Version Number: 01-2019

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NOAA8873-National Data Buoy Center (NDBC)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NDBC

Unique Project Identifier: 006-48-01-12-01-3119-00

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:

The National Data Buoy Center (NDBC), a part of the National Oceanic and Atmospheric Administration (NOAA), National Weather Service (NWS), Office of Observations (OBS) provides marine and coastal observations in support of the mission goals of NOAA to: Enable an informed society anticipating and responding to climate and its impacts; Prepare for and respond to weather-related events; Sustain marine fisheries, habitats, and biodiversity within healthy and productive ecosystems; and sustain the environment and economy of coastal and Great Lakes communities.

To support these goals the NDBC operates and provides data from four (4) observing systems of records:
Coastal Weather Buoy (CWB): A network of moored buoys, primarily located within the exclusive economic zone (EEZ) of the United States, which provide meteorological and oceanographic data in realtime.
Coastal-Marine Automated Network (C-MAN): A network of land based nearshore observation stations.
Deep-ocean Assessment and Reporting of Tsunamis (DART): A network of moored buoys, primarily located along the Pacific Ocean and Hawaiian islands, which provide tsunameter data to the National Tsunami Warning Center for assessment and warning.
Tropical Atmosphere Ocean (TAO): A network of moored buoys, primarily located within the equatorial Pacific, which provide oceanographic data to the NOAA scientific community.

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

Stennis Space Center, Mississippi
Silver Spring, Maryland

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

Amazon Web Services (AWS) –NOAA0201 WOC: Data Processing servers are IaaS within the FedRAMP GovCloud/SLA (NOAA BPA)

US Air Force Space Command Iridium: Satellite communications to transmit/receive data from stations/IAA

GOES—NOAA/NESDIS: Satellite communications to transmit/receive data from stations/ISA

HFRadar—Univeristy of California: NDBC hosts website to deliver radar data/ISA

Inmarsat Government: Satellite communications to transmit/receive data from stations/Contract

NOAA0201—NOAA WOC: Hosts NDBC's main website/SLA

NOAA3100—PMEL: NDBC hosts OSMC database and website to deliver weather data/ISA

NOAA8860—WCCIS: Provides OneNWSNet connection to NDBC/None

NOAA8865—NTWC: Access to raw tsunami data/ISA

d) The purpose that the system is designed to serve

NDBC's systems of record provide critical data on oceanic and atmospheric conditions used by weather and hurricane forecasters, researchers, climatologists, oceanographers, commercial fishers, and recreational boaters, among others. Surveys of meteorologists have shown about 40 percent of NWS marine warnings and advisories are based, at least in part, on NDBC's meteorological data. In addition to this critical purpose, the observations are used by meteorologists who need to adjust flight level wind speeds reported by hurricane reconnaissance aircraft to surface winds; by geophysicists who use our sea surface temperature, wind, and wave reports to help calibrate remotely sensed measurements from spacecraft; and by engineers who obtain directional wave measurements to study beach erosion and shore protection. Additionally, surfers, fishermen, and boaters acquire the reports via the Internet to help them determine if they want to venture offshore.

e) The way the system operates to achieve the purpose

The NDBC manages the development, operations, and maintenance of the national data buoy network. It

serves as the NOAA focal point for data buoy and associated meteorological and environmental monitoring technology. It provides high quality meteorological/environmental data in real time from automated observing systems that include buoys and a Coastal-Marine Automated Network (C-MAN) in the open ocean and coastal zone surrounding the United States. It provides engineering support, including applications development, and manages data buoy deployment and operations, and installation and operation of automated observing systems installed on fixed platforms. In 2001 and 2005 respectively, NDBC began to assume responsibility for operating moored buoys supporting NOAA's Deep-Ocean Assessment and Reporting of Tsunami (DART) program and the Tropical Atmosphere Ocean (TAO) program that were developed and formerly operated by NOAA's Pacific Marine Environmental Laboratory (PMEL). NDBC currently operates and maintains 101 moored buoys and 46 C-MAN stations.

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

Identifying Numbers:

- Federal employees can only view their personnel actions when on site (remote access is not allowed) via the Electronic Official Personnel Folder (e-OPF) which does contain SSNs on selected records.
- DoD ID Numbers from employee (federal and contractor) Common Access Cards (CAC) are collected in support of two-factor authentication required by HSPD-12.
- Passports (including SSNs) of Foreign National visitors are collected via fax and transmitted electronically via Kiteworks to the NOAA security office and in person to the NASA security office. The individual user (HR Liaison role) within the Resources Branch (OBS23) has been provided an encrypted drive (non-portable) for storage of PII/BII in addition to NOAA's Google Suite (maintained per NOAA CIO requirements).

General Personal Data:

- Name, home address, and telephone numbers are collected from NDBC employees (federal and contractor) in support of Continuity of Operations (COOP) activities.
- When contacting the NDBC webmaster, customers' (i.e., general public, government, private sector, educational institutions), email addresses are used in order to provide a response to questions and service requests. Further, the customers voluntarily provide contact information to include their name and phone numbers based on the type of response expected.

