Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NOAA5050/GOES-R
Ground System

U.S. Department of Commerce Privacy Threshold Analysis

NOAA GOES-R Ground System

Unique Project Identifier: NOAA5050/GOES-R

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).

The NOAA5050/GOES-R Ground System (GS) is a Major Application and is comprised of the Satellite Operations Zone (SOZ) which operates from three sites which include: The NOAA Satellite Operations Facility (NSOF) in Suitland, MD which houses the primary Mission Management (MM), and selected Product Generation (PG), Product Distribution (PD), Enterprise Management (EM), and Infrastructure (IS) functions. The Wallops Command and Data Acquisition Station (WCDAS), located in Wallops, VA, provides the primary space communications services, MM, EM, and IS functions, and selected PG and PD functions. The third site is a geographically diverse Consolidated Backup facility (CBU) located at Fairmont, WV sometimes also referred to as the RBU. It functions as a completely independent backup for the MM and selected PG and PD functions for the production of Key Performance Parameters (KPPs) and GOES Rebroadcast (GRB) data, and is capable of concurrent and remote operations from NSOF and WCDAS. The CBU has visibility to all operational and on-orbit spare satellites. The KPPs consist of the L2+ Cloud and Moisture Imagery (CONUS, Full Disk, and Mesoscale) product and its sectorized products. The EM function is integrated across all ground segment components and locations. The IS Element's primary purpose is to provide common services for the Ground Segment that are utilized by all GS elements. The GS Antenna System provides the Space-to-Ground and Ground-to-Space interface with the GOES-R series satellites.

The GOES-R GS also includes the Product Processing Zone (PPZ), a separate operational enclave within the NOAA5050 Assessment and Authorization (A&A) boundary that is logically separated via distinct access controls and mechanisms. The GOES-R PPZ is comprised of its own implementations of PG, PD, EM, IS and includes the PPZ Edge.

The GOES-R PPZ PG Element produces Level 1b and Level 2+ end-products from the data collected by the GOES-R instruments and turn hands these products over to the PPZ PD Element where it distributes the following product files to PDA: L1b and L2+ GOES-R Products, Metadata, Mission Operations Data, L1b and L2+ Algorithm Packages, GRB Information files,

Instrument Calibration Data, Sample Outlier Files, L2+ and L1b Processing Parameters. The GOES-R Edge, in turn, distributes instrument calibration data, GRB info and sample outlier files that are forwarded to NSOF for distribution to PDA.

The raw sensor data is received by WCDAS, processed by the PG function at WCDAS to create L1b and L2+ GLM products. These L1b and L2+ GLM products are then rebroadcasted through the spacecraft GRB transponder. The GRB data are then received at NSOF where the rest of the L2+ products are created. Ancillary data used in generating the L2+ products are ingested from the Ancillary Data Relay System (ADRS) - (external to NOAA5050/GOES-R). Applicable products are directly distributed to 1) the National Weather Service (NWS) Advanced Weather Interactive Processing System (AWIPS) - (external to NOAA5050/GOES-R) where key NWS Weather Forecast Offices (WFO) and other AWIPS users get their data, and 2) the Product Distribution and Access (PDA) component of the Environmental Satellite Processing and Distribution System (ESPDS) - (external to NOAA5050/GOES-R), which includes the GOES-R Access Subsystem (GAS) functionality and ADRS functionality, provides data to NESDIS, NWS, and other GOES data users. There are approximately 300 users of NOAA5050/GOES-R (primarily at the NSOF and WCDAS sites).

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 NOAA5050/GOES-R 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 NOAA5050/GOES-R 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): _____

Victor Kalu, ISSO

Signature of ISSO or SO: KALU.VICTOR.EYE.1510028933 Digitally signed by KALU.VICTOR.EYE.1510028933 Date: 2018.05.04 11:33:15 -04'00' Date: 05/04/2018

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: _____