Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NOAA Environmental Security Computing Center

(NESCC) – NOAA0520

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NOAA Environmental Security Computing Center (NESCC)

Unique Project Identifier: NOAA0520

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: NESCC SCADA integrated information system (NOAA0520 or "0520") is a general facility support system which provides multiple environmental and physical access control resources to the NOAA Environmental Security Computing Center facility ("NESCC") and multiple NOAA programs. NOAA0520 system is a supervisory control and data acquisition (SCADA) system which monitors the facility's environment controls and physical access control points. The NESCC facilities primary function is to provide co-location resources and services, including common physical and environmental controls, to the various NOAA programs that reside in the building. The tenants within the NESCC facility include:

1. NOAA Research and Development High Performance Computing System (R&D HPCS);
2. NOAA Cyber Security Division (CSD);
3. One (1) NOAA Leadership COOP site;
4. Bureau of Industry and Standards (BIS)
5. NESDIS (JPSS)
6. Information Technology Center (ITC)
7. NOAA Service Delivery Division (SDD)

NOAA0520 is under the Department of Commerce, National Oceanic and Atmospheric Administration, Office of the Chief Information Officer (DOC/NOAA/OCIO). It is located Fairmont, West Virginia inside a leased facility designed to support multiple mission requirements for NOAA assisting in high availability and redundancy with high environmental and physical capabilities. As a leased facility, NOAA0520 shares office and computer space with all tenants listed above.

PII consists of information provided for building and restricted area access, including video data. PII inside of the NOAA0520 system boundary is only accessible by Federal employees and NOAA0520 support contractors for the determination of access and badge coding.

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.*

__X_ 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.*

__X_ 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

__X_ 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..."

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

__X_ DOC employees

__X_ 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?

__X_ 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 NOAA Environmental Security Computing Center (NESCC) 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 NOAA Environmental Security Computing Center (NESCC) 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):

Justin May (ISSO)_____

Signature of ISSO or SO: MAY.JUSTIN.NATHANIEL.1039635980 2018.08.08 10:04:37 -06'00' Date: 08 Aug 18

Name of Information Technology Security Officer (ITSO):

Jean Apedo_____

Signature of ITSO: ROGERS.WILLIAM.GUY.1520768811 Digitally signed by ROGERS.WILLIAM.GUY.1520768811 Date: 2018.08.13 07:21:58 -04'00' Date: 8 Aug 2018

Name of Authorizing Official (AO):

Douglas Perry_____

Signature of AO: PERRY.DOUGLAS.A.1365847270 Digitally signed by PERRY.DOUGLAS.A.1365847270 Date: 2018.08.14 07:30:14 -04'00' 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: 2018.08.14 12:18:53 -04'00' Date: _____