Version Number: 01-2019

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
National Oceanographic Data Center (NODC) LAN
NOAA5010

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/National Oceanographic Data Center LAN/NOAA5010

Unique Project Identifier: 006-000321900

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).

Description of the information system and its purpose:

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

NOAA5010 is a General Support System.

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. NCEI located in Maryland and Mississippi comprise the NOAA5010 system.

NCEI-MD provides access to the world's most comprehensive sources of marine environmental data and information. NCEI-MD maintains and updates a national ocean archive with environmental data

acquired from domestic and foreign activities and produces products and metadata, and research from these data that help monitor global environmental changes.

These data include physical, biological, and chemical measurements derived from in situ oceanographic observations, satellite remote sensing of the oceans, and ocean model simulations. NCEI-MD manages and operates the World Data Center (WDC) for Oceanography in Silver Spring, MD. Its personnel directly interact with federal, state, academic, and industrial oceanographic activities; represent NESDIS on various interagency domestic panels, committees and councils; and represent the United States in various international organizations, such as the International Oceanographic Data Exchange. NCEI-MD and NCEI-MS represent NESDIS and NOAA to the general public, government agencies, academic institutions, foreign governments, and the private sector on matters involving oceanographic data.

External users of the Public Web consist of an average of 170,000 unique visitors per month. These users include but are not limited to other NOAA agencies, other federal government agencies such as U.S. Geological Survey, the Environmental Protection Agency, universities-Mississippi State University, University of New Hampshire, Texas A&M, University of South Florida, and state agencies- Mississippi Department of Marine Resources, Louisiana Department of Natural Resources, Alabama Department of Conservation and Natural Resources, Texas Parks and Wildlife, and Florida Fish and Wildlife Commission.

The NESDIS HQ Administrative (Admin) Local Area Network (LAN) (NOAA5006) boundary has been extended to provide common administrative services across NESDIS. NCEI-MD and NCEI-MS users and laptops/desktops physically reside within the Admin LAN boundary. The Mission LAN hosts a terminal server cluster which allows Admin LAN users to access Mission services. NOAA5010 System Administrators maintain direct access to the NOAA5010 Mission LAN for system maintenance and management. The System of Records Notice (SORN): COMMERCE/DEPT-25, Access Control and Identity Management System covers the collection of this information.

If written consent is obtained using the DOC consent form, employee and contractor photographs may also be used for staff posters and shared with the public. The applicable SORN is COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies.

In order to better fulfill its mission, NCEI-MS receives data and information about the data providers (contact information on data providers consists of name, email address and physical address) from other NOAA groups, other federal government agencies such as Department of the Interior/Bureau of Ocean Energy Management, NASA, and the U.S. Navy; state agencies such as Alabama Department of Conservation and Natural Resources and Alaska Department of Environmental Management; academia such as Appalachian State University, Auburn University, Binghamton University, etc.; for-profit businesses such as Alpine Geophysical Associates, Inc., Arthur D. Little, Inc., Barry A. Vittor and Associates, Inc., etc.; non-profit organizations such as Battelle Memorial Institute, Bernice Apuahi Bishop Museum, etc.; and their non-U.S. equivalents such as South African Data Centre for Oceanography, Australian Oceanographic Data Center, Aichi Prefectural Fisheries Experimental Station (Japan), etc., and intergovernmental entities such as European Space Agency, World Climate Research Programme, International Oceanographic Data and Information Exchange, etc. Metadata information is initiated at the time of data collection and acquisition planning. As part of the data management process, metadata citation and contacts are reviewed and approved by the data owner. A Web-based submission form is being used to provide another means to collect this data and hold it for review before permanently placing it in the NCEI archive holdings. Data provider information is found within the

metadata for archived data and is made available to the public when data is downloaded from the archive. Per the U.S. Government Policy on Open Data M-13-13 – Memorandum for the Heads of Executive Departments and Agencies, Section 1, "Open data will be consistent with the following principles: Managed Post-Release. A point of contact must be designated to assist with data use and to respond to complaints about adherence to these open data requirements." Thus the contact information collected is made available to the public for contact purposes. In addition, the Project Open Data Metadata Resources for Schema v1.1 states the implementation requirements for Project Open Data metadata and name and email address are minimally required based on this guidance, see https://project-open-data.cio.gov/v1.1/schema/. NOAA NAO 212-15, the NOAA Data Documentation Directive, and the NOAA Plan for Public Access to Research Results all provide specific citation guidance for general documentation including metadata. The data provider contact information is covered by this SORN: COMMERCE/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.

Contractors provide support for the NOAA5010 mission by supporting acquisition, preservation, monitoring, and assessment of the Nation's treasure of coastal, oceanographic, and geophysical data and information. Contractors perform scientific analyses, product development, and data ingest, archive, and dissemination support. Contractors also provide system and network administration and security support of the NOAA5010 IT infrastructure.

b) System location

NCEI located in Maryland and Mississippi comprise the NOAA5010 system. NCEI-MD is located in Silver Spring, MD. NCEI-MS is located at the Mississippi State University Research and Technology Corporation (MSURTC) at Stennis Space Center (SSC), MS. Both the SSMC3 and Stennis Space Center are controlled-access government facilities.

