection

Major Functions/Applications

The NFPLRS integrates three functional mission applications.

Web Application

The NMFS Permit Web Site application provides general information about permits as well as a means to apply for HMS, Swordfish, and/or Atlantic tunas permits online. In addition, the system provides general documentation and guidance. The system also accepts information regarding HMS catch/landings. The web site is accessible from Internet and was developed using JAVA. The NMFS Permit Web Site application stores data in the NFPLRS Database.

EM Data Review Application

EM Data Review Application (DRA) is web-based application for reviewing videos and metadata captured from fishing vessels. The video footage captures only data related to fish caught/landed. This allows NOAA4011 to monitor fishing activities of Atlantic Tunas Longline permit holders. The data is stored in Amazon Web Services (AWS) GovCloud S3 and AWS RDS database. Prior to uploading files to AWS, the videos go through a Data Pre-processing System (DPS). DPS is located at ERT Office at Suite 100A, 8380 Colesville Road, Silver Spring, MD 20910.

Database

The NMFS Permit Web Site application stores Permit and Catch/Landings data in the NFPLRS Database in the AWS GovCloud. The NMFS EM application stores catch/landings monitoring data in the AWS GovCloud as well. The database management system used is Oracle 11g for Windows. The NFPLRS Database subsystem consists of the COTS DBMS (Oracle) as well as the tables, stored procedures, and constraints that make up the database application. These Database servers are virtual machines are secured and managed by AWS's Platform as a Service (PaaS) cloud service offering.

Permit data is shared internally with NOAA NMFS/ Southeast Regional Office (SERO)/ Northeast Regional Office (NERO) and externally with Atlantic Coastal Cooperative Statistics Program (ACCSP). This system uses permit data to validate trip level reports.

Authorities: This data allows NMFS to manages living marine resources under U.S. jurisdiction under the authority of the Magnuson-Stevens Fishery Conservation and Management Act, the Marine Mammal Protection Act, Atlantic Tunas Convention Act (ATCA), the Endangered Species Act (ESA), and the Highly Migratory Species Fishery Management Plan, as well as be compliant with international obligations pursuant to the International Commission for the Commission of Atlantic Tunas (ICCAT).

The Federal Information Processing Standard (FIPS) 199 security impact category for the system is Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- This is a new information system.
- This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (Check all that apply.)

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	x	o. Medical Information	
d. Gender		j. Telephone Number	x	p. Military Service	
e. Age		k. Email Address	x	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	x	g. Salary	
b. Job Title		e. Email Address	x	h. Work History	
c. Work Address	x	f. Business Associates			
i. Other work-related data (specify): Information is captured about the vessel and landings. Data includes all information is listed below: Vessel Information					
<ul style="list-style-type: none"> • Owner's Name 					

- Owner's Address
- Owner's Telephone Number
- Owner's Email Address
- U.S. Coast Guard documentation number and/or state registration number for the vessel
- Vessel name
- home port city & state
- principal port city & state
- length in feet
- year built
- crew size
- construction (e.g., wood)
- gross tonnage
- propulsion (e.g., gasoline)
- main engine horsepower
- hold capacity in pounds (if applicable)
- Fees collected
- Permit category to which landing is assigned
- Record ID
- Date fish was landed
- Type of gear used to catch fish
- Length of fish measured in inches
- Round weight (w/ head, fins & guts) in lbs,
- Dressed weight (head, fins, and guts removed) in lbs
- Unique tag number of each fish
- City and State where fish were landed
- Area where fish was caught
- Total amount of fish caught
- Price per pound for both round and dressed weight
- Paid under consignment or on dockside basis
- Grade for freshness , fat, color, shape
- Destination of fish
- Date landing report submitted

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify): The system processes electronic monitoring videos, but only fish catch is recorded.					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify): . Error message					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	x
Telephone	x	Email			
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify): N/A					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application	x*				
Other (specify):					

* Permits site is hosted by a NOAA contractor: <https://hmspermits.noaa.gov/>

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)				
Smart Cards			Biometrics	
Caller-ID			Personal Identity Verification (PIV) Cards	
Other (specify): Data files are used in an Oracle database (AWS RDS) and videos files of fish are stored on a file server (AWS S3).				

There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities				
Audio recordings			Building entry readers	
Video surveillance	x		Electronic purchase transactions	
Other (specify):				

There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.
(Check all that apply.)

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	x	To promote information sharing initiatives	
For litigation	x	For criminal law enforcement activities	x
For civil enforcement activities	x	For intelligence activities	
To improve Federal services online	x	For employee or customer satisfaction	x
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): The system was developed to make it easier for vessels to apply for and obtain permits and to report landings.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The permit and catch reporting data are used to comply with MSA.
 The electronic monitoring videos are used to meet the needs of the observer program.
 This information is collected from members of the public.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau		x	
DOC bureaus			
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify): Cooperative State/Federal program		X (ACCSP)	

*For criminal law enforcement.

The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

x	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Permit data is shared internally with NOAA NMFS/ Southeast Regional Office (SERO)/ Greater Atlantic Regional Office). It is also shared with ACCSP, and an interconnection security agreement is in place. The only information shared is about the permits and vessels. No electronic monitoring or landings data is
---	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	shared.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. (*Check all that apply.*)

Class of Users			
General Public	x*	Government Employees	x
Contractors	x		
Other (specify):			

*Permits Web site only.

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. (*Check all that apply.*)

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
x	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: http://www.nmfs.noaa.gov/aboutus/privacy.html . The online applications page, https://hmspermits.noaa.gov/library , has a link to a new privacy act statement in the list of applications, following the PRA statement link. All elements of a Privacy Act Statement are also included in the PRA Statement on forms downloadable at https://hmspermits.noaa.gov/downloadPackage , page 3 of application form.	
x	Yes, notice is provided by other means.	Specify how: Notice is provided on the permit application. SAAD: A supervisor provides written notice of employee account set-up, explaining the purpose for providing the PII.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

x	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Applicants can choose to not complete an application and thereby forgo fishing privileges requiring the permit. The permit application states that the information is required for review of the application. SAAD: An employee can respond in writing to the supervisor that he/she declines to provide the PII, but this would affect employment, as an account is needed to perform the work.
	No, individuals do not have an	Specify why not:

	opportunity to decline to provide PII/BII.	
--	--------------------------------------------	--

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: The data that is being collected is used and analyzed for management purposes. There is only one purpose for this data collection, as stated on the application. Thus, if not consenting to the stated purpose, the applicant would not complete the application. SAAD: an employee could respond to the supervisor in writing that he/she does not consent to the use of the information provided for account set-up, but there is only the one use.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

x	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: If users want to know what data is being stored, they can request it via the online Feedback Entry form at http://hmspermits.noaa.gov/feedback . Users also have the ability to update their own information via the website, per website instructions. Employees can provide their supervisor or the system administrator with changes to their PII.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

x	All users signed a confidentiality agreement or non-disclosure agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to the PII/BII is restricted to authorized personnel only.
x	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: As part of our continuous monitoring activities, access to data is logged and reviewed periodically. Additionally, scans are executed to check vulnerabilities and weakness in the system.
	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): September 25, 2017 <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a

	moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
x	Contracts with customers establish ownership rights over data including PII/BII.
x	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
x	Other (specify): Contract with Web Master includes FAR Part 24, regarding PII collected its ownership.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

PII is stored in an Oracle database hosted in Amazon GovCloud Web Service (AWS). Access to the database is restricted to the Permits application webserver and via AWS administrative console. Database connection is open only to the internal network. Access to the AWS console is restricted to only system administrators and requires multifactor authentication (password and PIN). Webserver access utilizes SSL certificates using TLS protocol and strong cipher suites. All access to shared read-only data is restricted by source IP address and requires public/private key pairs.

As part of our continuous monitoring activities, access to data is logged and reviewed periodically. Additionally, scans are executed to check vulnerabilities and weakness in the system.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C.

§ 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

x	Yes. This information collection is included in a comprehensive NMFS Permits and Registrations System of Records Notice (SORN), COMMERCE/NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries.
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

x	There is an approved record control schedule. 1504 Fishery Management and Coordination Files. These files relate to programs to coordinate plans and research of the Federal Government in the area of fisheries management with those of the states; to obtain maximum uniformity of regulations; to institutionalize cooperation; to issue permits to foreign and domestic fishing vessels; and award related grants
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
x	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	x	Overwriting	
Degaussing	x	Deleting	x
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
x	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

x	Identifiability	Individuals are not easily identifiable.
x	Quantity of PII	There is a significant quantity in that each permit application contains some PII; however, the PII in these records does not easily identify individuals.

x	Data Field Sensitivity	Provide explanation: As per NIST 800-60 “Guide for Mapping Types of Information and Information Systems to Security Categories”, the highest level based on the information types captured is Moderate. The information collected and stored in NOAA4011 system is non-sensitive PII related to vessel and owner information. The information includes: Owner Name Address Email Address Telephone Number Vessel Name Vessel ID Video footage of fishing activities (not showing individuals) are also collected and stored for audit and enforcement purposes.
	Context of Use	Provide explanation:
X	Obligation to Protect Confidentiality	Provide explanation: Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801, Section 402b.
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis



12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
x	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
x	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

<p>Information System Security Officer or System Owner Name: Wilbert Francis Office: NMFS Phone: (202)427-6397 Email: wilbert.francis@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: center;">FRANCIS.WILBER Digitally signed by FRANCIS.WILBERT.R.1463197551 Date: 2018.01.31 21:11:50 -05'00'</p> <p>Signature: T.R.1463197551</p> <p>Date signed:</p>	<p>Information Technology Security Officer Name: Catherine Amores Office: NMFS OCIO Phone: (301)427-8871 Email: catherine.amores@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: center;">AMORES.CATHERINE.S Digitally signed by AMORES.CATHERINE.SOLEIDAD.1541314390 Date: 2018.01.13 10:08:02 -05'00'</p> <p>Signature: OLEDAD.1541314390</p> <p>Date signed:</p>
<p>Authorizing Official Name: Alan Risenhoover Office: NMFS/OSF Phone: (301)427-8502 Email: alan.risenhoover@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: center;"> Digitally signed by RISENHOOVER.ALAN.D.1365879490 Date: 2018.02.02 08:49:06 -05'00'</p> <p>Signature: </p> <p>Date signed:</p>	<p>Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p style="text-align: center;">GRAFF.MARK. Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.02.14 13:54:27 -05'00'</p> <p>Signature: HYRUM.1514447892</p> <p>Date signed: 47892</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: National Fishing Permit and Landings Reporting System

FISMA Name/ID (if different): NOAA4011

Name of IT System/ Program Owner: Margo Schulz-Haugen

Name of Information System Security Officer: Wilbert Francis

Name of Authorizing Official(s): Alan Risenhoover

Date of Last PIA Compliance Review Board (CRB): 2/10/2017

(This date must be within three (3) years.)

Date of PIA Review: 1/30/2018

Name of Reviewer: Wilbert Francis

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: FRANCIS.WILBERT.R.1463197551 Digitally signed by FRANCIS.WILBERT.R.1463197551
Date: 2018.02.14 10:06:38 -05'00'

Date of Privacy Act (PA) Review: 2/13/2018

Name of Reviewer: Sarah Brabson

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Digitally signed by BRABSON SARAH 1365710488
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER,
cn=BRABSON SARAH 1365710488
Date: 2018.02.14 14:09:06 -05'00'

Date of BCPO Review: 2/14/18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: GRAFF.MARK.HYRU M.1514447892

Digitally signed by GRAFF MARK HYRUM 1514447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=OTHER, cn=GRAFF MARK HYRUM 1514447892
Date: 2018.02.14 13:55:03 -0500

**U.S. Department of Commerce
National Marine Fisheries Service**



**Privacy Threshold Analysis
for the
National Fisheries Permit and Landings Reporting System
(NFPLRS)**

U.S. Department of Commerce Privacy Threshold Analysis

National Fisheries Permit and Landing Reporting System (NFPLRS)

Unique Project Identifier: 006 03 02 00 01 0511 00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this information technology (IT) system. This PTA is primarily based on the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

The National Fishing Permit and Landings Reporting System (NFPLRS) allows members of the recreational and commercial fishing communities to acquire permits for certain species of fish, renew permits, report catch/landings, and access a library of related information (e.g., online brochures). The system also provides an information source to NMFS through real-time reports accessible via web browsers.

The secondary function in the system is Electronic Monitoring (EM). EM consists of monitoring catch/landings via video footage. The EM services support catch/landings data retrieval, catch/landings data analysis/review, and on-land data storage in order to support a program for approximately 135 vessels.

The system is part of the Office of Sustainable Fisheries and we coordinate as needed with the Office of Law Enforcement, and the NMFS Office of Management and Budget, which calculates applicable permit fees.

- Users include the general public, NMFS staff and customer service staff.
- Supported applications include excel spreadsheets, PDF files, database development and management, electronic mail, and web server applications.

The major functions the system provide are:

- Allow constituents to apply for and renew permits for highly migratory species (HMS), swordfish, and Atlantic tunas
- Accept reports of bluefin tuna, swordfish, and billfish landings
- Provide the public timely information regarding fisheries regulations
- Provide the public documents and forms related to fisheries activities and permitting

- Provide NMFS staff and customer service staff administrative access to permits
- Provide NMFS staff access to update information on the NFPLRS website.
- Provide enforcement agents access to permit status
- Provide NMFS staff with statistical reports on permit holdings and landings
- Provide users access to EM catch/landing footage and data
- Support fee collection

Major Functions/Applications

The NFPLRS integrates three functional mission applications.

Web Application

The NFPLRS website application provides general information about permits and facilitates online applications for HMS, swordfish, and Atlantic tunas permits. In addition, the system provides general documentation and guidance. The system also accepts information regarding HMS catch/landings. The web site is accessible from Internet and was developed using Java. The NMFS Permit website application stores data in the NFPLRS Database.

EM Data Review Application

EM Data Review Application (DRA) is a web-based application for reviewing videos and metadata captured from fishing vessels. The video footage only captures data related to fish caught/landed. This allows NFPLRS to monitor fishing activities of Atlantic tunas longline permit holders. The data is stored in Amazon Web Services (AWS) GovCloud utilizing S3 and AWS RDS database services. Prior to uploading files to AWS, videos go through a data pre-processing system (DPS). The servers hosting the DPS are located at ERT Office at Suite 100A, 8380 Colesville Road, Silver Spring, MD 20910.

