Version Number: 01-2017

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

Privacy Threshold Analysis
for the
NESDIS Headquarters Information System NOAA5006

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NESDIS HQ LAN/NOAA5006

Unique Project Identifier: NOAA IT Infrastructure investment code 006-000351100

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: NESDIS Assistant Chief Information Officer –Satellites (ACIO-S), located in NOAA/NESDIS Headquarters. NOAA5006 provides the Local Area Network (LAN) and Windows administrative support and services for the following offices and locations
NESDIS Headquarters facility in the Silver Spring Metro Center (SSMC) Building 1 and Building 3, the NOAA Joint-Polar Satellite System (JPSS) Office (NJO) located in the Aerospace building and GreenTec4 [GT4] building of the NASA Goddard Space Flight Center (GSFC), Lanham, Maryland, National Centers for Environmental Information (NCEI) offices located in Maryland, Mississippi, Colorado, and North Carolina,
Center for Satellite Applications and Research (STAR) in College Park, Maryland and the NOAA Satellite Operations Facility (NSOF).

NOAA5006 also supports the Office of Space and Commerce (OSC) located in the Herbert C. Hoover Building located at 1401 Constitution Avenue Washington, DC. NOAA5006 does not provide LAN or VoIP services to OSC. The purpose of NOAA5006 is to provide mission support and resources for IT management functions and overall office automation support for the programs, offices, and staff of the offices listed above. NOAA5006 servers are located in each of the physical locations and managed by NOAA5006 Support Staff at the specified locations.

NOAA5006 is a Federal Information Processing Standard (FIPS) 199 moderate security impact category system.

Questionnaire:

1. What is the status of this information system?

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

__X__ 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	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): Addition of users from NCEI, STAR and NSOF systems.					

____ 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.*

_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.)."

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

___X_ Companies
__X__ 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..."

___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 NOAA5006 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 NOAA5006 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): Ericka Evans Sterling

Signature of ISSO or SO: STERLING.ERICKA.EVANS.1471844817 Digitally signed by STERLING.ERICKA.EVANS.1471844817 Date: 2018.03.08 07:04:10 -05'00' Date: 03/08/2018

Name of Information Technology Security Officer (ITSO): Nancy DeFrancesco

Signature of ITSO: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 Date: 2018.03.08 07:39:43 -05'00' Date: 03/08/2018

Name of Authorizing Official (AO): Irene Parker

Signature of AO: Irene Parker Date: 3/8/2018

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: 2018.03.08 09:15:05 -05'00' Date: _____