Version Number: 01-2019

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the

NESDIS Center for Satellite Applications and Research (STAR) LAN

NOAA5018

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/STAR LAN

Unique Project Identifier: 006-48-01-16-01-3201-00 and 006-48-01-16-01-3202-00

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 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

NOAA5018 is a general support system.

b) System location

NOAA5018 is at the NOAA Center for Weather and Climate Prediction (NCWCP), College Park, MD 20740.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA5018 interconnects with the following systems:

- NOAA0100, NOAA Security Operations Center (SOC)
- NOAA0550, NOAA N-Wave Network
- NOAA5006, NESDIS Headquarters LAN
- NOAA5048, NESDIS GRAVITE (Government Resource for Algorithm Verification, Independent Test, and Evaluation)
- NOAA8860, NWS/NCEP WCCIS (Weather and Climate Computing Infrastructure Services)

d) The purpose that the system is designed to serve

NOAA5018 is the main scientific IT system for the NESDIS Center for Satellite Applications and Research (STAR).

STAR is the science arm of the National Environmental Satellite, Data, and Information Service (NESDIS), which acquires and manages the nation's environmental satellites for the National Oceanic and Atmospheric Administration (NOAA). STAR research activities, integral to the implementation of NOAA's research priorities, are aligned with and carried out in direct support of NOAA and NESDIS programs, strategic goals, and performance objectives.

STAR's mission is to accelerate the transfer of satellite observations of the land, atmosphere, ocean, and climate from scientific research and development into routine operations, and offer state-of-the-art data, products and services to decision-makers.

e) The way the system operates to achieve the purpose

NOAA5018 consists of approximately 400 CentOS Linux workstations and servers, connected to Cisco/IOS switches and a Cisco ASA firewall. NOAA5018 also contains one Oracle Solaris server, a few OpenBSD systems, a few Apple Mac OS-X systems, a large amount of disk storage systems from Dell, NetApp, and Supermicro, and VMware ESXi hypervisors.

f) A general description of the type of information collected, maintained, use, or disseminated by the system

NOAA5018 is primarily used for scientific research and development. In this respect, it primarily contains scientific data, code, documentation, publications, etc. The type of scientific data processed, stored, and transmitted by STAR, includes remote-sensing observations of the land, atmosphere, ocean, and climate, provided by Earth-orbiting satellite observing systems and in-situ readings.

g) Identify individuals who have access to information on the system

Approximately 300 individuals utilize NOAA5018. Ten of those individuals are privileged IT Administrators of the system. The remainder are non-privileged scientists and developers.

h) How information in the system is retrieved by the user

Information in the system is retrieved by users, via secure protocols such as SSH, SCP, HTTPS, FTPS, and SFTP.

i) How information is transmitted to and from the system

Information is transmitted to and from the system via secure protocols such as SSH, SCP, HTTPS, FTPS, and SFTP.

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). *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 01-2017 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. *(Check all that apply.)*

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

_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.

_X_ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII 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."

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

_X_ DOC employees
____ National Institute of Standards and Technology Associates
_X_ Contractors working on behalf of DOC
____ Other Federal Government personnel
____ 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 Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.

Provide the legal authority which permits the collection of SSNs, including truncated form.

_X_ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. 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.

4d. 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, 4c, and/or 4d 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 NOAA5018 STAR LAN 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 NOAA5018 STAR LAN 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): Joseph Brust

Signature of ISSO or SO: BRUST.JOSEPH.P.1365839405 Digitally signed by BRUST.JOSEPH.P.1365839405 Date: 2020.10.13 14:45:59 -04'00' Date: _____

Name of Information Technology Security Officer (ITSO): Joseph Mangin

Signature of ITSO: MANGIN.JOSEPH.THOMAS.1387933316 Digitally signed by MANGIN.JOSEPH.THOMAS.1387933316 Date: 2020.10.22 13:49:40 -04'00' Date: _____

Name of Privacy Act Officer (PAO): Adrienne Thomas

Signature of PAO: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2020.10.23 09:50:52 -04'00' Date: _____

Name of Authorizing Official (AO): Harry Cikanek

Signature of AO: CIKANEK.HARRY.ARTHUR.1407278204 Digitally signed by CIKANEK.HARRY.ARTHUR.1407278204 Date: 2020.10.20 11:41:05 -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 Date: 2020.11.02 08:37:23 -05'00' Date: _____