Database

The NFPLRS and EM DRA applications both store data in AWS GovCloud. The database management system used is Oracle 11g for Windows. The database consists of tables, stored procedures, and constraints. These database servers are virtual machines that are secured and managed by AWS's Platform as a Service (PaaS) service offering.

Permit data is shared internally with NOAA NMFS/ Southeast Regional Office (SERO)/ Northeast Regional Office (NERO) and externally with Atlantic Coastal Cooperative Statistics Program (ACCSP). This system uses permit data to validate trip level reports.

Authorities: This data allows NMFS to manage living marine resources under U.S. jurisdiction under the authority of the Magnuson-Stevens Fishery Conservation and Management Act, the Marine Mammal Protection Act, Atlantic Tunas Convention Act (ATCA), the Endangered

Species Act (ESA), and the Highly Migratory Species Fishery Management Plan, as well as be compliant with international obligations pursuant to the International Commission for the Commission of Atlantic Tunas (ICCAT).

Questionnaire:

1. What is the status of this information system?

- This is a new information system. *Continue to answer questions and complete certification.*
- This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

- This is an existing information system in which changes do not create new privacy risks. *Note (Existing PTA requires that questions 2, 3 and 4 are reviewed and addressed for accuracy as well)*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

- Yes. *Please describe the activities which may raise privacy concerns.*

NFPLRS collects the following information from users in the process of submitting a permit request

- Vessel Information
 - Owners Name
 - Owners Address
 - Owners Telephone Number

- Owner's email address
- U.S. Coast Guard documentation number and/or state registration number for the vessel
- Vessel name
- Home port city & state
- Principal port city & state
- Length in feet
- Year built
- Crew size
- Construction (e.g., wood)
- Gross tonnage
- Propulsion (e.g., gasoline)
- Main engine horsepower
- Hold capacity in pounds (if applicable)
- Video footage of fishing activities.

No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

- Companies
- Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

I certify the criteria implied by one or more of the questions above **apply** to the **NFPLRS** and as a consequence of this applicability, a NMFS Permits PIA which includes this system's information has been submitted to DOC for review.

I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer (ISSO) or System Owner (SO):

Name: _____

Signature of ISSO or SO: BARRETT.KATHLEEN.E
LIZABETH.1516972480 Digitally signed by
BARRETT KATHLEEN ELIZABETH 1516972480
DN: c=US, o=U S Government, ou=DoD, ou=PKI
ou=OTHER
cn=BARRETT KATHLEEN ELIZABETH 1516972480
Date: 2017.09.18 17:04:29 -04'00' Date: _____


Information Technology Security Officer (ITSO):

Name: Richard Miner

Signature of ITSO:  Digitally signed by
MINER.RICHARD.SCOTT.139860451
9
Date: 2017.09.20 14:26:20 -04'00' Date: _____

Authorizing Official (AO):

Name: _____

Signature of AO:  Digitally signed by RISENHOOVER ALAN D 1365879490
DN: c=US, o=U S Government, ou=DoD, ou=PKI,
ou=OTHER, cn=RISENHOOVER ALAN D 1365879490
Date: 2017.09.16 17:34:20 -0400 Date: _____

Bureau Chief Privacy Officer (BCPO):

Name: _____

Signature of BCPO:  GRAFF.MARK.HY
RUM.1514447892 Digitally signed by GRAFF MARK HYRUM 1514447892
DN: c=US, o=U S Government, ou=DoD, ou=PKI,
ou=OTHER, cn=GRAFF MARK HYRUM 1514447892
Date: 2017.09.20 15:14:05 -0400 Date: _____

Sarah Brabson - NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Wednesday, February 14, 2018 9:03 AM
To: Mark Graff NOAA Federal
Subject: Re: NOAA4800 PTA for your signature
Attachments: NOAA4800 PTA 02 07 2018 signed (1).pdf

Here you go. thx

On Wed, Feb 14, 2018 at 8:54 AM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:
I think you forgot the attachment on this one.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
[\(301\) 628 5658](tel:3016285658) (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Wed, Feb 14, 2018 at 8:51 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
Mark, this is good except they forgot to insert the system name in the certification line. I am loathe to have them redo the NMFS signatures for that.

Could you please sign and return to me?

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce **(b)(6)**

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751

Ce (b)(6)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Mark Graff - NOAA Federal

From: Mark Graff NOAA Federal
Sent: Wednesday, February 14, 2018 9:22 AM
To: Sarah Brabson NOAA Federal
Subject: Re: NOAA4800 PTA for your signature
Attachments: NOAA4800 PTA 02 07 2018 signed (1) mhg.pdf

Signed and attached. Nice graphics :)

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Wed, Feb 14, 2018 at 9:02 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
Here you go. thx

On Wed, Feb 14, 2018 at 8:54 AM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:
I think you forgot the attachment on this one.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
[\(301\) 628 5658](tel:3016285658) (O)
(b)(6) (C)

Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Wed, Feb 14, 2018 at 8:51 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
Mark, this is good except they forgot to insert the system name in the certification line. I am loathe to have them redo the NMFS signatures for that.

Could you please sign and return to me?

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office [301 628 5751](tel:3016285751)
Ce (b)(6)

**U.S. Department of Commerce
National Oceanic and Atmospheric Administration**



**Privacy Threshold Analysis
for the NOAA4800 - Alaska Fisheries Science Center (AKFSC)
Network**

U.S. Department of Commerce Privacy Threshold Analysis
National Oceanic and Atmospheric Administration
NOAA4800 - Alaska Fisheries Science Center (AKFSC) Network

Unique Project Identifier: 006-03-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: The NOAA4800 system consists of a series of Local Area Networks (LANs) connected via a shared Wide Area Network (WAN) connection. The LANs are separated from the WAN by a firewall and router. Via the system identified as NOAA4000, NMFS CIO staff manage the WAN and all of the firewalls except for the Seattle LAN firewall. A common Active Directory, managed by the NMFS EAD staff, binds the LANs into one system. See diagram below.

System Specific Information:

- a) NOAA4800 is a General Support System.
- b) The primary site of NOAA4800 is Seattle, WA. Additional locations are Newport, OR, Juneau, AK, Anchorage, AK, Kodiak, AK, and Dutch Harbor, AK.
- c) NOAA4800 is interconnected with the NMFS LAN (NOAA4000), which provides transport services.
- d) The purpose of the NOAA4800 system is to provide information storage and computational resources for NOAA Fisheries scientists.
- e) In order to achieve its purpose, NOAA4800 provides connectivity between individual end-user computers to infrastructure devices such as files servers, through networking devices such as firewalls, routers, and switches.
- f) NOAA4800 collects, maintains, and uses several types of information, including natural resource data (conservation, marine ecosystems, and mammals), administrative data (budget formulation, budget planning), general workforce management data (number of contractors,

contracting budgets, etc.), and information technology data (help desk, infrastructure, system development, and security).

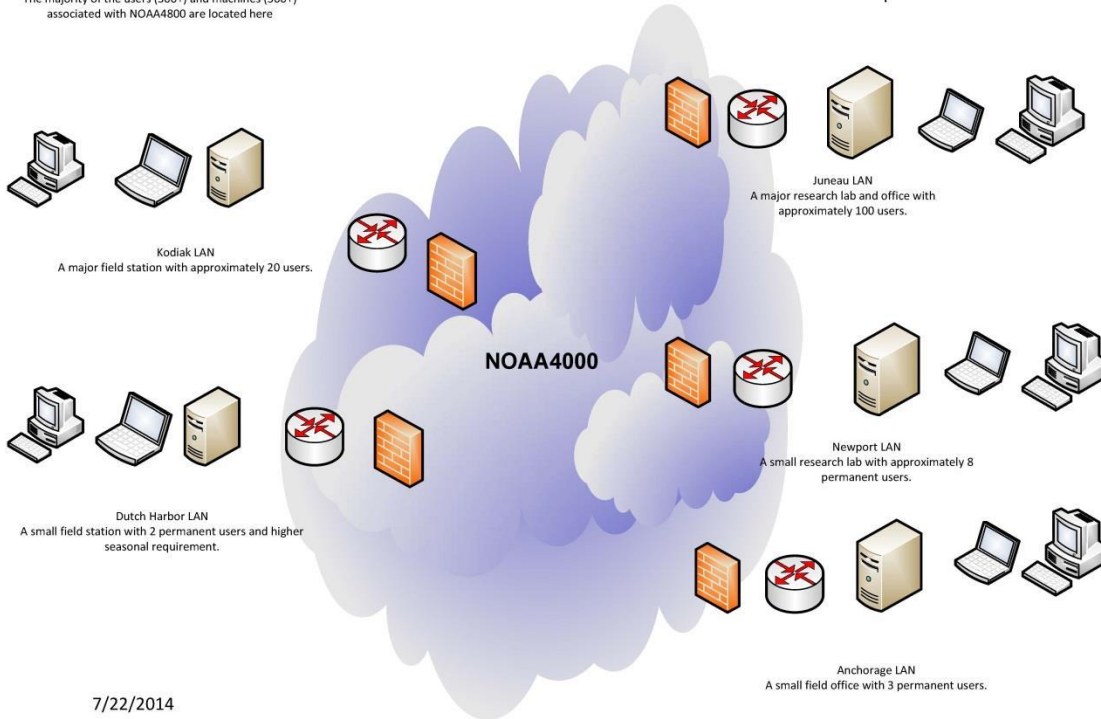
- g) A staff of approximately 500 people composed of biologists, physical scientists, administrative, and support professionals have access to information on the NOAA4800 system.
- h) Information is retrieved from servers to desktop and laptop computers via file sharing technologies.
- i) Information is transmitted locally via file sharing protocols, and externally via NOAA4000.



Seattle LAN
The majority of the users (300+) and machines (500+) associated with NOAA4800 are located here.

NOAA4800 System Description Diagram

This is a simplified description of how the various LANs that comprise NOAA4800 are interconnected. With the exception of the Seattle firewall, all routers and firewalls are managed by the NMFS OCIO WAN team as part of NOAA4000.



7/22/2014

Questionnaire:

1. What is the status of this information system?

This is a new information system. *Continue to answer questions and complete certification.*

This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Continue to answer questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *Please describe the activities which may raise privacy concerns.*

No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the

submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

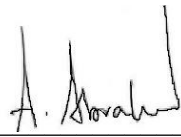
If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the [IT SYSTEM NAME] and as a consequence of this applicability, I will perform and document a PIA for this IT system.

I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Ajith Abraham

Signature of SO:  Digitally signed by ABRAHAM.AJITH.1365899238 Date: 2018.02.07 08:22:31 -08'00'

Name of Information Technology Security Officer (ITSO):

Signature of ITSO: AMORES.CATHERINE.SOLEIDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEIDAD.1541314390 Date: 2018.02.13 13:20:28 -05'00' Date:

Name of Authorizing Official (AO): Jeremy Rusin

Signature of AO: RUSIN.JEREMY.DEWITT.1380624407 Digitally signed by RUSIN.JEREMY.DEWITT.1380624407 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=RUSIN.JEREMY.DEWITT.1380624407 Date: 2018.02.07 13:35:40 -08'00' Date:

Name of Bureau Chief Privacy Officer (BCPO):

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.02.14 09:16:08 -05'00' Date:

Andre Sivels - NOAA Federal

From: Andre Sivels NOAA Federal
Sent: Wednesday, February 14, 2018 4:09 PM
To: Mark Graff NOAA Federal
Subject: Records Transfer Procedures
Attachments: SF 135 form for FOIA Records Example.pdf; RECORDS DESTRUCTION REQUEST FORM example for FOIA Records.doc; Chapter 200 Administrative and Housekeeping Records.pdf; Records Transfer Process (4).ppt

Hi Mark

Please contact GSA at [1 800 525 8027](tel:18005258027) to request Records Center Cartons. The item number is NSN 8118 00 117 8249. The cartons are sent in a bundle of 25. A good way to estimate the number of boxes needed is to use the conversion of (1) lateral file cabinet or 36 linear inches = (3) Records Center Cartons. Please do not put hanging file folders in the boxes, just pack with regular folders in a logical order, and leave 1 inch of space from the inside edges of the box .

1. Records Transfer Process:

1. See the attached Sf 135 form as a guide for the required information. I will need to input your data from the SF 135 form into the ARCIS system for approval. You would just need to update the attached SF 135 form with the correct number of boxes and date range and return to me.
2. After packing boxes, please send me a box index or inventory listing of what is in each box. Nothing fancy, it can be a word document, spreadsheet or printout. I must also submit the box index as part of the transfer request.
3. Once I enter the required data, I will receive a transfer number for you to enter on each box. Each box must be number sequentially as well.
4. After a couple days, I will check the ARCIS system for an "Approved" status. Once the transfer is approved, I will contact NARA's transportation office to schedule the records for pick up and confirm the pick up date with you.
5. NARA will pick up the records from the designated staging area on your floor and deliver the Washington National Records Center(WNRC) in Suitland MD. They normally call me an hour before pick up. I normally escort the NARA staff throughout to process..

I have attached a slide deck outlining the transfer procedures for you to use as a guide for sorting, packing and labeling boxes. Once you send me the updated Sf 135, I will handle the process from there. (FYI) I will be updating transfer procedures on a new Bi fold bulletin later this year.

2. Records Disposal

See the attached disposal form as a guide to for recording disposal data. The Record Disposal form should be completed and signed before the records are destroyed. Let me know if you need a vendor for records

disposals.

See item 205 on the attached Administrative and Housekeeping Schedule for FOIA related records schedules. Please contact me if you have any additional questions. Thanks again.

