Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NOAA5044
NOAA Satellite Operations Facility (NSOF) Administrative LAN

U.S. Department of Commerce Privacy Threshold Analysis

NOAA5044

NOAA Satellite Operations Facility (NSOF) Administrative LAN

Unique Project Identifier: [Number]

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).

General Description – NSOF Admin LAN (NOAA5044) is a FIPS 199 moderate designated general support system that is physically located in the NOAA building at 4231 Suitland Road, Suitland, Maryland, a suburb of Washington, D.C. The building is owned by NOAA and managed and secured by the General Services Administration. The NSOF Admin LAN provides standard office automation for all NESDIS employees located within the NSOF. It also provides access to the Internet. The LAN provides end-to-end connectivity and network access to all LAN Federal employee and contract users, to increase productivity through the use of applications, data resources, or other electronic office automation tools.

The two types of applications supported by the NSOF Admin LAN -- server applications and client applications -- are considered minor applications in that they are accredited as a GSS rather than separately. There are no major applications (as defined by OMB A-130) in the NSOF Admin LAN environment.
There are five user communities located in the NSOF: the Office of Satellite Ground Systems (OSGS), the Office of Satellite and Product Operations (OSPO), the General Services Administration (GSA), the National Ice Center (NIC) and the Defense Meteorological Satellite Program (DMSP). These user communities have dedicated workstations connected to the NSOF Admin LAN. NOAA5044 provides access to automated programs and systems supporting administrative programs such as budget and financial management, personnel management, procurement, building operation and management, interagency programs, IT planning, and IT security. The system also supports access to the Internet. There is electronic personnel related information about NOAA employees and prospective employees maintained on the NSOF Admin LAN, containing information such as SSN, Passport, Credit Card, Vehicle identifier, Name, Maiden Name, Gender, Age, Date of Birth, Place of Birth, Home Address, Telephone

Number, Email Address, Financial Information, Military Service, Occupation, Job Title, Work Address, Telephone Number, Work History. In addition, the system maintains onboarding forms, training forms (SF-182), resumes, and vehicle information for parking. Version Number: 01-2015

DOC and DOD performance evaluation are also compiled and maintained in the system. The appropriate forms are completed on the NOAA5044 Manager's secure home directory. They are then printed, hand-carried for signature, and then transferred via the agency-specific secure electronic transfer procedure.
There is also ESPC account management, collecting contact information, such as name, work phone number and work email address from individuals or organizations wishing to access ESPC data via its distribution mechanisms, or to supply data as may be appropriate. This information is voluntarily submitted through the use of forms or email and is stored in restricted areas of the NSOF Admin LAN shared drive only accessible by authorized personnel. The information is collected to ensure the user receives the correct products in line with their request, or to allow an ESPC program manager to validate that a proposed supplier is a legitimate organization able to supply the information being proposed. The information may also be used to notify users and suppliers in the event of an outage or other type of service disruption.
In addition, the NOAA5044 collects PII of NSOF LAN personnel on a voluntary basis for purposes of Continuity of Operations Planning (COOP). This data is stored on a LAN shared drive only accessible by authorized personnel.
The PII/BII information collected by NOAA5044 is shared with other agencies or parties on a case-by-case basis, as described below. If any of the data is sensitive or For Official Use Only (FOUO), then the data is restricted by drives and folders to only NSOF Admin LAN personnel authorized to access the information.

NSOF Admin LAN currently has interconnections with 6 other NOAA systems. NOAA5044 is connected to NOAA0100 via network using SSL Protection transmitting and receiving unclassified information. NOAA5044 is connected to NOAA0200 via network using SSL protection to send but not receive unclassified data. NOAA5044 is connected to NOAA5006 via network using a site to site VPN to transmit and receive unclassified data. NOAA5044 is connected to NOAA5008 via network using a site to site VPN to send unclassified data. NOAA5044 is connected to NOAA5032 via network using a site to site VPN to send unclassified data. NOAA5044 is connected to NOAA5040 via network using SSL Protection transmitting and receiving unclassified information.

Transfers - The system collects PII of DOC (NOAA employees only) and DOD civilian and military personnel to the extent necessary for preparation of performance, promotion, and awards for these personnel. The NSOF Admin LAN contains personally assigned network shares (H:\), which are accessible only by the person assigned the shared drive.
DOC electronic personnel related forms (NOAA employees only) may be transferred to DOC Bureau HR personnel in bulk or on a case-by-case basis via DOC Accellion (for DOC records only) or via tracked United Parcel Service (UPS) package.

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.)."

_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 NOAA5044 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 NOAA5044 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): Brian Little, NOAA5044 ISSO

Signature of ISSO or SO: LITTLE.BRIAN.WILLIAM.1365841230 Digitally signed by LITTLE.BRIAN.WILLIAM.1365841230 Date: 2018.03.13 15:03:02 -04'00' Date: _____

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

Signature of ITSO: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 Date: 2018.03.13 15:21:20 -04'00' Date: 03/13/2018

Name of Authorizing Official (AO): Vanessa L. Griffin

Signature of AO: GRIFFIN.VANESSA.L.1204308663 Digitally signed by GRIFFIN.VANESSA.L.1204308663 Date: 2018.03.15 16:34:59 -04'00' Date: 03/15/2018

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: 2018.03.20 16:06:22 -04'00' Date: 3/20/18