Version Number: 01-2015

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

National Oceanographic Data Center LAN/NOAA5010

Unique Project Identifier: 006-000321800 00-48-01-13-02-00

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 of the information system and its purpose 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).

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.

The NCEI-MD and NOAA Central Library, with its regional branch assets, are integrated to provide 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.

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):					

__X__ This is an existing information system in which changes do not create new privacy risks. *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.)."

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

____ Companies
____ Other business entities

__X__ 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
__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 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 NOAA5010 and as a consequence of this applicability, a PIA for this IT system is necessary. NOAA5010 has an approved PIA from 2016. PIA approved 9/6/2016. As there have been no changes creating new privacy risks, we will submit to DOC a certification that a new PIA is not needed at this time.

____ I certify the criteria implied by the questions above **do not apply** to the 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): _Juanita Sandidge_

Signature of ISSO or SO: SANDIDGE.JUANITA.C.1232228055 Digitally signed by SANDIDGE.JUANITA.C.1232228055 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=SANDIDGE.JUANITA.C.1232228055 Date: 2017.03.02 14:21:34 -06'00' Date: 3-2-2017

Name of Information Technology Security Officer (ITSO): _Nancy A. DeFrancesco_____

Signature of ITSO: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=DEFRANCESCO.NANCY.A.1377370917 Date: 2017.03.02 14:11:15 -05'00' Date: 03/02/2017

Name of Authorizing Official (AO): __Margarita Gregg_____

Signature of AO: GREGG.MARGARITA.ELENA.1365899017 Digitally signed by GREGG.MARGARITA.ELENA.1365899017 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GREGG.MARGARITA.ELENA.1365899017 Date: 2017.03.03 14:10:43 -05'00' Date: 03-03-2017

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: 2017.03.07 09:07:08 -05'00' Date: 3/7/17