Andre

Andre Sivels
NOAA Records Officer
U.S. Department of Commerce
1305 East West Highway Rm 7439
Silver Spring, MD 20910
Phone: 301628 0946
Fax: [301 713 1169](tel:3017131169)

(Revised on 10/2017 to include Updates to Several GRS Schedules)

NOAA Records Schedules
Chapter 200
Administrative and Housekeeping Records

Chapter 200 Table of Contents

200	Administrative and Housekeeping Records
200-01	Office Administrative Files
200-02	Files Planning, Organization, and Maintenance: Designating Files
200-03	Suspense Log
200-04	Schedules of Daily Activities
200-05	Transitory Records (First bullet only)
200-06	Library Records
200-07	Technical Reference Materials
200-08	Non-Recordkeeping Copies of Electronic Records
200-09	Intermediary Records
200-10	Records of Non-Mission Related Internal Agency Committees (Removed from 100-17)

201 Management Control Records

201-01 Audit and Investigation Case Files

201-02 Deemed Export Program Files

201-03 Management Control Records

201-04 Project Control Files

201-05 Feasibility Studies

201-06 Report Control Files

202 BUDGET AND FINANCE RECORDS

202-01 Budget Background Records

202-02 Budget Estimates and Narrative Statement Records

202-03 Budget Correspondence Files

202-04 Agency-wide Budget Projection Records

- 202-05 Electronic Budget Tracking Records
- 202-06 Credit/Bank Card Transactions
- 202-07 General Correspondence Files
- 202-08 Federal Financial System Data Input Records
- 202-09 Fund Use and Availability Records
- 202-10 Routine Procurement/Contract Records **(Administrative copies only, see Chapter 700 for program records)**

203 HUMAN RESOURCES RECORDS

- 203-01 Time and Attendance Input Records
- 203-02 Time and Attendance Source Records
- 203-03 Personnel Records: Supervisor's and Duplicate Official Personnel Folder Documentation
- 203-04 Training and Workshop Records
- 203-05 Telework Agreement Records
- 203-06 Equal Employment Opportunity (EEO) General Records **(See Chapter 302 for EEO program records)**

204 RECORDS MANAGEMENT PROGRAM

- 204-01 Tracking and Control Records
- 204-02 Records Management Program Records
- 204-03 Vital or Essential Records Program Records
- 204-04 Copies of Vital Records
- 204-05 Forms Management Records
- 204-06 Email Managed Under a Capstone Approach
- 204-07 Email of Non-Capstone Officials

205 INFORMATION RESOURCE MANAGEMENT RECORDS

- 205-01 FOIA, Privacy Act, and Classified Documents Administrative Records
- 205-02 General Information Request Files
- 205-03 Access and Disclosure Request Files
- 205-04 Information Access and Protection Operational Records
- 205-05 Accounting for and Control of Access to Classified and Controlled Unclassified Records and Records Requested Under FOIA, PA, and MDR

- 205-06 Privacy Act Accounting of Disclosure Files
- 205-07 Erroneous Release Records
- 205-08 Agency Reports to the Congress, Department of Justice, or other Entities Regarding FOIA, MDR, PA, and Similar Access and Disclosure Programs
- 205-09 Legal and Regulatory Compliance Reporting Records
- 205-10 Privacy Act Amendment Request Files
- 205-11 Automatic and Systematic Declassification Review Program Records
- 205-12 Fundamental Classification Guidance Review Files
- 205-13 Classified Information Nondisclosure Agreements
- 205-14 Personally Identifiable Information Extracts
- 205-15 Personally Identifiable Information Extract Logs
- 205-16 Privacy Act System of Records Notices (SORNs)
- 205-17 Records Analyzing Personally Identifiable Information (PII)
- 205-18 Computer Matching Program Notices and Agreements
- 205-19 Virtual Public Access Library Records

206 Administrative Help Desk Records

206-01 Technical and Administrative Help Desk Operational Records

207 Public Customer Service Records

207-01 Public Customer Service Operations Records

207-02 Customer/Client Records

Series #	Records Series Title	Records Description	Disposition Authority	Disposition Instruction
200	Administrative Management and Housekeeping Records.	This Chapter lists the most common administrative and housekeeping records that are maintained in all levels of NOAA offices. These records include routine and facilitative records that many or all government agencies create and maintain for day-to-day administrative and management functions. These functions are already scheduled in the General Records Schedule (GRS) , issued and approved by the National Archives and Records Administration (NARA) , or by a SF-115 approved and signed by the Archivist of the United States at NARA.		
200-01	Administrative Records Maintained in any Agency Office.	Records accumulated by individual offices that relate to routine day-to-day administration and management of the office rather than the mission-specific activities for which the office exists. Records include: <ul style="list-style-type: none"> • staff locators, unofficial organizational 	DAA-GRS- 2016-0016-0001 (GRS 5.1, item 010) <i>Supersedes NOAA Schedule Item 201-01 (GRS 23, item 1)</i>	TEMPORARY. Destroy when business use ceases.

		<p>charts, and office seating charts (see Exclusion 1)</p> <ul style="list-style-type: none">• office-level administrative policies and procedures and files related to their development (see Note 1)• calendars or schedules of daily activities of non-high-level officials (high-level officials are defined in GRS 6.1; this item covers those positions not defined as high-level)• informal requests and tracking of personnel training, travel, supplies, and equipment, excluding procurement and payment records and forms requesting training (e.g. SF-182)• internal office activity and workload reports• studies and analyses of office administrative functions and activities• non-mission related management reviews and surveys• minutes of meetings related to administrative activities <p>Exclusion 1: This item does not apply to</p>		
--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

		<p>recordkeeping copies of organizational charts, functional statements, and related records that document the mission-related organization, staffing, and procedures of the office. Agencies must schedule those records on an agency-specific schedule.</p> <p>Note 1: <i>This item covers administrative policies and procedures at the office/unit level. See NOAA Series 100-03 for agency-level administrative issuances; directives, bulletins, organization manuals and charts, functional statements, delegations of authority, and similar administrative issuances and manuals.</i></p>		
200-02	Files Planning, Organization, and Maintenance: Designating Files Stations	<p>An office file plan must be created for each file location. The file plan lists each record series maintained by the office, the disposition instruction for the series, and its location. A copy of the plan should be filed in the front of the first drawer of the first cabinet at each file location. Copies of the plan, or consolidated plans, may be kept at other file locations - higher level offices, or individual desks, if such reference needs exist. Each office must have its file plan approved by the proper Records Liaison Officer/and Records Officer.</p>	<p>DAA-GRS-2013-0002-0016 (GRS 4.1, Item 010)</p> <p><i>Previously, NOAA Schedule Item 200-47, (N1-74-228, item 1).</i></p>	<p>TEMPORARY. Destroy when no longer needed.</p> <p>Note: <i>There must be an active file plan before a superseded file plan can be destroyed.</i></p>
200-03	Suspense Logs	<p>Documents arranged in chronological order as a reminder that an action is required on a given date or that a reply to action is</p>	<p>DAA-GRS-2017-0003-0001 (GRS 5.2, item 010)</p>	<p>TEMPORARY. Follow disposition for 200-05 below.</p>

		expected and, if not received, should be traced on a given date.	<i>Supersedes NOAA Schedule Item 200 03 (GRS 23, item 6a and b)</i> <i>Previously, NOAA Schedule Item 200-29.</i>	
		a. A note or other reminder to take action:		TEMPORARY. Destroy after action is taken.
		b. The record copy or an extra copy of an out-going communication, filed by the date on which a reply is expected.	<i>Supersedes NOAA Schedule Item 200 03 (GRS 23, item 6b)</i> <i>Previously, NOAA Schedule Item 200-29.</i>	TEMPORARY. Withdraw documents when reply is received. (1) If suspense copy is an extra copy, destroy immediately. (2) If suspense copy is the record copy, incorporate it into the official files.
200-04	Schedules of Daily Activities.	Calendars, appointment books, schedules, logs, diaries, and other records documenting meetings, appointments, telephone calls, trips, visits and other activities by federal employees while serving in an official capacity, created and maintained in hard copy or electronic form.		
		a. Records containing substantive information relating to official activities, the substance of which has not been incorporated into official records, at the	DAA-GRS-2016-0016-0001 (GRS 5.1, item 010) <i>Supersedes NOAA</i>	TEMPORARY. Follow the disposition instructions for

		<p><u>division level and below.</u></p> <p>Note: High level officials include the heads of departments and independent agencies; their deputies and assistants; the heads of program offices and staff offices including assistant secretaries, administrators, and commissioners; directors of offices, bureaus, or equivalent; principal regional officials; staff assistants to those aforementioned officials, such as special assistants, confidential assistants, and administrative assistants; and career Federal employees, political appointees, and officers of the Armed Forces serving in equivalent or comparable positions.</p> <p>See the 100 records series for Schedules of Daily Activities for High Level Officials.</p>	<p>Schedule Item 200-04 (GRS 23, item 5a)</p> <p>Previously, NOAA Schedule Item 200-27.</p>	200-05 below.
		<p>b. Records documenting routine activities containing no substantive information and records containing substantive information which has been incorporated into organized files</p>	<p>DAA-GRS-2016-0016-0001 (GRS 5.1, item 010)</p> <p><i>Supersedes NOAA Schedule Item 200 04 (GRS 23, item 5b)</i></p> <p>Previously, NOAA Schedule Item 200-27.</p>	<p>TEMPORARY. Follow the disposition instructions for 200 05 below.</p>
200-05	Transitory Records	<p>Records required only for a short time (generally less than 180 days) and that are not required to meet legal or fiscal</p>	<p>DAA-GRS-2017-0003- 0001 (GRS 5.2, item, 010)</p>	<p>TEMPORARY. Destroy when no longer needed for</p>

		<p>obligations, or to initiate, sustain, evaluate, or provide evidence of decision making. Records include, but are not limited to:</p> <ul style="list-style-type: none"> • messages coordinating schedules, appointments, and events • transmittal documents such as e-mail, letters, cover memos, and facsimile cover sheets that do not provide evidence of approval, concurrence, or decision-making, or include substantive comments • received copies of circulated internal information such as agency instructions, notifications, circulars, newsletters, and email blasts to employees • messages received from agency distribution lists or listservs • “to-do” or task lists and assignments 	<p><i>Supersedes NOAA Schedule Item 200-05 (GRS 23, item 7)</i> <i>Previously, NOAA Schedule Item 200-07.</i></p>	<p>business use, or according to agency predetermined time period or business rule.</p>
200-06	Library Records.	<p>Documents made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications.</p> <p>Note: Does not include Library Program Records.</p>	<p>Nonrecord, authorized disposition is not required.</p> <p><i>Previously, NOAA Schedule Item 200-21.</i></p>	<p>Discard when superseded or no longer needed, upon approval of supervisor.</p>
200-07	Technical Reference Materials	<p>Publications, phone books, extra copies of administrative or procedure manuals, and</p>	<p>Nonrecord, authorized disposition is not</p>	<p>TEMPORARY. Discard when</p>

		directives acquired and preserved solely for reference, or stocked for general distribution or handout.	required. <i>Previously, NOAA Schedule Item 200-30.</i>	superseded or no longer needed.
200-08	Non-Recordkeeping Copies of Electronic Records.	<p>Non-recordkeeping copies of electronic records agencies maintain in email systems, computer hard drives or networks, web servers, or other locations after agencies copy the records to a recordkeeping system or otherwise preserve the recordkeeping version. This includes:</p> <ul style="list-style-type: none"> • documents such as letters, memoranda, reports, handbooks, directives, manuals, briefings, or presentations created on office applications, including those in Portable Document Format (PDF) or its equivalent • senders' and recipients' versions of electronic mail messages that meet the definition of Federal records, and any related attachments • electronic spreadsheets • digital still pictures or posters • digital video or audio files • digital maps or architectural drawings • copies of the above electronic records maintained on websites or web servers, but EXCLUDING web pages themselves 	<p>DAA-GRS-2016-0016- 0002 (GRS 5.1, item 020) <i>Supersedes GRS 4.3, 040.</i></p>	<p>TEMPORARY. Destroy immediately after copying to a recordkeeping system or otherwise preserving, but longer retention is authorized if required for business use.</p>

		<p>Note 1: <i>Non-recordkeeping copies may be Federal records. Often, copies are non-records and can be immediately destroyed, but not always. Copies are non-record if they are kept only for convenience of reference. If copies are used in the course of agency business to make decisions or take action, they are Federal records. The copies described here are Federal records if they are still being used by the agency for such business purposes, but are not recordkeeping copies of those records.</i></p> <p>Note 2: <i>For electronic mail records, the recordkeeping system must capture the names of sender and recipients, date (transmission data for recordkeeping purposes), and any receipt data, along with the message text. Sender/recipient information should be individual account information, not the name of a distribution list.</i></p>		
200-09	Intermediary Records.	<p>Records of an intermediary nature, meaning that they are created or used in the process of creating a subsequent record. To qualify as an intermediary record, the record must also not be required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision-making. Records include:</p>	<p>DAA-GRS-2017-0003- 0002 (GRS 5.2, item 020) <i>Supersedes GRS 4.3, 040.</i></p>	<p>TEMPORARY. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is</p>

		<ul style="list-style-type: none">• non-substantive working files: collected and created materials not coordinated or disseminated outside the unit of origin that do not contain information documenting significant policy development, action, or decision making. These working papers do not result directly in a final product or an approved finished report. Included are such materials as rough notes and calculations and preliminary drafts produced solely for proof reading or internal discussion, reference, or consultation, and associated transmittals, notes, reference, and background materials.• audio and video recordings of meetings that have been fully transcribed or that were created explicitly for the purpose of creating detailed meeting minutes (once the minutes are created)• dictation recordings• input or source records, which agencies create in the routine process of creating, maintaining, updating, or using electronic information systems and which have no value beyond the input or output transaction:		later.
--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--------

		<p>o hardcopy input source documents where all information on the document is incorporated in an electronic system (See Exclusion 1 and Note 1)</p> <p>o electronic input source records such as transaction files or intermediate input/output files</p> <ul style="list-style-type: none">• ad hoc reports, including queries on electronic systems, whether used for one-time reference or to create a subsequent report• data files output from electronic systems, created for the purpose of information sharing or reference (see Exclusion 2) <p>Exclusion 1: This item does not allow destruction of original hardcopy still pictures, graphic materials or posters, aerial film, maps, plans, charts, sound recordings, motion picture film, or video recordings once they are digitized. Agencies must follow agency-specific schedules for these records. If the records are unscheduled, the agency must submit a schedule for them.</p>		
--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

		<p>Exclusion 2: This item does not include the following data output files (agencies must follow agency-specific schedules for these records, except for the final bullet, which the GRS covers in another schedule):</p> <ul style="list-style-type: none">• files created only for public access purposes• summarized information from unscheduled electronic records or inaccessible permanent records• data extracts produced by a process that results in the content of the file being significantly different from the source records. In other words, the process effectively creates a new database file significantly different from the original• data extracts containing Personally Identifiable Information (PII). Such records require additional tracking and fall under GRS 4.2, item 130 (DAA-GRS-2013-0007-0012) <p>Note 1: <i>An agency must submit a notification to NARA per 36 CFR 1225.24(a)(1) prior to destroying hardcopy input records previously scheduled as permanent. An agency must schedule the electronic version of unscheduled hardcopy input records prior to destroying the input record.</i></p>		
--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