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

NOAA5010 has interconnections with NCEI-NC (NOAA5009) and NCEI-CO (NOAA5011) 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. NOAA5010 agreements are in place for services between NOAA5010 and other government agencies or universities.

In addition, the below connection agreements are in force:

NOAA5010 Site	Organization	Purpose	Agreement Type
MS	Mississippi State University (MSU)	Bldg Lease	License
MD & MS	NOAA NOAA0100	SOC ISAs/SLAs	NOAA CIO Waiver
MS	Web Operation Center (WOC) NOAA0201	DNS Services	ISA
MS	National Ocean Service/Office of Coastal Management (NOS/OCM) NOAA6101	Internet & Office Space	LOA
MD	NOAA Satellite Operations Facility (NSOF) Mission Support LAN (MSL) NOAA5044	COOP	MOU
MS	NOAA Office of the Chief Information Officer (OCIO) NOAA0100	N-Wave Services	LOA
MD	NOAA Network Operation Center (NOC) (NOAA0200)	Internet Access	NOC does not require signed agreements for their standard services.

d) The purpose that the system is designed to serve

NOAA5010 provides access to the world's most comprehensive source of marine environmental data and information. 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

NOAA5010 maintains and updates a national ocean archive with environmental data acquired from domestic and foreign activities and produces products and metadata, and research from these data that help monitor global environmental changes.

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

The data stored in the NOAA5010 archive include physical, biological, and chemical measurements derived from in situ oceanographic observations, satellite remote sensing of the oceans, and ocean model simulations. NCEI-MD manages and operates the World Data Center (WDC) for Oceanography in Silver Spring, MD. Its personnel directly interact with federal, state, academic, and industrial oceanographic activities; represent NESDIS on various interagency domestic panels, committees and councils; and represent the United States in various international organizations, such as the International Oceanographic Data Exchange. NCEI-MD and NCEI-MS represent NESDIS and NOAA to the general public, government agencies, academic institutions, foreign governments, and the private sector on matters involving oceanographic data.

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

NOAA5010 has approximately 66 users that connect within NOAA5010's security boundary (internal users). The NOAA5010 user environment consists mainly of web developers, scientists, system administrators, administrative assistants, managers, customer service representatives, database administrators, and graphic designers. External users of the NOAA5010 public web consist of an average of 170,000 unique visitors per month. These external users include but are not limited to other NOAA agencies, other federal government agencies such as U.S. Geological Survey, the Environmental Protection Agency, universities-Mississippi State University, University of New Hampshire, Texas A&M, University of South Florida, and state agencies- Mississippi Department of Marine Resources, Louisiana Department of Natural Resources, Alabama Department of Conservation and Natural Resources, Texas Parks and Wildlife, and Florida Fish and Wildlife Commission.

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

Internal NOAA5010 users retrieve data via internal file servers, the public web presence, and via anonymous FTP. External users retrieve data via the NOAA5010 public web presence and via anonymous FTP downloads of public data.

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

NOAA5010 (NCEI-MD) has a dedicated 100 megabits per second (Mbps) link provides Wide Area Network (WAN) access from NCEI-MD to the Internet through the NOAA Network Operation Center (NOC) (NOAA0200) campus Metropolitan Area Network (MAN). NCEI-MS' physical infrastructure for Internet connection from the N-Wave router is provided by the Mississippi State University Research and Technology Corporation (MSURTC) which routes through the University of Southern Mississippi router. This Internet connection is NCEI-MS' only external connection. Physical connectivity is provided via multimode fiber and utilizes two 10 Gbps connections which provide connectivity to N-Wave's Washington and Denver TICAPs. In addition, NCEI-MS receives data from NOAA ships via external disk drives for data processing. The data from these disks are loaded onto local file servers on NOAA5010.

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). *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 01-2017 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):			

_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.)."

____ Yes, the IT system collects, maintains, or disseminates BII.

_X_ 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."

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

_X_ DOC employees
____ National Institute of Standards and Technology Associates
_X_ Contractors working on behalf of DOC
____ Other Federal Government personnel
_X_ 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.

_X_ 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?

_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.

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 National Oceanographic Data Center LAN/NOAA5010 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 National Oceanographic Data Center LAN/NOAA5010 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): Scott Hausman

Signature of ISSO or SO: HAUSMAN.SCOTT.ALTON.1036374590 Digitally signed by HAUSMAN.SCOTT.ALTON.1036374590 Date: 2020.07.07 10:47:51 -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: 2020.07.07 16:31:33 -04'00' Date: 7/7/2020

Name of Privacy Act Officer (PAO): Adrienne Thomas

Signature of PAO: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2020.07.17 14:10:01 -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: 2020.07.07 13:33:06 -04'00' Date: _____

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

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2020.08.03 12:49:14 -04'00' Date: _____