Work-Related Data:

- Occupation, job title, work address, telephone number, and email addresses are maintained on NDBC employees (federal and contractor) for administrative purposes.
- Electronic personnel-related forms (which include SSNs) of NDBC employees (federal) are transferred to NOAA HR in bulk or on a case-by-case basis via Kiteworks or via tracked Federal Express (FedEx) package. The individual user (HR Liaison role) within the Resources Branch (OBS23) has been provided an encrypted drive (non-portable) for storage of PII/BII in addition to NOAA's Google Suite (maintained per NOAA CIO requirements).
- Performance plans of NDBC employees (federal) are maintained for administrative purposes.
- Proprietary information related to federal acquisition actions are maintained for administrative purposes.

Distinguishing Features/Biometrics:

- NDBC management utilizes photographs of NDBC employees (federal and contractor) to populate an organizational chart that is shared strictly within NDBC. Further, photographs are taken during NDBC buoy deployments and maintained on the shared drives. NDBC personnel (federal and contractor) give written permission for use of photos via the DOC Photo Release Form maintained by the HR liaison.
- NDBC outfits data collection platforms (i.e., buoys, CMAN stations) with cameras that collect visual environmental data. The photographs are made available to the public via the NDBC website as a data point. Further, station camera images are kept in accordance with the federal records retention schedule.

System Administration/Audit Data:

- User IDs of NDBC employees (federal and contractor) are administered and maintained via a local implementation of Active Directory.
- Login success/failure is monitored on NOAA8873 for IT security purposes (ArcSight).
- Date/Time of access is monitored on NOAA8873 for IT security purposes (ArcSight).
- ID files accessed are monitored on NOAA8873 for IT security purposes (ArcSight).
- Contents of files are monitored on NOAA8873 for IT security purposes (ArcSight).

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

Forecasters/Researchers/Climatologists/Oceanographers
Commercial fishers/Recreational/General Public
NDBC Director
AGO Representative
NDBC Mission Control Center
NDBC IT Techs/SW Developers
NDBC Field Operations
NDBC Production Engineering
NDBC Technology Development
NDBC Mission Support Engineering
NDBC Logistics & Facilities
NDBC Business Services

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

NDBC and NDBC Technical Services Contract (NTSC) personnel have network access via GFE devices

to the information in the system.

NOAA forecasters and the like have access to the information in the system via the NOAA Global Telecommunications System (GTS).

Members of the public have access to the information in the system via the public website at ndbc.noaa.gov.

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

Data is transmitted to the information system using contracted satellite communications servers to transmit/receive data from the stations (Coastal WxBuoy, C-MAN, DART, TAO).
NDBC partner data is also ingested via file transfer protocol (FTP) and application programming interface (API). **POA&M 105542 is to secure FTP at NDBC.**

Information is transmitted from the system in various ways. The public can consume data via the NDBC website (ndbc.noaa.gov). The weather community can access data via the Global Telecommunications System (GTS). NDBC and NTSC personnel have access (according to role) to the NDBC network via GFE devices. Interconnected systems may also have remote access to the NDBC network via SSL or API (Least Privilege—access only for intent of the interconnection).

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.

X Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	X
Video surveillance	X	Electronic purchase transactions	
Other (specify): Video surveillance is conducted on buoys equipped with buoycams to collect visual environmental data. Video surveillance is also conducted at the entry and inside the NOAA8873 data center for IT Security purposes.			

___ 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.)."

X 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."

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
_X_ 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?

_X_ 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.
Electronic personnel-related forms (which includes SSNs) of NDBC employees (federal) are transferred to NOAA HR in bulk or on a case-by-case basis via Kiteworks or via tracked Federal Express (FedEx) package. The individual user (HR Liaison role) within the Resources Branch (OBS23) has been provided an encrypted drive (non-portable) for storage of PII/BII in addition to NOAA's Google Suite (maintained per NOAA CIO requirements).

Provide the legal authority which permits the collection of SSNs, including truncated form.
• 5 USC 2101 to 10210 (Government Organizations and Employees, Part III, Employees) • COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies • DEPT-13, Investigative and Security Records • OPM/GOVT-1, General Personnel Records

____ 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 Data Buoy Center (NOAA8873) 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 Data Buoy Center (NOAA8873) 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):

Joy Callaway (ISSO)

Signature of ISSO or SO: CALLAWAY.JOY.ALLISON.1269758577 Digitally signed by CALLAWAY.JOY.ALLISON.1269758577 Date: 2020.05.26 14:03:08 -05'00' Date: _____

Name of Information Technology Security Officer (ITSO): Andrew Browne

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2020.05.26 15:50:40 -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: 2020.07.15 14:20:24 -04'00' Date: _____

Name of Authorizing Official (AO): Thomas Cuff

Signature of AO: CUFF.THOMAS.JAMES.1071092450 Digitally signed by CUFF.THOMAS.JAMES.1071092450 Date: 2020.07.13 21:24:30 -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: 2020.08.04 08:39:46 -04'00' Date: _____