		Legal citations: 36 CFR 1225.22 (h)(2); 36 CFR 1225.24 (a)(1)		
200-10	Records of Non-Mission Related Internal Agency Committees.	<p>Records created and maintained by committees established by an agency for facilitative or operational purposes unrelated to the agency's mission, such as organizing events, selecting interior furnishings, overseeing volunteer activities, or employee recreational activities. Records include:</p> <ul style="list-style-type: none"> • meeting minutes, summaries, agendas, and transcripts • reports and studies • membership records • correspondence, mailing, and distribution records <p>Exclusion: These items do not cover records of Federal Advisory Committee Act or interagency committees. GRS 6.2 covers Federal Advisory Committee Act committee records.</p> <p>Note: Records of mission-related committees are potentially permanent and</p>	<p>DAA-GRS-2016-0016-0003 (GRS 5.1, item 030)</p> <p><i>Supersedes NOAA Series 100 17, N1 370 90 3 (12/9/92) and GRS 26, item 1a</i></p>	<p>TEMPORARY. Destroy when business use ceases.</p>

		agencies must schedule them by an agency-specific records schedule.		
--	--	---------------------------------------------------------------------	--	--

Series #	Records Series Title	Records Description	Disposition Authority	Disposition Instruction
201	Management Control Records.			
201-01	Audits and Investigation Case Files.	<p>The NOAA Office of Audits provides direction and guidance to NOAA offices on the development of responses to the Department of Commerce, (DOC), Office of Inspector General (OIG) and Government Accountability Office (GAO) regarding audits and investigations. In addition, the NOAA Office of Audits assists in negotiation and resolution of disputed findings and recommendations and ensures that responses to the OIG reflect the NOAA perspective. The Final Reports of Audits and Investigations are issued and maintained by the Department of Commerce (DOC), Office of the Inspector General; however the NOAA Office of Audits retains a copy of the Report of Findings, and background and supporting material accumulated to document the audit or investigation. NOAA Office of Audits follows the guidance, policies, manuals and operating procedures issued by the DOC, Office of Inspector General.</p>	<p>DAA-0370-2015-0006 (03/04/16)</p> <p>Supersedes NOAA Schedule Item N1-370-99-6.</p> <p><i>Previously, NOAA Schedule Item 200-02.</i></p>	

		The following records series are created and maintained by the Office of Audits to support its programmatic and recordkeeping responsibilities. The records series cited in this schedule are media neutral.		
	Audit Case Files.	<i>Supersedes N1-370-99-06, item 1, Audit Case Files.</i> Case files of internal and external audits of agency programs, operations, and procedures, including contractors and grantees, containing audit reports, correspondence, memoranda, and supporting working papers.		
		a (1). Records Maintained by NOAA Office of Audits.	DAA-370-2015-0006-0001 (03/04/16)	TEMPORARY. Cut off at the end of FY in which case is closed Destroy 8 year(s) after cutoff.
		a (2). Records Maintained by NOAA Line and Staff Offices	DAA-370-2015-0006-0002 (03/04/16)	TEMPORARY. Cut off at the end of FY. Destroy 8 year(s) after cutoff.
	Inspector General Complaint Case Files.	Record documents NOAA Office of Audits investigations of allegations of known or alleged fraud and abuse, irregularities and violations of laws and regulations, mismanagement, gross waste of funds, abuse of authority or a substantial and specific danger to the public health and		

		<p>safety involving NOAA. These cases are initiated through a referral from the DOC, Office of Inspector General requesting the NOAA Office of Audits to investigate a specific matter. These cases may relate to agency personnel and programs and operations administered or financed by the agency, including contractors and others having a relationship with the agency.</p> <p>At the conclusion of the internal investigation, the NOAA Office of Audits responds to the DOC, Office of the Inspector General with a report of its finding. The NOAA Office of Audits retains a copy of the Report of Findings and internal investigative reports, correspondence, notes, attachments, and working papers which are collected or created to document their review, investigation of an activity or complaint. The NOAA program office that is the subject to the inquiry or allegation also establishes and maintains a record of the inquiry or allegation which may include, but not limited to, preliminary drafts, working files, meeting notes and other information supporting their review and response to the allegation.</p>		
		<p>b (1). Records Maintained by NOAA</p>	<p>DAA-0370-2015-0006-0003</p>	<p>TEMPORARY. Cut off</p>

		Office of Audits.	(03/04/16)	at the end FY in which case is closed. Destroy 10 year(s) after cutoff or when no longer needed for research and investigative purposes occurs, whichever is later.
		b (2). Records Maintained by NOAA Line and Staff Offices.	DAA-0370-2015-0006-0004 (03/04/16)	TEMPORARY. Cut off at the end FY in which case is closed. Destroy 10 year(s) after cutoff or when no longer needed for research or investigative purposes occurs, whichever is later.
	Files Containing Information or Allegations Which are of an Investigative Nature but do not Relate to a Specific Investigation.	These records include anonymous or vague allegations not warranting an investigation, matters referred to constituents or other agencies for handling, and support files providing general information that may prove useful in Inspector General Investigations.		
		c (1). Records Maintained by NOAA Office of Audits.	DAA-0370-2015-0006-0005 (03/04/16)	TEMPORARY. Cut off at the end FY in which case is closed. Destroy 5 year(s) after cutoff.

		c (2). Records Maintained by NOAA Line and Staff Offices.	DAA-0370-2015-0006-0006 (03/04/16)	TEMPORARY. Cut off at the end FY in which case is closed. Destroy 5 year(s) after cutoff.
201-02	Deemed Export Program Records.	Records derived from any release of source code subject to the Export Administration Regulations (EAR) to a foreign national within the United States. Such a release is deemed to be an export to the home country or countries of the foreign national. All records are media neutral.	<i>Previously, NOAA Schedule Item 200-23.</i>	
		1. Records Maintained by the Chief Administrator		
		a. Controlled Technology Inventory – This record captures data including, but not limited to, the name of the equipment/technology/item, the Export Control Number (ECCN), the description and location of the equipment, and the responsible NOAA manager, and whether or not access to the controlled technology is required by a foreign national and, if so, whether or not a license would be required for access.	DAA-0370-2013-0001-0001 (Sequence No. 1.1)	TEMPORARY. Cut off list at the end of FY and destroy 5 year(s) after cutoff.
		b. Deemed Export Licenses Record that identifies the foreign national and the controlled technology	DAA-0370-2013-0001-0002 (Sequence No. 1.2)	TEMPORARY. Cut off list at the end of FY and destroy year(s) after cutoff.

		which licenses have been obtained. A record of any licenses issued by BIS is also maintained.		
		<p>c. Foreign National List</p> <p>This record captures data including, but not limited to, the name of the foreign national as well as their county or citizenship, home country, duty station, description of work, and Federal employee sponsor. This record also identifies whether or not the foreign national requires access to controlled technology and whether or not a license would be required for such access.</p>	DAA-0370-2013-0001-0003 (Sequence No. 1.3)	TEMPORARY. Cut off list at the end of FY and destroy 5 years after cutoff.
		2. Records Maintained in the Line Offices (LOs) and Staff Offices (SOs)		
		<p>a. Access Control Plans</p> <p>Records containing sufficient measures, safeguards, and procedures to ensure full EAR/ITA compliance to protect against unauthorized release of controlled technology to foreign nationals, at each facility/lab/program office. Each piece of controlled equipment/technology must have an accompany Access Control Information Sheet that identifies all measures and procedures to control foreign nation access to the controlled technology regulated under EAR/ITAR.</p>	DAA-0370-2013-0001-0004 (Sequence No. 2.1)	TEMPORARY. Destroy 5 years after plan is superseded.
		b. Certification Statements	DAA-0370-2013-0001-0005	TEMPORARY. Cut

		Annual certification signed by the LO/DAA or SO Director including DAA/SO Director Certification Statement, controlled technology inventory, list of foreign national Guests, Access Control Plans, list of deemed exports censes, and a list of facilities/labs/programs that completed the controlled technology assessment.	(Sequence No. 2.2)	off at the end of the FY, and destroy 5 years after cut off.
		3. NOAA Endorsement Supplement (ESF) for the Line Office (LO)/Staff Office Department Sponsor/NOAA (DSN) and NAO 200-12, Appendix B. The ESF documents that DOC Sponsor/NOAA (DSN) has balanced the need to collaborate with a foreign national with the need to protect sensitive agency assets. The LO/SO and DSN certifies the ESF that the facility/lab/program has been assessed for export controlled technology, the DSN certifies on the ESF that he/she has taken reasonable steps to ensure that foreign nationals will not have unauthorized physical access to classified, sensitive, or not for public release data, information, or technology, etc. The form is also signed by the LO/SO Controlled Technology Coordinator (CTC) or the DAA as the designated official.		
		a. Records Maintained by the Chief	DAA-0370-2013-0001-0006	TEMPORARY.

		Administrator	(Sequence No. 3.1)	Destroy 5 year(s) after cut off.
		b. Records Maintained in the Line Offices (LOs) and Staff Offices (SOs).	DAA-0370-2013-0001-0007 (Sequence No. 3.2)	TEMPORARY. Destroy 5 year(s) after cut off.
		4. Summary Reports of Department Administrative Order (DAO)/NOAA Administrative Order 207-12 Violations. The report focuses on the circumstances surrounding the violation and actions to prevent future occurrences. The report also addresses the potential of unauthorized release of controlled technology or otherwise sensitive data or information to the subject foreign national.		
		a. Records Maintained by Office of the Chief Administrative Officer (OCAO)	DAA-0370-2013-0001-0008 (Sequence No. 4.1)	TEMPORARY. Destroy 5 year(s) after cut off.
		b. Records Maintained in the Line Offices (LOs) and Staff Offices (SOs)	DAA-0370-2013-0001-0009 (Sequence No. 4.2)	TEMPORARY. Destroy 5 year(s) after cut off.
201-03	Management Control Records	Records created in accordance with procedures mandated by OMB Circular A-123, Management Accountability and Control Systems, and Pub.L. 97-255, the Federal Managers' Financial Integrity Act. Under these authorities, agencies are	<i>Previously, NOAA Schedule Item 200-39.</i>	

		required to perform evaluations of their accounting and administrative controls to prevent waste, fraud, and mismanagement.		
		<p>a. Policy, procedure, and guidance files.</p> <p>Copies of internal directives maintained by the agency's internal control staff (but not those copies maintained in the agency's official file of internal directives); external directives such as OMB Circular A-123; and correspondence outlining policy and procedure for performing management reviews.</p>	GRS 16, item 14a	TEMPORARY. Destroy when superseded.
		<p>b. Management control plans.</p> <p>Comprehensive plans documenting the agency's efforts to ensure compliance with OMB Circular A-123.</p>	GRS 16, item 14b	TEMPORARY. Destroy when superseded.
		<p>c. Risk analyses.</p> <p>Reports and supporting materials used to document review of program areas for susceptibility to loss or unauthorized use of resources, errors in reports and information, and illegal and unethical actions.</p>	GRS 16, item 14c	TEMPORARY. Destroy after next review cycle.
		<p>d. Annual reports and assurance statements created by organizational components below the agency</p>	GRS 16, item 14d	TEMPORARY. Cut off closed files annually. Destroy after next

		<p>(department or independent agency) level and compiled by the agency into a single unified report for direct submission to the President or Congress.</p> <p><i>[NOTE: This item does not cover the consolidated final reports submitted directly to the President or Congress. The final reports must be scheduled by submitting an SF 115 to NARA.]</i></p>		reporting cycle.
		<p>e. Tracking files.</p> <p>Files used to ensure the completion and timeliness of submission of feeder reports, including schedules of evaluations, interim reporting, lists of units required to report, and correspondence relating to the performance of the reviews.</p>	GRS 16, item 14e	TEMPORARY. Destroy 1 year after report is completed.
		<p>f. Review files. [See note after item 14f(2).]</p> <p>Correspondence, reports, action copies of audit findings, and other records that identify program internal control weaknesses, and corrective actions taken to resolve such problems. Since A-123 provides for alternative internal control reviews under OMB Circulars A-76, A-127, or A-130, this item also applies to copies of these reviews, provided they are</p>		

		identified as alternative reviews in the management control plan.		
		(1) Office with responsibility for coordinating internal control functions.	GRS 16, item 14f(1)	TEMPORARY. Cutoff when no further corrective action is necessary. Destroy 5 years after cutoff.
		(2) Copies maintained by other offices as internal reviews. <i>[NOTE: Alternative reviews such as computer security reviews and management and consultant studies may need to be kept longer than provided in item 14f(2). This item applies only to copies maintained as internal reviews.]</i>	GRS 16, item 14f(2)	TEMPORARY. Cut off when no further corrective action is necessary. Destroy 1 year after cutoff.
201-04	Project Control Files	Memoranda, reports, and other records documenting assignments, progress, and completion of projects.	GRS 16, item 5 <i>Previously, NOAA Schedule Item 200-41.</i>	TEMPORARY. Destroy 1 year after the year in which the project is closed.
201-05	Information Technology Development Project Records. (Feasibility Studies)	Infrastructure project records. Information Technology (IT) infrastructure, systems, and services project records document the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications. Includes requirements for and implementation of	DAA-GRS-2013-0050007 (GRS 3.1, item 011) <i>Supersedes NOAA Schedule 200-43, (GRS 16, item 9, Feasibility Studies).</i>	TEMPORARY. Destroy 5 years after project is terminated, but longer retention is authorized if required for business use.

		<p>functions such as:</p> <ul style="list-style-type: none">• maintaining network servers, desktop computers, and other hardware,• installing and upgrading network operating systems and shared applications, and• providing data telecommunications; and infrastructure development and maintenance such as acceptance/authorization of infrastructure components, analysis of component options, feasibility, costs and benefits, and work associated with implementation, modification, and troubleshooting <p>Includes records such as:</p> <ul style="list-style-type: none">• installation and testing records• installation reviews and briefings• quality assurance and security review• requirements specifications• technology refresh plans • operational support plans• test plans		
--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

		<ul style="list-style-type: none"> models, diagrams, schematics, and technical documentation <p>Exclusion: Records relating to specific systems that support or document mission goals are not covered by this item and must be scheduled individually by the agency by submission of a records schedule to NARA.</p> <p><i>Note: Records concerning the development of each information technology (IT) system and software application are covered under the item for System Development Records.</i></p>		
201-06	Reports Control Files	Case files maintained for each agency report created or proposed, including public use reports. Included are clearance forms, including OMB 83 (formerly SF 83); copies of pertinent forms or descriptions of format; copies of authorizing directives; preparation instructions; and documents relating to the evaluation, continuation, revision, and discontinuance of reporting requirements.	GRS 16, item 6	TEMPORARY. Destroy 2 years after the report is discontinued.

