Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
NOAA8873

National Data Buoy Center (NDBC)

Template Version Number: 01-2021

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NWS/OBS/NDBC

Unique Project Identifier: NOAA8873

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).

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.

Address the following elements:

a) Whether it is a general support system, major application, or other type of system

General Support System (GSS)

b) System location

NDBC Data Center at Stennis Space Center, Mississippi
NOAA Enterprise Data Center at Ashburn, Virginia
Amazon Web Services (AWS) GovCloud East at Virginia (AZ1) and Ohio (AZ6)

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): Alternate Processing Site utilizing IaaS within the FedRAMP GovCloud/SLA (NOAA BPA).

Department of Homeland Security (DHS) US Coast Guard (USCG): Nationwide Automatic Information System (NAIS) for tracking adrift buoys/SLA

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

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

NOAA0100—NOAA Cyber Security Center: enterprise IT security tools/Memorandum

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

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

NOAA0520—NOAA Enterprise Data Center-Ashburn/SLA

NOAA0550—NOAA Enterprise Network (NWAVE)/SLA

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.
See the NOAA8873 PIA Section 4.1.

e) The way the system operates to achieve the purpose

The system operates in a hybrid model which employs traditional client servers, virtual servers/hosts, and Infrastructure as a Service (IaaS) with the cloud service provider, Amazon Web Services (AWS). Data is hosted on servers and made available via various protocols such as HTTPS, FTP, SFTP, API, and SSH.

NOAA8873 groups elements of the system into the following areas, each of which serves a distinct and specific function:

- Network Devices – Wide Area Network (WAN), Local Area Network (LAN), Wireless Network (Wifi), and Virtual Private Network (VPN).
- Data Collection and Processing – Virtual servers/hosts and the AWS cloud environment provides data collection mechanisms from the buoys, automated quality control of the data, and distribution of the data to the NWS Global Telecommunication System (GTS).
- Application Servers -- The Windows and RHEL server components provide services and applications such as file shares, printing, database hosting, and CADD.
- Web Application Servers – Web site and web application hosting services.

NOAA8873 operates with network infrastructure, virtual server infrastructure, physical servers, workstations, and various area networks, and printers/faxes to support staff in meeting the mission. The NOAA8873 system has internal and external web servers. The internal servers are used for business processes such as the IT help desk, training, tracking budgets, development, etc. The external web sites display data from our primary mission (buoys) which is also released to the GTS for incorporation into weather forecast models. NDBC has official social media sites (Facebook, Twitter, LinkedIn) which are used to connect with different audiences like Federal, State, and university partners as well as the public.

f) A general description of the type of information collected, maintained, used, 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 within NDBC. Further, photographs are taken during NDBC buoy deployments and maintained on the shared drives. Finally, photographs containing employees may be used in social media postings to the public from the official NDBC platforms/accounts. 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	
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	

See the NOAA8873 PIA Sections 6.4 and 8.2.

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 111574 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 Telecommunication 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. 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.*

X__ 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	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): Official NDBC social media platforms may utilize photographs containing employees (federal and contractor) in social media postings if there is a DOC Photo Release Form on file.					

____ 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.

X__ 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 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 which is used to protect against vandalism and can be used for law enforcement purposes in the event of buoy vandalism.

Video surveillance is also conducted at the entry and inside the NOAA8873 data center for IT Security purposes.

Official NDBC social media platforms may utilize photographs containing employees (federal and contractor) in social media postings if there is a DOC Photo Release Form on file.

____ 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
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?

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 NOAA employees only are transferred to NOAA HR in bulk or on a case-by-case basis via DOC Kiteworks (for NOAA records only) or via tracked Federal Express (FedEx) package. Foreign nationals (FNs) requesting access to NDBC provide passports (including SSNs) in support of the NOAA FN clearance process (application). The passports are transmitted via Kiteworks by the NDBC HR liaison. NASA also requires clearance of FNs since NDBC is a tenant on a NASA installation. FN passport information is delivered in person by the NDBC HR liaison in support of this process.
Provide the legal authority which permits the collection of SSNs, including truncated form.
EO 10450 – Security Requirements for Government Employment EO 9397 – Numbering System for Federal Accounts Relating to Individual Persons (as amended by 13478, 9830, and 12107) DAO 207-12 – Foreign Visitor and Guest Access Program 8 U.S.C Chapter 12 – Immigration and Nationality 15 U.S.C 1501 et seq. – Department of Commerce

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

CERTIFICATION

X The criteria implied by one or more of the questions above **apply** to the National Data Buoy Center (NDBC) 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 National Data Buoy Center (NDBC) 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: Joy Callaway Office: NOAA/NWS/OBS/NDBC Phone: 228-688-2801 Email: joy.callaway@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: CALLAWAY.JOY.ALLISON.12697 Digitally signed by CALLAWAY.JOY.ALLISON.1269758577 Date: 2022.03.09 10:34:29 -06'00' Date signed: 58577	**Information Technology Security Officer** Name: Andrew Browne Office: NOAA/NWS/OACIO Phone: 301-427-9033 Email: Andrew.browne@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: BROWNE.ANDREW.PATRICK.14721493 Digitally signed by BROWNE.ANDREW.PATRICK.14721493149349 Date: 2022.03.08 17:02:28 -05'00' Date signed: 49
Privacy Act Officer Name: Adrienne Thomas Office: NOAA OCIO Phone: 828-257-3148 Email: Adrienne.thomas@noaa.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2022.03.22 12:22:20 -05'00' Date signed: 600	**Authorizing Official** Name: Michelle Mainelli Office: NOAA/NWS/OBS Phone: 301-427-9760 Email: michelle.m.mainelli@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: MAINELLI MCINERNEY.MICHELLE.1365819722 Digitally signed by MAINELLI MCINERNEY.MICHELLE.1365819722 Date: 2022.03.18 16:26:14 -04'00' Date signed:
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2022.03.28 10:42:47 -04'00' Date signed:	

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PTA.