

**U.S. Department of Commerce**  
**NOAA**



**Privacy Threshold Analysis**  
**for the**  
**Data Archive Management and User System**  
**NOAA5011**

## U.S. Department of Commerce Privacy Threshold Analysis

### NOAA/Data Archive Management and User System

**Unique Project Identifier: 06-000321900**

**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).

NOAA's National Centers for Environmental Information (NCEI) are responsible for hosting and providing access to one of the most significant archives on earth, with comprehensive oceanic, atmospheric, and geophysical data. From the depths of the ocean to the surface of the sun and from million-year-old tree rings to near real-time satellite images, NCEI is the Nation's leading authority for environmental information. By preserving, stewarding, and maximizing the utility of the Federal government's billion-dollar investment in high-quality environmental data, NCEI remains committed to providing products and services to private industry and businesses, local to international governments, academia, as well as the general public.

The demand for high-value environmental data and information has dramatically increased in recent years. NCEI is designed to improve NOAA's ability to meet that demand. The Consolidated and Further Continuing Appropriations Act, 2015, Public Law 113-235, approved the consolidation of NOAA's existing three National Data Centers: the National Climatic Data Center, the National Geophysical Data Center, and the National Oceanographic Data Center into the National Centers for Environmental Information. NCEI has employees in four major locations: Asheville, NC; Boulder, CO; Silver Spring, MD; and Stennis Space Center, MS.

**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*

General Support System (GSS)

b) *System location*

NOAA5011 is physically located in the David Skaggs Research Center in Boulder, CO.

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

NOAA5011 has interconnections with NCEI-NC (NOAA5009) and NCEI-MD/MS (NOAA5010) that were created to facilitate sharing internal resources. These include access to each system's intranet applications and shared code repositories. Access to resources is approved via the configuration management process. NOAA5009, NOAA5010, and NOAA5011 are classified as moderate systems and may exchange data at that categorization level. NOAA5011 agreements are in place for services between NOAA5011 and other government agencies or universities.

The below connection agreements are in force:

<b>Organization</b>	<b>Purpose</b>	<b>Agreement Type</b>
<b>NOAA0100 - NOAA Cyber Security Center</b>	SOC ISAs/SLAs	NOAA CIO Waiver
<b>NOAA0550 – NOAA NWAIVE</b>	NW Connectivity	ICD
<b>NOAA5006 - Headquarters Information Technology Support Local Area Network</b>	NW / Office Apps	ICD
<b>NOAA5040 - Comprehensive Large Array-data Stewardship System</b>	Internet & Office Space	C

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

NOAA5011 conducts a data and data- information service in all scientific and technical areas involving solid earth geophysics, marine geology and geophysics, glaciology, space environment, solar activity, and the other areas of solar-terrestrial physics. All data provided is publicly available and is harvested from the archive or via public web sites. None of this data is subject to interconnection agreements.

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

NCEI-CO receives data from other NOAA groups, other federal government agencies such as NASA, the U.S. Air Force, the U.S. Geological Survey; federally funded research institutions such as the National Center for Atmospheric Research (NCAR), and the Woods Hole Oceanographic Institution; universities such as the University of Colorado - National Snow and Ice Data Center (NSIDC), and the Ocean Drilling Program at Texas A&M University; state agencies such as the Alaska Department of Natural Resources, California Department of Water Resources; and intergovernmental entities such as the European Space Agency, and the Australian Surveying and Land Information Group (AUSLIG). The system operates in the traditional client-server model. Data is hosted on servers and made available via various protocols such as HTTPS, FTP, SFTP, and SSH.

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

NOAA5011 data and data-information services encompass all scientific and technical areas involving solid earth geophysics, marine geology and geophysics, glaciology, space environment, solar activity, and the other areas of solar-terrestrial physics. The Center prepares systematic and special data products and performs data-related research studies to enhance the utility of the service to the users. It performs all functions related to data acquisition, archiving, retrieval, indexing, quality assessments, evaluation, synthesis, dissemination, and publication.

Employee Info:

- Name
- Personal email address
- Personal phone number
- Home address

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

NOAA5011 has approximately 108 users that connect within NOAA5011's security boundary (internal users). The NOAA5011 user environment consists mainly of web developers, scientists, system administrators, administrative assistants, managers, customer service representatives, database administrators, and graphic designers.

External users include, but are not limited to, other federal government agencies such as NASA, the U.S. Air Force, the U.S. Geological Survey; federally funded research institutions such as the National Center for Atmospheric Research (NCAR), and the Woods Hole Oceanographic Institution; universities such as

the University of Colorado - National Snow and Ice Data Center (NSIDC), and the Ocean Drilling Program at Texas A&M University; state agencies such as the Alaska Department of Natural Resources, California Department of Water Resources; and intergovernmental entities such as the European Space Agency, and the Australian Surveying and Land Information Group (AUSLIG).

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

Internal NOAA5011 users retrieve data via internal file servers, the public web presence, and via anonymous FTP. External users retrieve data via the NOAA5011 public web presence and via anonymous FTP downloads of public data.

Organizational users authenticate using GFE (Government Furnished Equipment) and their Common Access Card to access in the information system. This provides users secure access that is managed by the program and supported by NOAA 5011.

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

NOAA5011 (NCEI-CO) has a dedicated 10 gigabits per second (Gbps) link providing Wide Area Network (WAN) access from NCEI-CO to the Internet through the NOAA NWAVE (NOAA0550). Physical connectivity is provided via standard Ethernet configured at 10 Gbps. Endpoint access to the Internet is configured at 30 Gbps and provided via the N\_WAVE TICAP Service in Boulder, CO. In addition, NCEI-CO receives data from NOAA ships via external disk drives for data processing. The data from these disks are loaded onto local file servers on NOAA5011.

Information is transmitted to and from the system using the following protocols using a client/server model: SFTP, FTP, SSH, and HTTPS.

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.*

<b>Changes That Create New Privacy Risks (CTCNPR)</b>					
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.*

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.

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.

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 Data Archive Management and User System (NOAA5011 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 Data Archive Management and User System (NOAA5011 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): Jason Symonds

Signature of ISSO or SO: 77411 Digitally signed by SYMONDS.JASON.T.13667 Date: 2020.08.05 12:40:15 -04'00' Date: \_\_\_\_\_

Name of Information Technology Security Officer (ITSO): Robert Bunge

Signature of ITSO: BUNGE.ROBERT.DAVID.1207631279 Digitally signed by BUNGE.ROBERT.DAVID.1207631279 Date: 2020.08.07 15:34:40 -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: 2020.08.11 10:01:35 -04'00' Date: \_\_\_\_\_

Name of Authorizing Official (AO): Mary Wohlgemuth

Signature of AO: WOHLGEMUTH.MARY.STANFORD.1228710519 Digitally signed by WOHLGEMUTH.MARY.STANFORD.1228710519 Date: 2020.08.11 09:23:25 -04'00' Date: \_\_\_\_\_

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

Signature of BCPO: 47892 Digitally signed by GRAFF.MARK.HYRUM.15144 Date: 2020.08.13 12:14:30 -04'00' Date: \_\_\_\_\_