Series #	Records Series Title	Records Description	Disposition Authority	Disposition Instruction
202	Budget and Finance Records			
202-01	Budget Background Records	Program office copies of materials which constitute program office input during the annual budget formulation cycle and the budget execution phase. Cost statements, rough data, and similar materials accumulated in the preparation of annual budget estimates, including duplicates of budget estimates and justifications and related appropriation language sheets, narrative statements, and related schedules, and originating offices' copies of reports submitted to budget offices.	GRS 5, item 2 <i>Previously, NOAA Schedule Item 200-03.</i>	TEMPORARY. Recordkeeping paper copy: Destroy 1 year after the close of the fiscal year covered by the budget.
202-02	Budget Estimate and Narrative Statement Records	Documents pertaining to budget estimates prepared or consolidated by budget offices; and including appropriation language sheets, narrative statements, and papers related to associated meetings and briefings. <i>Note: These records are located in the NOAA Budget Office only. All other offices, use 200-03.</i>	NC1-370-74-228 <i>Previously, NOAA Schedule Item 200-04.</i>	PERMANENT. Cut off at end of fiscal year. Transfer to the FRC two years after closure. Transfer to the National Archives 20 years after closure.
202-03	Budget Correspondence Files.	Correspondence files in a formally organized budget office pertaining to	GRS 5, item 1	TEMPORARY. Destroy when 2 years

		routine administration, internal procedures, and other matters not covered elsewhere in this schedule, EXCLUDING files relating to agency policy and procedure maintained in formally organized budget offices.	<i>Previously, NOAA Schedule Item 200-38.</i>	old.
202-04	Agency-wide Budget Projection Records	Projections of resources needed to meet program needs and future goals. These projections are made by the office responsible for oversight of the program area.	<i>Previously, NOAA Schedule Item 200-05.</i>	
		a. Projections not duplicated in budget submissions that deal with overall program.	NC1-370-76-5, item 9a (8/6/76)	TEMPORARY. Recordkeeping paper copy records: Close files at the end of FY and transfer to the FRC after 3 years. Destroy 10 years after closure.
		b. Projections which are "feeder" reports to those in "a" above or which are duplication in budget submissions.	NC1-370-76-5, item 9b (8/6/76)	TEMPORARY. Destroy when 5 years old
202-05	Electronic Budget Tracking Records	Electronic spreadsheets used to track office expenditures for budgetary control.	DAA-GRS- 2016-0016-0001 (GRS 5.1, item 010) <i>Supersedes NOAA Schedule Item 202-05 (GRS 23, item 1)</i> <i>Previously, NOAA Schedule Item 200-06.</i>	TEMPORARY. Follow disposition instructions for 200-01.
202-06	Credit/Bank Card	Copies of bank statements of credit card		

	Transactions.	<p>transactions receipts, reports and related documentation.</p> <p>NOTE: Always consult both Purchase and Travel Card Policy Materials to confirm current NOAA retention policy.</p>		
		Official Record Held in the Office of Record:	DAA-GRS-2013-0003-0001 (GRS 1.1, item 010)	TEMPORARY. Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.
		All Other Copies:	DAA-GRS-2013-0003-0002 (GRS 1.1, item 011)	TEMPORARY. Destroy when business use ceases.
202-07	General Correspondence Files:	<p>Correspondence files of operating procurement units concerning internal operation and administration matters not covered elsewhere in this schedule.</p> <p>Records include:</p> <ul style="list-style-type: none"> • correspondence • subject files • feeder reports • workload management assignment 	<p>DAA-GRS-2016-0013-0001 (GRS 1.1, item 001)</p> <p><i>Supersedes</i> (GRS 3, item 2) (GRS 6, item 5a) (GRS 6, item 5b) (GRS 7, item 1) (GRS 8, item 1) (GRS 9, item 4a)</p>	TEMPORARY. Destroy when 3 years old, but longer retention is authorized if needed for business use.

		records		
		Official Record Held in the Office of Record:	DAA-GRS-2013-0003-0001 (GRS 1.1, item 010) <i>Previously, NOAA Schedule Item 200-09.</i>	TEMPORARY. Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.
		All Other Copies:	DAA-GRS-2013-0003-0002 (GRS 1.1, item 011)	TEMPORARY. Destroy when business use ceases.
202-08	Federal Financial System Data Input Records.	Records relating to office expenditures such as acquisitions, training, travel or other expenses which have been processed into the Federal Financial System.	DAA-GRS- 2016-0016-0001 (GRS 5.1, item 010) <i>Supersedes NOAA Schedule Item 202-07 (GRS 23, item 1)</i> <i>Previously, NOAA Schedule Item 200 13.</i>	TEMPORARY. Follow the disposition instructions for 200-01.
202-09	Fund Use and Availability Records.	Reports and other documents pertaining to the accounting of funds spent and the status of apportioned accounts; also related briefings and meetings.	<i>Previously, NOAA Schedule Item 200 18.</i>	
		a. Recordkeeping paper copy of End of fiscal year report:	GRS 5, item 3a	TEMPORARY. Cut off at end of fiscal year. Destroy after 5 years.
		b. All Other Copies:	GRS 5, item 3b	TEMPORARY. Cut off

				at end of fiscal year and destroy after 3 years.
202-10	Routine Procurement/Contract Records (Administrative copies only, see Chapter 700 for program records).	Non-contract related requisitions, purchase order, lease, bond and surety records, including correspondence and related papers pertaining to award, administration, receipt, inspection, and payment and Tax Exemption Record. Includes copies of records described above used by component elements of a procurement office for administrative purposes. Original records are maintained in Procurement. Note 1: <i>These are copies used for administrative or reference purposes.</i> Note 2: <i>If you have questions or concerns please ask your procurement or contract contact for policies on records retention.</i>	DAA-2013-0003-0002 (GRS 1.1, item 011) <i>Previously, NOAA Schedule Item 200 26.</i> [Administrative copy only, for original program records, see Chapter 700]	TEMPORARY. Destroy when business use ceases.

Series #	Records Series Title	Records Description	Disposition Authority	Disposition Instruction
203	Human Resources Records (Administrative records only, see Chapter 300 for mission records)			
203-01	Time and Attendance Records.	<p>Sign-in/sign-out records, time cards, leave applications and approvals of all types (annual, sick, family medical, military service, jury duty, leave donations, etc.); overtime, compensatory, and credit time requests and approvals; premium pay authorizations; and other records documenting employees' presence at or absence from work.</p> <p>Legal citation: 29 U.S.C. 516.5a</p> <p><i>Note: Every office involved in documenting employees' time worked is responsible for retaining the records it receives and creates for 3 years.</i></p> <p><i>Timekeepers in individual offices need to be able to document that the time and attendance information they sent to the payroll system provider was accurate. Only</i></p>	<p>DAA-GRS- 2016-0015- 0003 (GRS 2.4, item 030)</p> <p><i>Supersedes NOAA Schedule Item 203 01 (GRS 2, item 8)</i></p> <p><i>Previously, NOAA Schedule Item 205 31.</i></p>	<p>TEMPORARY. Destroy after GAO audit or when 3 years old, whichever is sooner.</p>

		<i>total hours of time worked and leave taken is forwarded to the payroll system provider. Backup documentation justifying those totals is usually retained by the timekeeper.</i>		
203-02	Time and Attendance Source Records	All time and attendance records upon which leave input data is based.	DAA-GRS- 2016-0015- 0003 (GRS 2.4, item 030) <i>Supersedes NOAA Schedule Item 203 01 (GRS 2, item 7)</i> <i>Previously, NOAA Schedule Item 200 32.</i>	TEMPORARY. Follow disposition instructions for 203-01 above.
203-03	Supervisor's Personnel Files.	Records on positions, authorizations, pending actions, position descriptions, training records, individual development plans, telework agreements, award recommendations, and records on individual employees not duplicated in or not appropriate for the OPF. These records are sometimes called supervisors' working files, unofficial personnel files (UPFs), and employee work folders or "drop" files. Exclusion 1: Records that become part of a grievance file, an appeal or discrimination complaint file, a performance-based reduction-in-grade or removal action, or an adverse action. These records are covered under GRS 2.3, Employee Relations Records.	DAA-GRS-2017-0007-0012 (GRS 2.2, item 080) <i>Supersedes NOAA Schedule Item 203 03 (GRS 1, item 18)</i> <i>Previously, NOAA Schedule Item 200 36.</i>	TEMPORARY. Review annually and destroy superseded documents. Destroy remaining documents 1 year after employee separation or transfer.

		<p>Exclusion 2: Employee medical documents, unless part of employee's initial request for reasonable accommodation. Following approval, the agency's reasonable accommodation decision replaces medical documentation and becomes the record. Reasonable accommodation employee case files are covered under GRS 2.3, Employee Relations Records.</p>		
203-04	Employee Training Records.	<p>This schedule covers records about designing, developing, and implementing employee training within Federal agencies that is not mission-related. Typically, such training is routine or mandatory and covers general knowledge and actions all agencies expect of employees, such as training on information security, anti-harassment, ethics, EEO compliance, drug-free workplace, records management, and travel card use. In other words, training on administrative activities.</p> <p>This schedule does not include specialized training for firearms, health and safety, national defense, political appointees, or mission-specific training, which may document an agency's program objectives or illustrate program operations. This</p>		

		<p>schedule includes documentation of employee training provided from any source (internally or externally via private vendors or other agencies) and applies to all groups of Federal workers, civilian, military, and contractors.</p>		
		<p>a. Non-mission Employee Training Program Records.</p> <p>Exclusion: This item does not cover ethics-related training. Ethics training is scheduled by item 020. Records about planning, assessing, managing, and evaluating an agency's training program:</p> <ul style="list-style-type: none"> • plans, reports and program evaluations • organizational and occupational needs assessments • employee skills assessments • employee training statistics • notices about training opportunities, schedules, or courses 	<p>DAA-GRS-2016-0014-0001 (GRS 2.6, item 010)</p> <p><i>Supersedes NOAA Schedule Item 200-37 (GRS 1, item 29a1)</i></p> <p><i>Supersedes NOAA Schedule Item:</i></p> <p><i>304-02 (GRS 1, item 29b) Training by Outside Opportunities;</i></p> <p><i>(GRS 1, item 29a1) General in-house training, excluding curriculum;</i></p> <p><i>(GRS 1, item 29a2) Background Training Records;</i></p> <p><i>(GRS 21, item 3) Filmstrips and Slides</i> of Programs that do not Reflect the Mission of the</p>	<p>TEMPORARY. Destroy when 3 years old, or 3 years after superseded or obsolete, whichever is appropriate, but longer retention is authorized if required for business use.</p>

			<p>Agency;</p> <p><i>(GRS 21, item 9) Motion Picture</i> - Films Acquired from Outside Sources for Personnel and Management Training;</p> <p><i>(GRS 21, item 14) Video Recordings of</i> Programs Acquired from Outside Sources for Personnel and Management Training;</p> <p><i>(GRS 21, item 17) Video Recordings of</i> Training Programs that do not Reflect the Mission of the Agency.</p>	
		<ul style="list-style-type: none"> • mandatory training tracking and reporting files • logistics and coordination documents • Authorization, Agreement and Certification of Training (SF-182) and similar records • registration forms, employee attendance records • syllabi, presentations, instructor guides, handbooks, and lesson plans 		

		<ul style="list-style-type: none"> • reference and working files on course content • other course materials, such as presentations and videos • student, class, or instructor evaluations <p>Note: Financial records related to purchase of training or travel for training are scheduled under GRS 1.1, item 010.</p>		
		<p>b. Ethics training records.</p> <p>Records include but are not limited to:</p> <ul style="list-style-type: none"> • administration of new employee ethics orientations, annual, and other types of ethics training • agency's annual written plans • notices about training requirements and course offerings • rosters of employees required to attend and verification of training completed • instructor guides, handbooks, handouts and other materials 	<p>DAA-GRS-2016- 0014-0002 (GRS 2.6, item 020)</p> <p><i>Supersedes NOAA Schedule Item:</i></p> <p><i>(GRS 28, item 8a)</i> Records relating to the administration of new employee ethics orientations, annual, and other types of ethics training and education.</p> <p><i>(GRS 28, item 8b)</i> Record copy of materials used in providing new employee ethics orientations, annual, and other types of ethics training.</p>	<p>TEMPORARY. Destroy when 6 years old or when superseded, whichever is later, but longer retention is authorized if required for business use.</p>
		<p>c. Individual employee training records.</p>	<p>DAA-GRS-2016- 0014-0003 (GRS 2.6, item 030)</p>	<p>TEMPORARY. Destroy when</p>

		<p>Records documenting training required by all or most Federal agencies, such as information system security and anti-harassment training, and training to develop job skills. Records may include:</p> <ul style="list-style-type: none"> • completion certificates or verification documents for mandatory training required of all Federal employees or specific groups of employees (e.g., supervisors, contractors) • Individual Development Plans (IDPs) • mentoring or coaching agreements <p>Exclusion: Academic transcripts, professional licenses, civil service exams, or documentation of mission-related training are not covered by this item.</p>	<p><i>Supersedes NOAA Schedule Item:</i></p> <p>304-02 (GRS 1, item 29b)</p>	<p>superseded, 3 years old, or 1 year after separation, whichever comes first, but longer retention is authorized if required for business use.</p>
		<p>d. Senior Executive Service Candidate Development Program (SESCDP).</p> <p>SESCDP is an OPM-approved training program designed to develop employees with strong executive potential to qualify them for and authorize their initial career appointment in the Senior Executive Service.</p>		
		<p>(1) Program records.</p>	<p>DAA-GRS-2016- 0014-0004 (GRS 2.6, item 040)</p>	<p>TEMPORARY. Destroy when</p>

		Records documenting program scope, policies, planning, budget, and curriculum planning.	New Item	Destroy when no longer needed for business use.
		(2) Case records on SESCDP participants. Records documenting training, developmental assignments, mentor agreements and evaluations, and SES Development Plans.	DAA-GRS-2016- 0014-0005 (GRS 2.6, item 041) New Item	TEMPORARY. Destroy upon certification by OPM’s Qualifications Review Board (QRB) or 1 year after separation from SESCDP, but longer retention is authorized if required for business use.
203-05	Telework/ Alternate Worksite Records.	Records generated by the designated Telework Managing Officer (TMO), agency telework coordinators and other related staff.		TEMPORARY. Follow disposition authority 2.3, item 080 and 081 under Chapter 300, Personnel.
203-06	Equal Employment Opportunity (EEO) General Records (See Chapter 203-11 for program records)	General correspondence and copies of regulations with related records pertaining to the Civil Rights Act of 1964, the EEO Act of 1972, and any pertinent later legislation, and agency EEO Committee meeting records, including minutes and reports. NOTE: EEO records relating to the oversight of the EEO Program, please refer	DAA-GRS- 2015-0007- 0006 (GRS 2.3, item 030) <i>Supersedes NOAA Schedule Item 203 06 (GRS 1, item 25)</i> <i>Previously, NOAA Schedule Item 200 11. See Chapter 302 for EEO program records.</i>	TEMPORARY. Destroy when 3 years old, but longer retention is authorized if required for business use.

