

**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: 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 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:

1. Enable an informed society anticipating and responding to climate and its impacts;
2. Prepare for and respond to weather-related events;
3. Sustain marine fisheries, habitats, and biodiversity within healthy and productive ecosystems;
4. 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:

1. 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.
2. Coastal-Marine Automated Network (C-MAN): A network of land based nearshore observation stations.
3. Deep-ocean Assessment and Reporting of Tsunamis (DART): A network of moored buoys, primarily located along the Pacific Ocean and Hawaiian islands, which provide tsunami data to the National Tsunami Warning Center for assessment and warning.
4. Tropical Atmosphere Ocean (TAO): A network of moored buoys, primarily located within the equatorial Pacific, which provide oceanographic data to the NOAA scientific community.

These 4 systems provide critical data on oceanic and atmospheric conditions used by weather and hurricane forecasters, researchers, climatologists, oceanographers, commercial fishers, and recreational boaters, among others.

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. It supports the Volunteer Observing Ship (VOS) program to acquire additional meteorological and oceanographic observations supporting NWS mission requirements. It operates the NWS test center for all surface sensor systems. It maintains the capability to support operational and research programs of NOAA and other national and international organizations.

NDBC is located at the Stennis Space Center in Bay St. Louis, Mississippi, and has operated a network of off-shore weather buoys and unmanned coastal observing stations (Coastal Marine Automated Network or C-MAN stations) since 1990. 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. Under a 1993 memorandum of understanding, the U.S. Coast Guard provides ship transit services for NDBC so that it can repair and maintain its weather buoys. The Coast Guard also maintains a small staff at NDBC. NOAA vessels provide support for the NDBC mission when their schedules allow. NDBC also leases privately-owned vessels when required to support the mission and maintenance schedules.

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.

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): <i>Images collected from buoys outfitted with cameras</i>					

- ☐ 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 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. *Please describe the activities which may raise privacy concerns.*

- 1) Access to the information technology (IT) areas is physically controlled via room entry readers.
- 2) Select buoys are outfitted with cameras to collect visual environmental data and images collected are stored on the information system.

☐ 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

☐ 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..."

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

☒ DOC employees

☒ Contractors working on behalf of DOC

☒ 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?

☒ 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.

☒ 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 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 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 Baker, ISSO

Signature of ISSO or SO: BAKER.JOY.ALLISON.1269 758577 Digitally signed by
BAKER.JOY.ALLISON.1269758577
Date: 2019.04.17 16:17:46 -05'00' Date:

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

Signature of ITSO: BROWNE.ANDREW.PATRICK.147 2149349 Digitally signed by
BROWNE.ANDREW.PATRICK.1472149349
Date: 2019.04.23 11:26:40 -04'00' Date:

Name of Authorizing Official (AO): Thomas Cuff, AO

Signature of AO:  Date: 5/15/19

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

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: 2019.10.10 09:48:21 -04'00' Date: