

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



**Privacy Threshold Analysis
for the
NESDIS Administrative
LAN (NOAA5006)**

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NESDIS Admin LAN/NOAA5006

Unique Project Identifier: NOAA IT Infrastructure investment code 006-000351100-00-48-02-00-01-00

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: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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*

NOAA5006 is a general support system provided by the NESDIS Assistant Chief Information Officer – Satellites (ACIO-S) to most of the NESDIS offices.

b) *System location*

System locations are:

- NESDIS Headquarters facility in Silver Spring Metro (SSMC) Center I and III
- NOAA Joint Polar Satellite System (JPSS) Office (NJO) located at GreenTec4 (GT4) building of the NASA Goddard Space Flight Center (GSFC), Lanham MD
- National Centers for Environmental Information offices located in Maryland, Mississippi, Colorado, and North Carolina
- Center for Satellite Applications and Research (STAR) in College Park, Maryland
- NOAA Satellite Operations Facility (NSOF) in Suitland, MD
- Wallops Control and Data Acquisition Station (WCDAS) in Wallops Island, Virginia
- Fairbanks Control and Data Acquisition Station (FCDAS) in Fairbanks, Alaska

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.

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

NOAA5006 is a Moderate-level system which maintains interconnects with:

- NOAA (NOAA0100, NOAA0200, NOAA0500, NOAA1200) for shared services (VPN, Internet, McAfee, ArcSight, SOC, etc.)
- NOAA (NOAA1300) for National Service Desk
- NASA for SharePoint services at NJO
- NOAA5009, NOAA5010, NOAA5011 for access to those mission systems
- NOAA5018 for mission system access
- NOAA5040 for mission system access
- NOAA5044 for mission system access

- d) *The purpose that the system is designed to serve*

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.

- e) *The way the system operates to achieve the purpose*

To operate, NOAA5006 maintains a hardware stack (pod) at each location which hosts virtual servers that provide services needed by that site. Workstations connect to the pod via Cisco switches, and pods interconnect with each other over N-Wave. The Boulder and NSOF locations provide services used by multiple locations and contain backups of all data from all other pod sites.

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

General administrative data, which includes some PII and BII. NOAA5006 stores this information for administrative purposes but does not process it.

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

Access is limited to authorized user operating within the requirements of their job.

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

Typically, users retrieve information from the system by accessing files on their local file server, or on a remote file server in some cases. They also access websites using HTTP or HTTPS (internal as well as external) and Commerce applications. Network printers allow users to print when necessary.

i) How information is transmitted to and from the system.

Transmissions from the system take place over secured protocols (HTTPS and SFTP primarily) and go through NOAA5006 IPS and the NOAA NOC's security filters and systems before the Internet.

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): The Decommission of two NOAA FISMA Systems (NOAA5008 and NOAA5032) The users and data have been merged on to NOAA5006.					

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.

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):			

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.

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."

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

DOC employees

- National Institute of Standards and Technology Associates
- 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.

Badging requires I-9 forms, security paperwork, and similar needs.

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

This information is collected under the authority of 5 U.S.C., including Section 301. In addition, Title 31 U.S.C. 66a, 492, Title 44 U.S.C. 3101, 3309 and the Federal Collection Claim Act of 1966 apply. Additional authorities include E-Government Act of 2002 (Pub. L. 107-347) Section 204 and Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204 and 2 CFR, Subtitle A, Chapter I, and Part 25.

From NOAA-11: 5 U.S.C. 301, Departmental Regulations and 15 U.S.C. 1512, Powers and duties of Department.

From DEPT-5: Freedom of Information Act, 5 U.S.C. 552; Privacy Act of 1974 as amended, 5 U.S.C. 552a; 5 U.S.C. 301, and 44 U.S.C. 3101.

From DEPT-9: Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966.

From DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 *et seq.*; 28 U.S.C. 533-535; 44 U.S.C. 3101; Equal Employment Act of 1972; and all existing, applicable Department policies, and regulations.

From DEPT-14: 5 U.S.C. 301; 44 U.S.C. 31101; 42 U.S.C. 3211; 31 U.S.C. 240; 28 U.S.C. 533-535 and 1346(b); 15 U.S.C. 277 and 278e(b); E.O. 10450; E.O. 11478, as amended and all other authorities of the Department.

From DEPT-18: Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

From DEPT-25: 5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075.

From GSA/GOVT-9: For the Entity Management functional area of SAM, the authorities for collecting the information and maintaining the system are the Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204 and 2 CFR, Subtitle A, Chapter I, and Part 25, as well as 40 U.S.C. 121(c). For the exclusions portion of the Performance Information functional area, the authorities for collecting the information and maintaining the system are FAR Subparts 9.4 and 28.2, Executive Order 12549 (February 18, 1986), Executive Order 12689 (August 16, 1989).

From GSA/GOVT-10: E-Government Act of 2002, Section 204; Davis-Bacon and Related Acts; 40 U.S.C. 3141-3148; 40 U.S.C. 276a; 29 CFR parts 1, 3, 5, 6 and 7; Section 5 of the Digital Accountability and Transparency Act (DATA Act); Public Law 113-101.

From OPM/GOVT-1: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

From OPM/GOVT-5: 5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397.

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?

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.

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 PIA 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):

Manan Dalal

Signature of ISSO or SO: DALAL.MANAN.SU Digitally signed by DALAL.MANAN.SUNIL.1380715577 Date: 2019.12.30 12:44:07 -05'00' NIL.1380715577 Date: _____

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

Signature of ITSO: MENZER.FRANK.E.1 Digitally signed by MENZER.FRANK.E.1026670450 Date: 2019.12.31 08:30:53 -05'00' 026670450 Date: 12/31/2019

Name of Privacy Act Officer (PAO): _____

Signature of PAO: THOMAS.ADRIENNE.M.13 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2020.01.03 16:21:16 -05'00' 65859600 Date: _____

Name of Authorizing Official (AO): Irene Parker

Signature of AO: Irene Parker Date: 12/31/2019

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

Signature of BCPO: INDIVIGLIO.FRANK.M.1380923714 Digitally signed by INDIVIGLIO.FRANK.M.1380923714 Date: 2020.01.13 16:28:20 -05'00' _____