		to NOAA Records Series 312.		
--	--	-----------------------------	--	--

Series #	Records Series Title	Records Description	Disposition Authority	Disposition Instruction
204	Records Management Records.	This schedule covers records created and maintained by Federal agencies that relate to the management of records and information. It includes records related to tracking and controlling agency records and documents, records management, forms management, and managing vital or essential records		
204-01	Tracking and Control Records.	<p>Records used to provide access to and control of records authorized for destruction by the GRS or a NARA approved records schedule. Includes:</p> <ul style="list-style-type: none"> • indexes • lists • registers • inventories • logs <p>Exclusion 1: This schedule excludes records containing abstracts of records content or other information that can be used as an information source apart from the related records.</p>	<p>DAA-GRS-2013-0002-0016 (GRS 4.1, item 010)</p> <p><i>Supersedes NOAA Schedule Items:</i></p> <p>200-33 200-14</p>	<p>TEMPORARY. Destroy when no longer needed.</p>

		<p>Exclusion 2: This authority does not apply to tracking and control records related to records scheduled as permanent. The value of these records varies, so tracking and control records related to permanent records must be scheduled.</p>		
204-02	Records Management Program Records.	<p>Records related to the policies, procedures, and management of agency business records from creation to eventual disposition. Includes records created and maintained while planning, managing, evaluating, administering, and performing the function of agency records management. Activities include:</p> <ul style="list-style-type: none"> • providing oversight of entire records management program • transferring, destroying, and retrieving records • inventorying records and conducting records surveys • scheduling records • providing other records management services to customer units (such as records storage/reference assistance, and technical assistance with files plans and other records management questions) 	<p>DAA-GRS- 2013-0002- 0007 (GRS 4.1, item 020)</p> <p><i>Supersedes NOAA Schedule Items:</i></p> <p>200-24 200-46</p>	<p>TEMPORARY. Destroy no sooner than 6 years after the project, activity, or transaction is completed or superseded, but longer retention is authorized if needed for business use.</p>

		<ul style="list-style-type: none"> • conducting records "clean out" days • conducting special projects Records include: • agency records management program surveys or evaluations reports of surveys or evaluations • reports of corrective action taken in response to agency program surveys or evaluations • disposal authorizations, schedules, and reports • records schedules, legacy records schedules (SF 115, Request for Records Disposition Authority) • SF 135, Records Transmittal and Receipt • OF 11, Reference Request • Transfer Request (TR); Legal Transfer Instrument (LTI); SF 258, Agreement to Transfer Records to the National Archives of the United States. <p>Exclusion: This schedule item covers</p>		
--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

		copies of the records schedule, transfer request, legal transfer instrument, and similar forms maintained by agencies—not the copies maintained by NARA.		
204-03	Vital or Essential Records Program Records.	Records involved in planning, operating, and managing the agency’s vital or essential records program. Includes: <ul style="list-style-type: none"> • vital records inventories • vital records cycling plans • results of tests, surveys, or evaluations • reports of corrective action taken in response to agency vital records tests. 	DAA-GRS- 2013-0002-0008 (GRS 4.1, item 030) <i>Supersedes NOAA Schedule Items:</i> <i>200-46</i>	TEMPORARY. Destroy 3 years after project, activity, or transaction is completed or superseded, but longer retention is authorized if needed for business use.
204-04	Copies of Vital Records.	Copies of agency records deemed essential to restore agency functions in case of emergency.	DAA-GRS- 2013-0002- 0015 (GRS 4.1, item 031)	TEMPORARY. Destroy when superseded by the next cycle.
204-05	Forms Management Records.	Records involved with ensuring use of standard Federal and agency forms to support effective recordkeeping and ensuring that Federal standard forms are available and used as appropriate to support Federal record-keeping requirements. Includes: <ul style="list-style-type: none"> • registers or databases used to record and control the numbers and other 	DAA-GRS- 2013-0002-0009 (GRS 4.1, item 040) <i>Previously, NOAA Schedule Item 200 45.</i>	TEMPORARY. Destroy 3 years after form is discontinued, superseded, or cancelled, but longer retention is authorized if needed for business use.

		<p>identifying data assigned to each form</p> <ul style="list-style-type: none"> • official case files consisting of the record copy of each agency-originated form with related instructions and documentation showing inception, scope, and purpose of the form • background materials and specifications 		
204-06	<p>Email Managed Under a Capstone Approach.</p> <p>(Submitted by DOC to NARA 12/16 for DOC agencies, still pending NARA approval)</p>	<p>Email can be managed at an account level, at a mailbox level, in personal folder files, or other ways. This GRS applies to all email, regardless of how the email messages are managed or what email technology is used. Email, in the context of this GRS, also includes any associated attachments. This GRS may apply to records affiliated with other commonly available functions of email programs such as calendars/appointments, tasks, and chat.</p>	<p>DAA-GRS- 2014-0001- 0001 (GRS 6.1, item 010)</p>	<p>PERMANENT. Cut off in accordance with agency's business needs. Transfer to NARA 15-25 years after cutoff, or after declassification review (when applicable), whichever is later.</p>
		<p>Email of Capstone officials. Capstone Officials are senior officials designated by account level or by email addresses, whether the addresses are based on an individual's name, title, a group, or a specific program function. Capstone officials include all those listed on an approved NARA form 1005 (NA-1005), Verification for Implementing GRS 6.1, and must include, when applicable:</p>		

		<p>1. The head of the agency, such as Secretary, Commissioner, Administrator, Chairman or equivalent;</p> <p>2. Principal assistants to the head of the agency (second tier of management), such as Under Secretaries, Assistant Secretaries, Assistant Commissioners, and/or their equivalents; this includes officers of the Armed Forces serving in comparable position(s);</p> <p>3. Deputies of all positions in categories 1 and 2, and/or their equivalent(s);</p> <p>4. Staff assistants to those in categories 1 and 2, such as special assistants, confidential assistants, military assistants, and/or aides;</p> <p>5. Principal management positions, such as Chief Operating Officer, Chief Information Officer, Chief Knowledge Officer, Chief Technology Officer, and Chief Financial Officer, and/or their equivalent(s);</p> <p>6. Directors of significant program offices, and/or their equivalent(s);</p>		
--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

		<p>7. Principal regional officials, such as Regional Administrators, and/or their equivalent(s);</p> <p>8. Roles or positions that routinely provide advice and oversight to the agency, including those positions in categories 1 through 3 and 5 through 7, including: General Counsels, Chiefs of Staff, Inspectors General, etc.;</p> <p>9. Roles and positions not represented above and filled by Presidential Appointment with Senate Confirmation (PAS positions); and</p> <p>10. Additional roles and positions that predominately create permanent records related to mission critical functions or policy decisions and/or are of historical significance.</p> <p>This includes those officials in an acting capacity for any of the above positions longer than 60 days. Agencies may also include individual emails from otherwise temporary accounts appropriate for permanent disposition in this category.</p> <p>This item must include all existing legacy email accounts that correlate to the roles</p>		
--	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

		<p>and positions described above.</p> <p>If a Capstone official has more than one agency-administered email account, this item applies to all accounts. If a Capstone official has an email account managed by other staff (such as personal assistants, confidential assistants, military assistants, or administrative assistants), this item applies to those accounts. This item applies to all email regardless of the address names used by the Capstone official for agency business, such as nicknames or office title names. Email from personal or non-official email accounts in which official agency business is conducted is also included. A complete copy of these records must be forwarded to an official electronic messaging account of the officer or employee not later than 20 days after the original creation or transmission of the record.</p> <p>Please consult NA-1005, for more information on which positions are included within each category.</p> <p>Not media neutral; applies to records managed in an electronic format only.</p> <p>Note 1: <i>Cabinet level agencies</i></p>		
--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

		<p><i>implementing a Capstone approach that includes their components/operatives must apply the above definition to each component individually. In these cases, each component/operative is considered a separate agency in terms of the above definition of Capstone Officials. A component/operative of a cabinet level agency can implement a Capstone approach independent of their department but must also conform to the entirety of this definition.</i></p> <p><i>-Capstone Officials have complete oversight and responsibility spanning a larger region (e.g., multiple states or specific geographic area) in carrying out mission-critical activities. For example, an agency may have 10 regions, each with a Regional Administrator that is responsible for mission-critical activities within that region's jurisdictions; these 10 Regional Administrators would fall into this category. Heads (regardless of title) of offices outside of headquarters, but not under a regionalized structure, are not included in this category. For example, it does not pertain to the heads of individual offices in the field, such as, but not limited to, customer service centers, processing centers, or administrative offices that</i></p>		
--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

		<p>conduct routine activities (e.g., passport offices, or Social Security claims processing offices, IRS service centers, commissaries).</p> <p>Note 2: Smaller agencies, micro-agencies or Commissions implementing a Capstone approach may find that some of their Capstone positions fall into several of the categories above and/or that they do not have applicable roles or positions for all categories.</p>		
204-07	<p>Email of Non-Capstone Officials.</p> <p>(Submitted by DOC to NARA 12/16 for DOC agencies, still pending NARA approval)</p>	<p>Email of all other officials, staff, and contractors not included in item 010. Not media neutral; applies to records managed in an electronic format only.</p> <p>Note: Agencies only using item 011 and/or item 012 of this GRS may not dispose of any email of officials in item 010, Email of Capstone Officials, of this GRS without authority from NARA in the form of another GRS or agency specific schedule. Submission and approval of NA-1005 is still required in these instances to document those being exempted from Capstone.</p>		
		<p>All others except those in item 012.</p> <p>Includes positions and email not covered by items 010 or 012 of this schedule. This item applies to the majority of email accounts/users within an agency adopting</p>	<p>DAA-GRS- 2014-0001- 0002 (GRS 6.1, item 011)</p>	<p>TEMPORARY. Delete when 7 years old, but longer retention is authorized if required for business use.</p>

		a Capstone approach.		
		<p>Support and/or administrative positions.</p> <p>Includes non-supervisory positions carrying out routine and/or administrative duties. These duties comprise general office or program support activities and frequently facilitate the work of Federal agencies and their programs. This includes, but is not limited to, roles and positions that: process routine transactions; provide customer service; involve mechanical crafts, or unskilled, semi-skilled, or skilled manual labor; respond to general requests for information; involve routine clerical work; and/or primarily receive nonrecord and/or duplicative email.</p>	<p>DAA-GRS- 2014-0001- 0003 (GRS 6.1, item 012)</p>	<p>TEMPORARY. Delete when 3 years old, but longer retention is authorized if required for business use.</p>

Series #	Records Series Title	Records Description	Disposition Authority	Disposition Instruction
205	Information Access and Protection Records.	This schedule covers records created in the course of agencies (1) responding to requests for access to Government information and (2) protecting information that is classified or controlled unclassified, or contains personal data that is required by law to be protected.		
205-01	FOIA, Privacy Act, and Classified Documents Administrative Records.	<p>Records on managing information access and protection activities. Records include:</p> <ul style="list-style-type: none"> • correspondence related to routine implementation of the FOIA and Privacy Act and administration of security classification, control, and accounting for classified documents • associated subject files • feeder and statistical reports <p>Exclusion: This item does not cover records documenting policies and procedures accumulated in offices having</p>	<p>DAA GRS 2016 0013 0003 (GRS 4.2, item 001)</p> <p><i>Supersedes NOAA 200 53, and records covered by GRS 14, item 5; GRS 14, item 26; and GRS 18, item 1.</i></p>	<p>TEMPORARY. Destroy when 3 years old, but longer retention is authorized if needed for business use.</p>

		agency-wide responsibilities for FOIA, Privacy Act, and classified documents. These records must be scheduled by the agency on an agency-specific schedule.		
205-02	General Information Request Files.	Requests for information, publications, photographs, and other information involving no administrative action, policy decision, or special compilations or research. Also includes acknowledgements, replies, and referrals of inquiries to other offices for response.	DAA GRS 2013 0007 0001 (GRS 4.2, item 010)	
205-03	Access and Disclosure Request Files.	<p>Case files created in response to requests for information under the Freedom of Information Act (FOIA), Mandatory Declassification Review (MDR) process, Privacy Act (PA), Classification Challenge, and similar access programs, and completed by:</p> <ul style="list-style-type: none"> • granting the request in full • granting the request in part • denying the request for any reason including: <ul style="list-style-type: none"> o inability to fulfill request because records do not exist 	DAA GRS 2016 0002 0001 (GRS 4.2, item 020) <i>Supersedes NOAA Schedule Items:</i> 200-15 200-17 <i>Previously scheduled under N1 370 08 05</i>	TEMPORARY. Destroy 6 years after final agency action or 3 years after final adjudication by the courts, whichever is later, but longer retention is authorized if required for business use.

