Version Number: 01-2021

U.S. Department of Commerce
National Oceanic & Atmospheric Administration

Privacy Threshold Analysis for the
NOAA5006
NESDIS Administrative Local Area Network (NESDIS Admin LAN)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NESDIS/NESDIS Admin LAN

Unique Project Identifier: NOAA5006

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: *Provide a brief description of the information system.*

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).

NESDIS Administrative LAN (NOAA5006) operates under the authority of the NESDIS Assistant Chief Information Officer and provides the Local Area Network (LAN) and Windows administrative support and services for several NESDIS office locations. NOAA5006 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 and supports web pages providing NOAA information and data to the public.

Address the following elements:

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
- Comprehensive Large Array-data Stewardship System (CLASS) in Asheville, North Carolina

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, NOAA0201, NOAA0550) for shared services (VPN, Internet, McAfee, ArcSight, SOC, etc.)
- NOAA (NOAA1300) for National Service Desk
- NOAA1101 for MARS Application
- NASA for SharePoint services at NJO
- NOAA5009 and NOAA5011 for access to those mission systems
- NOAA5018 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, used, or disseminated by the system

NOAA5006 collects general administrative data, which includes some PII and BII. NOAA5006 stores this information for administrative purposes but does not process it. The Social Security Numbers are collected (temporarily) on NESDIS Admin LAN contractors and government employees for the sole purposes of conducting background investigations and on I-9 forms for hiring in accordance with 10 U.S.C. 133 and E.O. 9397. The processing of such information does not occur on NOAA5006. This information is only collected and, in some cases, may be stored electronically on the internal shared drives as well as in hard copies that are stored in locked file cabinets. The authorities are those in DEPT-18.

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

Access is limited to authorized user operating within the requirements of their job which include system owners, ITSO/ISSO, and other organizational employees including government employees, contractors, and support technicians.

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

Typically, users retrieve information from the system by using their Government Furnished Equipment (GFE) accessing files on their local file server, or on a remote file server (via VPN) 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. Status of the Information System

1a. 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. *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

____ No. This is not a new information system.

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

tothose 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
- ____ 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.

____ 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 PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ The criteria implied by one or more of the questions above **apply** to the NOAA5006 and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_____ 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.

Information System Security Officer or System Owner Name: Jeff Polyakov Office: NESDIS Phone: 240-408-6860 Email: Jeff.Polyakov@noaa.gov Signature: POLYAKOV.JEFF.1266288359 Digitally signed by POLYAKOV.JEFF.1266288359 Date: 2021.12.06 13:30:44 -05'00' Date signed:	**Information Technology Security Officer** Name: Rick Miner Office: ACIO-S Phone: 301-427-8822 Email: Rick.Miner@noaa.gov Signature: MINER.RICHARD.SCOTT.1398604519 2021.12.07 15:35:50 -05'00' Date signed:
Privacy Act Officer Name: Adrienne Thomas Office: NOAA OCIO Phone: 240-577-2372 Email: Adrienne.Thomas@noaa.gov Signature: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2021.12.13 11:16:55 -06'00' Date signed:	**Authorizing Official** Name: Irene Parker Office: ACIO-S Phone: 301-713-7080 Email: Irene.Parker@noaa.gov Signature: Irene Parker Date signed:
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2021.12.15 16:53:33 -05'00' Date signed:	