

U.S. Department of Commerce
NOAA



Privacy Threshold Analysis

**NESDIS Center for Satellite Applications and Research
(STAR) LAN**

NOAA5018

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/STAR LAN

Unique Project Identifiers: 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:

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.

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.

NOAA5018 resides on a private firewalled network, located at the NOAA Center for Weather and Climate Prediction (NCWCP), in College Park, MD 20740.

NOAA5018 is primarily used for scientific research and development. In this respect, it primarily contains scientific data, code, documentation, publications, etc. NOAA5018 does not facilitate e-commerce or other similar transactions. Rather, typical NOAA5018 "transactions" include scientific processes, and scientific data input, output, and production.

The type of data processed, stored, and transmitted by STAR includes scientific, remote-sensing observations of the land, atmosphere, ocean, and climate, provided by Earth-orbiting

satellite observing systems and in-situ readings.

The Security Categorization of NOAA5018 has been determined to be moderate using the guidance in FIPS 199 and NIST SP 800-60.

Relevant to this PIA, NOAA5018 hosts the following:

- PII in the form of a basic personnel roster available to the public via the STAR Web site.
- System Administration/Audit Data (SAAD) of STAR employees to facilitate IT administration, and especially IT Security administration.

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

X I certify the criteria implied by one or more of the questions above **apply** to NOAA5018 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 NOAA5018 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, SO

Signature of ISSO or SO: BRUST.JOSEPH.P.136583 9405 Digitally signed by BRUST.JOSEPH.P.1365839405 Date: 2019.08.13 10:09:27 -04'00' Date: _____

Name of Information Technology Security Officer (ITSO): Frank Menzer

Signature of ITSO: MENZER.FRANK.E.1026670450 Digitally signed by MENZER.FRANK.E.1026670450 Date: 2019.08.13 12:01:08 -04'00' Date: 8/13/2019

Name of Authorizing Official (AO): Harry Cikanek

Signature of AO: CIKANEK.HARRY.ARTHUR.III.140727820 4 Digitally signed by CIKANEK.HARRY.ARTHUR.III.1407278204 Date: 2019.08.22 16:53:30 -04'00' Date: _____

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

Signature of BCPO: GRAFF.MARK.HYRUM.1514 447892 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: 2019.09.05 16:04:00 Date: _____