		<ul style="list-style-type: none"> o inability to fulfill request because request inadequately describes records o inability to fulfill request because search or reproduction fees are not paid • final adjudication on appeal to any of the above original settlements • final agency action in response to court remand on appeal Includes: • requests (either first-party or third-party) • replies • copies of requested records • administrative appeals • related supporting documents (such as sanitizing instructions) Note 1: Record copies of requested records remain covered by their original disposal authority, but if disposable sooner than their associated access/disclosure case file, may be retained under this item for disposition with that case file. Note 2: Agencies may wish to retain 		
--	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

		redacted copies of requested records for business use after the rest of the associated request case file is destroyed.		
205-04	Information Access and Protection Operational Records.			
		<p>Information access and protection tracking and control records. Includes:</p> <ul style="list-style-type: none"> • records documenting receipt, internal routing, dispatch, and destruction of unclassified records • tracking databases and other records used to manage overall program • requests and authorizations for individuals to have access to classified files 	DAA-GRS-2016-0002-0002 (GRS 4.2, item 030)	TEMPORARY. Destroy 2 years after last form entry, reply, or submission; or when associated documents are declassified or destroyed; or when authorization expires; whichever is appropriate. Longer retention is authorized if required for business use.
		<p>Access control records. Includes:</p> <ul style="list-style-type: none"> • safe and padlock combinations • names or other personal identifiers of individuals who know combinations • comparable data used to control access into classified document containers 	DAA-GRS-2013-0007-0020 (GRS 4.2, item 031)	TEMPORARY. Destroy when superseded or obsolete, but longer retention is authorized if required for business use.
		Records relating to classified or controlled unclassified document	DAA-GRS-2016-0002-0003 (GRS 4.2, item 032)	TEMPORARY. Destroy 90 days after

		<p>containers. Includes forms placed on safes, cabinets, or vaults that record opening, closing, and routine checking of container security, such as SF-701 and SF-702.</p> <p>Note: <i>Forms involved in investigations are not covered by this item. They are instead retained according to the schedule item for records of the investigation.</i></p>		<p>last entry on form, but longer retention is authorized if required for business use.</p>
205-05	<p>Accounting for and Control of Access to Classified and <u>Controlled Unclassified Records, and Records Requested under FOIA, PA, and MDR.</u></p>	<p>Records documenting identity, internal routing, and final disposition of classified documents. Also, records documenting control points and accountability for information relating to access requests. Includes:</p> <ul style="list-style-type: none"> • forms, registers, ledgers, logs, and tracking systems documenting requester identity and contact information, request date, and nature or purpose of request • inventories of controlled records • forms accompanying documents to ensure continuing control, showing names of people handling the documents, inter-office routing, and comparable data • agent and researcher files 	<p>DAA-GRS- 2016-0002- 0004 (GRS 4.2, item 040)</p> <p><i>Supersedes NOAA Schedule Items:</i></p> <p>200-16 200-51</p>	<p>TEMPORARY. Destroy or delete 5 years after date of last entry, final adjudication by courts, or final action by agency (such as downgrading, transfer or destruction of related classified documents, or release of information from controlled unclassified status), as may apply, whichever is later; but longer retention is authorized if required for business</p>

				use.
205-06	Privacy Act Accounting of Disclosure Files.	Files maintained under the provisions of 5 U.S.C. §552a(c) for an accurate accounting of the date, nature, and purpose of each disclosure of a record to any person or to another agency. Includes: <ul style="list-style-type: none"> • forms with the subject individual's name • records of the requester's name and address • explanations of the purpose for the request • date of disclosure • proof of subject individual's consent 	NC1 64 77 1, item 27 (GRS 4.2, item 50) <i>Supersedes</i> GRS 14, item 23, and <i>NOAA Schedule Items: 200-50</i>	TEMPORARY. Dispose of in accordance with the approved disposition instructions for the related subject individual's records, or 5 years after the disclosure for which the accountability was made, whichever is later.
205-07	Erroneous Release Records.	Files relating to the inadvertent release of privileged information to unauthorized parties, containing information the disclosure of which would constitute an unwarranted invasion of personal privacy. Includes: <ul style="list-style-type: none"> • requests for information • copies of replies • all related supporting documents May include: • official copy of records requested or 		

		copies		
		Records filed with the record-keeping copy of the erroneously released records.	DAA-GRS- 2015-0002-0001 (GRS 4.2, item 060) <i>Supersedes NOAA Schedule Item 200-54a (GRS 14, item 36a)</i>	TEMPORARY. Follow the disposition instructions approved for the released record copy or destroy 6 years after the erroneous release, whichever is later.
		Records filed separately from the record-keeping copy of the released records.	DAA-GRS- 2015-0002- 0002 (GRS 4.2, item 061) <i>Supersedes NOAA Schedule Item 200-54b (GRS 14, item 36b)</i>	TEMPORARY. Destroy 6 years after the erroneous release, but longer retention is authorized if required for business use.
205-08	Agency Reports to the Congress, Department of Justice, or other Entities Regarding FOIA, MDR, PA, and Similar Access and Disclosure Programs.	Note: <i>This item does not apply to summary reports incorporating government-wide statistics. These must be scheduled separately by the summarizing agent.</i>	DAA-GRS- 2013-0007-0006 (GRS 4.2, item 070) <i>Supersedes NOAA Schedule Item 200-52</i>	TEMPORARY. Destroy 2 years after date of report, but longer retention is authorized if required for business use.
205-09	Legal and Regulatory Compliance Reporting Records.	Reports prepared in compliance with Federal laws and regulations, such as the E-Government Act (Public Law 107-347), Title III (Federal Information Security Management Act), and Title V		

		(Confidential Information Protection and Statistical Efficiency Act), as codified in 44 U.S.C. §101.		
		Annual reports by agency CIO, Inspector General, or Senior Agency Official for Privacy. Legal citation: OMB M-07-16.	DAA GRS 2013 0007 0022 (GRS 4.2, item 080)	TEMPORARY. Destroy 5 years after submission of report, but longer retention is authorized if required for business use.
		All other agency reports and internal reports by individual system owners to the Senior Agency Official for Privacy (SAOP).	DAA-GRS- 2013-0007- 0023 (GRS 4.2, item 081)	TEMPORARY. Destroy 2 years after submission of report, but longer retention is authorized if required for business use.
205-10	Privacy Act Amendment Request Files.	Files relating to an individual's request to amend a record pertaining to that individual under 5 U.S.C. §552a(d)(2), to the individual's request for review of an agency's refusal to amend a record under 5 U.S.C. §552a(d)(3), and to any civil action or appeal brought by the individual against the refusing agency under 5 U.S.C. §552a(g). Includes: • requests to amend and to review refusal to amend	DAA-GRS- 2013-0007- 0007 (GRS 4.2, item 090) <i>Supersedes NOAA Schedule Item 200-49</i>	TEMPORARY. Destroy with the records for which amendment was requested or 4 years after close of case (final determination by agency or final adjudication, whichever applies), whichever is later. Longer retention is authorized if

		<ul style="list-style-type: none"> • copies of agency’s replies • statement of disagreement • agency justification for refusal to amend a record • appeals • related materials 		required for business use.
205-11	Automatic and Systematic Declassification Review Program Records.	Files related to the review of permanent records in anticipation of automatic declassification at 25, 50, or 75 years per Executive Order 13526, and the periodic review of records exempted from automatic declassification. Files include program records documenting declassification decisions.	DAA-GRS- 2013-0007-0008 (GRS 4.2, item 100)	TEMPORARY. Destroy or delete 30 years after completion of review, but longer retention is authorized if required for business use.
205-12	Fundamental Classification Guidance Review Files.	Reports, significant correspondence, drafts, received comments, and related materials responding to “fundamental classification guidance review” as required by Executive Order 13526 Section 1.9. Note: This item does not cover reports and correspondence received at the Information Security Oversight Office (ISOO).	DAA-GRS- 2013-0007-0011 (GRS 4.2, item 110)	TEMPORARY. Destroy 5 years after report is submitted to ISOO, but longer retention is authorized if required for business use.
205-13	Classified Information Nondisclosure	Copies of nondisclosure agreements, such as SF 312, Classified Information		

	Agreements.	Nondisclosure Agreement, signed by civilian and military personnel with access to information that is classified under standards put forth by executive orders governing security classification.		
		Records maintained in the individual's official personnel folder.	GRS 4.2, item 120	Apply the disposition for the official personnel folder.
		Records maintained separately from the individual's official personnel folder.	DAA-GRS- 2015-0002-0003 (GRS 4.2, item 121)	TEMPORARY. Destroy when 50 years old.
205-14	Personally Identifiable Information Extracts.	System-generated or hardcopy print-outs generated for business purposes that contain Personally Identifiable Information. Legal citation: OMB M-07-16 (May 22, 2007), Attachment 1, Section C, bullet "Log and Verify."	DAA-GRS- 2013-0007-0012 (GRS 4.2, item 130)	TEMPORARY. Destroy when 90 days old or no longer needed pursuant to supervisory authorization, whichever is appropriate.
205-15	Personally Identifiable Information Extract Logs.	Logs that track the use of PII extracts by authorized users, containing some or all of: date and time of extract, name and component of information system from which data is extracted, user extracting data, data elements involved, business purpose for which the data will be used, length of time extracted information will be used. Also includes (if appropriate): justification and supervisory authorization for retaining extract longer than 90 days,	DAA-GRS- 2013-0007-0013 (GRS 4.2, item 140)	TEMPORARY. Destroy when business use ceases.

		and anticipated disposition date.		
205-16	Privacy Act System of Records Notices (SORNs).	Agency copy of notices about the existence and character of systems of records, documenting publication in the Federal Register when the agency establishes or revises the system, per the Privacy Act of 1974 [5 U.S.C. 552a(e)(4) and 5 U.S.C. 552a(e)(11)], as amended. Also significant material documenting SORN formulation, other than Privacy Impact Assessment records (see item 161).	DAA-GRS- 2016-0003-0002 (GRS 4.2, item 150)	TEMPORARY. Destroy 2 years after supersession by a revised SORN or after system ceases operation, but longer retention is authorized if required for business use.
205-17	Records Analyzing Personally Identifiable Information (PII).	Records documenting whether certain privacy and data security laws, regulations, and agency policies are required; how the agency collects, uses, shares, and maintains PII; and incorporation of privacy protections into records systems as required by the EGovernment Act of 2002 (Public Law 107-347, section 208), the Privacy Act of 1974 (5 U.S.C. 552a), and other applicable privacy laws, regulations, and agency policies. Includes significant background material documenting formulation of final products.		
		Records of Privacy Threshold Analyses (PTAs) and Initial Privacy Assessments (IPAs).	DAA-GRS- 2016-0003-0003 (GRS 4.2, item 160)	TEMPORARY. Destroy 3 years after associated PIA is published or

		Records of research on whether an agency should conduct a Privacy Impact Assessment (PIA).		determination that PIA is unnecessary, but longer retention is authorized if required for business use.
		Records of Privacy Impact Assessments (PIAs).	DAA-GRS- 2016-0003-0004 (GRS 4.2, item 161)	TEMPORARY. Destroy 3 years after a superseding PIA is published, after system ceases operation, or (if PIA concerns a website) after website is no longer available to the public, as appropriate. Longer retention is authorized if required for business use.
205-18	Computer Matching Program Notices and Agreements.	Agency copy of notices of intent to share data in systems of records with other Federal, state, or local government agencies via computer matching programs, and related records documenting publication of notice in the Federal Register per the Privacy Act of 1974 [5 U.S.C. 552a(e)(12)], as amended. Also agreements between agencies, commonly referred to as Computer	DAA-GRS- 2016-0003-0005 (GRS 4.2, item 170)	TEMPORARY. Destroy upon supersession by a revised notice or agreement, or 2 years after matching program ceases operation, but longer retention is authorized if

		Matching Agreements, prepared in accordance with Office of Management and Budget Final Guidance. Includes documentation of Data Integrity Board (DIB) review and approval of matching programs and agreements, and significant background material documenting formulation of notices and agreements.		required for business use.
205-19	Virtual Public Access Library Records.	<p>Records published by an agency on line to fulfill the requirement in 5 U.S.C. 552(a)(2)(A) through 5 U.S.C. 552(a)(2)(D) and 5 U.S.C. 552(g)(1) through 5 U.S.C. 552(g)(3) that agencies must make those records available for public inspection and copying. Includes:</p> <ul style="list-style-type: none"> • final concurring and dissenting opinions and orders agencies issue when adjudicating cases • statements of policy and interpretations the agency adopts but does not publish in the Federal Register • administrative staff manuals and instructions to staff that affect a member of the public • copies of records requested under the Freedom of Information Act (FOIA) which, because of the nature of their subject 	DAA-GRS- 2016-0008-0001 (GRS 4.2, item 180)	TEMPORARY. Destroy when no longer needed.

		<p>matter, the agency determines are, or are likely to become, the subject of subsequent requests for substantially the same records or which have been requested three or more times</p> <ul style="list-style-type: none">• indexes of agency major information systems• descriptions of agency major information and record locator systems• handbooks for obtaining various types and categories of agency public information <p>Exclusion: This item refers only to copies an agency publishes on line for public reference. The agency record copy of such material may be of permanent value and the agency must schedule it.</p> <p>Not media neutral. Applies to electronic records only.</p>		
--	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

Series #	Records Series Title	Records Description	Disposition Authority	Disposition Instruction
206	Administrative Help Desk Records.	Help desk services are provided by service centers to respond to Government and contract employees' technical and administrative questions. This schedule covers records on managing administrative, technical, and information technology (IT) help desks. It includes records on assistance provided both within the agency and through inter-agency service agreements on functions such as IT help, security, parking, payroll, timekeeping, human resources, etc.		
206-01	Technical and Administrative Help Desk Operational Records.	<ul style="list-style-type: none"> • records of incoming requests (and responses) made by phone, email, web portal, etc. • trouble tickets and tracking logs • quick guides and “Frequently Asked Questions” (FAQs) 	DAA-GRS-2017- 0001-0001 (GRS 5.8, item 010)	TEMPORARY. Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate.

		<ul style="list-style-type: none">• evaluations and feedback about help desk services• analysis and reports generated from customer management data• customer/client feedback and satisfaction surveys, including survey instruments, data, background materials, and reports <p>Exclusion: Public customer service records scheduled under GRS 6.5.</p>		
--	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

Series #	Records Series Title	Records Description	Disposition Authority	Disposition Instruction
207	Public Customer Service Records.	This schedule covers records an agency creates or receives while providing customer service to the public. Federal agencies that provide direct services to the public operate customer call centers or service centers to assist external customers. They may provide customer support through telephone discussions (toll free numbers), dialogue (via chat), and email.		
207-01	Public Customer Service Operations Records.	<p>Records from operating a customer call center or service center providing services to the public. Services may address a wide variety of topics such as understanding agency mission-specific functions or how to resolve technical difficulties with external-facing systems or programs. Includes:</p> <ul style="list-style-type: none"> • incoming requests and responses • trouble tickets and tracking logs • recordings of call center phone conversations with customers used for 	DAA-GRS- 2017-0002- 0001 (GRS 6.5, item 010)	TEMPORARY. Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate.

		<p>quality control and customer service training</p> <ul style="list-style-type: none"> • system data, including customer ticket numbers and visit tracking • evaluations and feedback about customer services • information about customer services, such as “Frequently Asked Questions” (FAQs) and user guides • reports generated from customer management data • complaints and commendation records; customer feedback and satisfaction surveys, including survey instruments, data, background materials, and reports. <p>Exclusion 1: Records of call or service centers the public uses to provide tips or allegations to oversight and enforcement agencies/offices. Agencies must schedule these records on an agency specific schedule.</p> <p>Exclusion 2: Reports that recommend changes or revisions to an agency’s customer service operation; agencies must schedule these records on an agency-</p>		
--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

		specific schedule.		
207-02	Customer/Client Records.	<p>Distribution lists used by an agency to deliver specific goods or services. Records include:</p> <ul style="list-style-type: none"> • contact information for customers or clients • subscription databases for distributing information such as publications and data sets produced by the agency • files and databases related to constituent and community outreach or relations • sign-up, request, and opt-out forms 	DAA-GRS-2017-0002-0002 (GRS 6.5, item 020)	TEMPORARY. Delete when superseded, obsolete, or when customer requests the agency to remove the records.



NOAA NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION

UNITED STATES DEPARTMENT OF COMMERCE



RECORDS DESTRUCTION REQUEST FORM

Person Completing Form/Office/Phone No.		Mark Graff/OCIO/FOIA Officer						
RECORD DATA								
Name of Record Series & Brief Description	Date Range		Date Eligible For Disposal	Disposition Instructions	Disposition Authority	Format		Volume
	Start	End				Paper	Elect	
Access and Disclosure Request files	10/1/06	9/30/11	10/1/17	Destroy 6 years after final agency action or 3 years after final adjudication by the courts, whichever is later	DAA GRS 2016 0002 0001	x		15 cuf
	Name	Signature		Date	Certification Statement			
Authorizing Official	Mark Graff				I certify that, to the best of my knowledge, these records are not subject to any current or pending litigation, audit, subpoena, or other legal demand, and they are being destroyed in accordance with the applicable, approved records control schedule.			
Records Liaison Officer	Sarah Brabson							
Destroyed By:					I certify that these records were destroyed by cross cut shredding, pulverizing, burning, or by any disposal method authorized by NARA. All records were destroyed on the same date.			
Witnessed By:								

1. Person Completing Form/Office/ Phone No.: Enter your name, office and telephone number.

INSTRUCTIONS

2. **Name of Record Series and Brief Description:** Enter name of records series name and brief description of the record.
3. **Date Range (Start/End):** Enter the beginning date and ending date of records eligible for disposal.
4. **Date Eligible for Disposal:** Enter date when records are eligible for disposal.
5. **Disposition Instructions:** Refer to [NOAA Records Schedules](#) to identify how long records should be maintained.
6. **Disposition Authority:** Specify records series item number which can be obtained from [NOAA Records Schedules](#) , example 1500-4.11, for Fisheries Vessel Permit files.
7. **Format (Paper/Electronic):** Enter (*v*) to specify the physical format of the records
8. **Volume:** Indicate volume in cubic feet or bytes (See examples below)
 - a. One standard records center carton holds 1 cubic foot
 - b. One letter-size file drawer holds 1.5 cubic feet of record
 - c. One legal-size file drawer holds 2 cubic feet of records
 - d. 1 GB, 100 MB, 100KB of records.
9. **Authorizing Official:** Enter the name, signature, and date signed by the official authorizing disposal, indicating they are authorized to approve disposal of records and certifying that these records are not subject to any current or pending litigation, audit, subpoena, or other legal demand, and they are being destroyed in accordance with the applicable, approved records control schedule.
10. **Records Liaison Coordinator:** Enter the name, signature, and date signed by the records liaison coordinator indicating they are authorized to approve disposal of records and certifying that these records are not subject to any current or pending litigation, audit, subpoena, or other legal demand, and they are being destroyed in accordance with the applicable, approved records control schedule.
11. **Destroyed by:** Enter the name, signature and date signed by the person performing the disposal of the records.
12. **Witnessed by:** Enter the name, signature and date signed by the person who witnessed the destruction of the records by an outside contractor. **A Witnessed destruction is mandatory for all Personal Identifiable Information (PII) or sensitive data such as social security numbers.**
13. **Recordkeeping:** **The Records Custodian is responsible for retaining the original of the completed records disposal form and submitting a copy to the Records Liaison Officer and the Agency Records Officer.**



How to Transfer Travel Records to the Federal Records Centers

6/17/11



STEP 1



IDENTIFY WHICH RECORDS TO TRANSFER

You should only transfer records if they:

- Are no longer needed for business, audit or legal purpose.
- Are consulted less than once per month.
- Are covered by a NARA-approved disposition from the General Records Schedules (GRS) or NOAA records control schedule
- Are not eligible for destruction less than 1 year from the date of transfer.



STEP 2



SORT RECORDS

- Remove all non-record material and extra copies from official files
- Identify and separate your records into series by the series title and number from your records schedule. Each item or subordinate item in your records schedule represents a series.
- Arrange the records by closing or cutoff year and the particular numerical, alphabetical, chronological or other identifiable sequence for that series.
- Transfer each series separately. Each transfer must contain at least one standard records center box of material. Loose papers or files will not be accepted.



STEP 3



ORDER RECORD CENTER BOXES AND PACK RECORDS

- All files must be packed in standard record center boxes with the dimensions of (14 ¾ x 12 x 9 ½).
- Estimate the number boxes needed for transfer
 - 1 standard records center box = 1 cubic feet
 - 1 letter-size file drawer = 1.5 cubic feet
 - 1 legal-size file drawer = 2.0 cubic feet
 - 1 lateral file drawer = 2.5 cubic feet
- Boxes can be purchased from GSA at 1-800-525-8027. The item number is NSN-8118-00-117-8249.



STEP 3 (Continued)



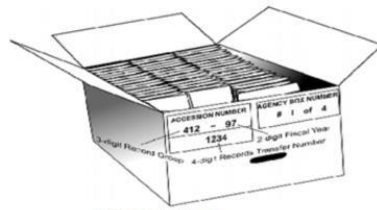
ORDER RECORD CENTER BOXES AND PACK RECORDS

- Place the records in proper order in records center boxes, following the same filing system used in the office. All records must be placed in folders and labeled with a unique specific and meaningful title.
- Place the folders in the boxes facing forward, toward the front of the box which will be marked for identification, opposite the stapled end.
- Place letter size records in the box with folders facing you as you're looking at the labeled end, opposite the stapled end.
- Place legal size records in the box so that the labels face the left side of the box as you're looking at the labeled end.
- Do not overfill the boxes. Allow about an inch leeway in each box to refile folders easily.
- Never place additional material on the bottom, side, or top of the records in the box.

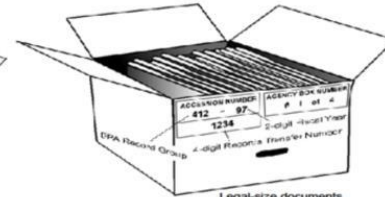


Packing Boxes

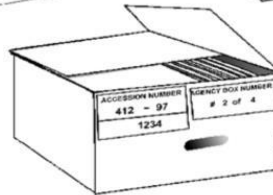
Records Retirement Box



Letter-Size Documents



Legal-size documents





STEP 4



CREATE A BOX INVENTORY LIST

- Prepare a box list of the contents of each box and place in the first box of the transfer.
- The list should be in letter-landscape format showing each folder's subject title, file number, and any other identifying information, as described in the records disposition instructions and according to the agency filing scheme.
- Identify the organizational component which created the records.
- Also include headings for each category of information provided, such as title or name, filing code, description, or date, along with page numbering at bottom-center, for easy reference.
- For subject files or case files containing materials spanning more than 1 year, note the date span for each folder.
- If there are two or more folders with the same case or subject title, note the number of folders on the box list.



Sample Box List

Agricultural Research Service
U.S. Department of Agriculture
Accession 310-98-0004
Files Closed November 1995

Box 1

AM 100.1 Compliance of ARS with the Animal Welfare Act
AM 100.2 Organization Changes
AM 100.3 Position Management
AM 105.2 Delegations of Authority
AM 110.6 ARS International Programs
AM 130.3 Human Metabolic Unit
AM 130.5 Research Assessment Committee:
Pesticide Impact Assessment
AM 150.1 Dissemination of Public Information by ARS
AM 150.6 Manuscript Clearance Procedures for Publishing in
Non-USDA Media
AM 150.7 Outside (Non-USDA) Publishing
AM 175.2 USDA Alphabetical and Organizational Lists

Box 2

AM 240.6 Pollution Abatement at ARS Facilities
AM 252.4 For Official Use Only Material
AM 310.5 Program Reports in ARS
AM 520.2 Approval of Proposed Projects
AM 945 Sponsored Research
AM 905 Releasing Plant Germ Plasm
AM 910 National Agricultural Pesticide Impact
Assessment Program

Page 1 of 1

Figure 3-2. Sample Box and Folder List for Permanent Records

19



STEP 5



COMPLETE RECORDS TRANSMITTAL AND RECEIPT FORM (SF-135) FORM

- **Block 1, TO:** The FRC Mailing address(4205 Suitland Road
Suitland MD 20746-8001(for offices in Washington Metro Area)
- **Block 2, Agency Authorization:** Agency Records Officer Signature
- **Block 3, Agency Contact:** Include the name, office, phone number, and email address of the person who knows the files and can answer any questions about them.
- **Block 4, Records Center Receipt:** Records Center completes this section
- **Block 5, From:** Name and address of the office submitting the records
- **Block 6(a), 6(b), 6(c), Accession Number:** Entered by FRC Staff
- **Block 6(d)** Include the number of cubic feet of records (1 standard records box = 1 cubic foot).
- **Block 6(f), Series Description.** Provide a complete and accurate description of the records from the records schedule including dates of the files.



STEP 5 (Continued)



COMPLETE RECORDS TRANSMITTAL AND RECEIPT FORM (SF-135) FORM

- **Block 6(g), Restrictions.** Most accessions are "N" or not restricted. Other files such as EEO-grievance files, that have sensitive information or confidential, should be identified with an "R" for restricted. List the names of persons who are authorized to have access to the restricted files on the SF-135 in the Series Description, block 6(f). The restriction codes are as follows:
 - C-Confidential security classification
 - N- No Restrictions
 - Q - Q-security classification
 - R - Restricted use - witnessed disposal not required (specify in column [f])
 - S - Secret security classification
 - T - Top Secret security classification
 - W - Restricted use - witnessed disposal required (specify in column [f])
- **Block 6(h), Disposal Authority.** Cite the GRS or agency schedule and specific item number authorizing disposal. Give the NARA disposition job and item number if it has not been incorporated into the agency records schedules.



STEP 5 (Continued)



COMPLETE RECORDS TRANSMITTAL AND RECEIPT FORM (SF-135) FORM

- **Block 6(i), Disposal Date:** Enter date records are eligible for disposal
- **Block 6(j), 6(k), 6(l), 6 (m):** Location is completed by the Records Center Staff



SAMPLE SF-135 FORM



RECORDS TRANSMITTAL AND RECEIPT		Complete and send original and one copy of this form to the appropriate Federal Records Center for approval prior to shipment of records. See specific instructions on reverse.		PAGE	OF					
1 TO		228.150		1	1 PAGES					
Federal Records Center Washington National Records Center (WNRC) 4205 Suitland Road, Suitland, MD 20746-8001		5 FROM (Enter the name and complete mailing address of the office retiring the records. The signed receipt of this form will be sent to this address.) Andre Sivels, Records Officer National Oceanic and Atmospheric Administration 1315 East West Highway SSMC3 - Room 10632 Silver Spring, MD 20910								
2 AGENCY TRANSFER AUTHORIZATION	TRANSFERRING AGENCY OFFICIAL (Signature and Title) Andre Sivels 301-713-3540 IG13 NOAA Records Officer Andre.Sivels@noaa.gov	DATE	1/8/09							
3 AGENCY CONTACT	TRANSFERRING AGENCY DESIGN OFFICIAL (Name, Office and Telephone No) Mary Cole - SSMC3 - RM 8008 301-713-xxxx, etc xxx	DATE								
4 RECORDS CENTER RECEIPT	RECORDS RECEIVED BY (Signature and Title)	DATE								
RECORDS DATA										
ACCESSION NUMBER			AGENCY BOX NUMBER	SERIES DESCRIPTION	DISPOSAL AUTHORITY	DISPOSAL DATE	LOCATION	COMPLETED BY RECORDS CENTER		
RG	FY	NR	VOLUME (cu ft)	(with inclusive dates of records)	(Schedule and item number)			INITIALS	DATE	TIME
(6)	(2)	(3)	(2)	(5)	(5)	(2)	(2)	(2)	(2)	(2)
370	11	001	B	1 - B	Travel Files (FY 06)	403-15	1/2016			
NIN 7542-00-534-4093			135-107			Standard Form 135 (Rev. 7-85) Facs Prescribed by NARA 36 CFR 1225.152				



STEP 6



ROUTING THE TRANSMITTAL AND RECEIPT FORM (SF-135)

- The custodian will send the SF-135 to the Records Liaison Officer for review.
- The Records Liaison Officer will forward the SF-135 to the Agency Records Officer for signature via email.
- After review, the Agency Records Officer will send the form back to the Records Liaison Officer, authorizing transfer.
- The Records Liaison Officer will send the SF-135 form to applicable FRC facility for approval.
- Within 3 to 5 days, the FRC will send the form back to the Records Liaison Officer authorizing transfer their facility. A transfer number (PT – 370-11-xxxx) will also be included in the accession number field of the SF-135.
- The Records Liaison Officer will send a copy of the form back to the custodian to arrange transfer.



STEP 7



PREPARING FOR RECORDS PICK-UP

- Records are ready transfer when the following has been completed
 - Inventory list is placed in the first box of the transfer
 - A copy of the approved SF-135 is placed in the last box of the shipment
 - Boxes are taped securely
 - Label boxes
 - Enter transfer Number (370-11-xxxx)
 - Boxes are sequentially numbered



STEP 8



SCHEDULING PICK-UP

- Transfers Inside the Washington Metro Area
 - Complete 41-1 form and fax to 301-372-2912
 - Contact Warehouse at 301-372-2925 to arrange pickup
 - Pick-ups are scheduled for every Thursday of the week.
- Transfers Options Outside the Washington Metro Area:
 - FRC courier service (contact nearest FRC)
 - FedEx: Shipments for less than 24 boxes
 - USPS
- Shipment greater than 24 boxes
 - Contact FRC to schedule transfer time and date
 - Commercial carriers must contact FRC 24 hours before delivery
- Shipments must be made within 90 days after SF-135 has been approved
- After records are shelved, the FRC will send a notification of receipt to the office transferring the records listed in box 5 of the SF-135 form.



RETRIEVING RECORDS FROM FRCs

Federal agencies can request the return of their records in two ways:

- Complete an Optional Form 11 (OF -11)
- Or through the ARCIS online system.
 - www.Archives.gov/FRC
 - Requester must have ARCIS account approved by Agency Records Officer.