

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



Privacy Impact Assessment
for the
NOAA8873
National Data Buoy Center (NDBC)

Reviewed by: Mark Graff Bureau Chief Privacy Officer

- ☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment

NOAA/NWS/OBS/NDBC

Unique Project Identifier: NOAA8873 (NDBC)

Introduction: System Description

Provide a brief description of the information system.

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 five (5) 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 real-time.
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 tsunameter data to the National Tsunami Warning Center (NTWC) 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.
5. Volunteer Observing Ship (VOS): A collection and transmission of real-time marine surface weather observations from research and commercial vessels. VOS ingests weather observations and there is no personally identifiable information/business identifiable information (PII/BII) PII/BII collected.

These five (5) 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.

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;
AWS East at Virginia (Availability Zone (AZ) 1);
AWS East at Ohio (AZ4).

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

AWS: Alternate Processing Site utilizing Infrastructure as a Service (IaaS)/Service Level Agreement (SLA) via the NOAA Blanket Purchase Agreement (BPA).

US Air Force Space Command Iridium: Satellite communications to transmit/receive data from stations/Inter-agency Agreements (IAA).

Geostationary Operational Environmental Satellite (GOES): NOAA/National Environmental Satellite, Data, and Information Service (NESDIS): Satellite communications to transmit/receive data from stations/Interconnection Security Agreement (ISA).

High Frequency (HF) Radar: University of California: NDBC hosts website to deliver radar data/ISA.

Git Iridium: Satellite communications to transmit/receive data from stations/Contract.

NOAA0100: NOAA Cyber Security Center: enterprise security tools/Memorandum.

NOAA0201: NOAA Web Operations Center (WOC): Hosts NDBC's websites/Service Level Agreement (SLA).

NOAA3100: Pacific Marine Environmental Laboratory (PMEL): NDBC hosts the Observing System Monitoring Center (OSMC) database and website to deliver weather data/ISA.

NOAA0550: NOAA Enterprise Network (NWAVE)/SLA.

NOAA8860: Weather Climate and Computing Infrastructure Services (WCCIS): Provides internet connection to NDBC/None.

NOAA8865: NTWC: Access to raw tsunami data/ISA.

(d) *The way the system operates to achieve the purpose(s) identified in Section 4*

The system operates in a hybrid model which employs traditional client servers, virtual servers/hosts, and IaaS with the cloud service provider, AWS. Data is hosted on servers and made available via various protocols such as hypertext transfer protocol secure (HTTPS), file

transfer protocol (FTP), secure FTP (SFTP), application programming interface (API), and secure shell (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 Linux server components provide services and applications such as file shares, printing, database hosting, and computer aided design and drafting (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 information technology (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, X, LinkedIn) which are used to connect with different audiences like Federal, State, and university partners as well as the public.

(e) How information in the system is retrieved by the user

NDBC and NDBC Technical Services Contract (NTSC) personnel have network access via government furnished equipment (GFE) devices to the information in the system.

NOAA forecasters and the like have access to the information in the system via the NOAA GTS.

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

(f) 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 (CWB, C-MAN, DART, TAO).

NDBC partner data is ingested via FTP, SFTP, and API.

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 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 secure

socket layer (SSL) or API (Least Privilege—access only for intent of the interconnection).

(g) Any information sharing

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 social security numbers (SSNs) on selected records.
- Department of Defense (DoD) identification (ID) Numbers from employee (federal and contractor) Common Access Cards (CAC) are collected in support of two-factor authentication (2FA) required by Homeland Security Presidential Directive 12 (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 National Aeronautics and Space Administration (NASA) security office. The individual user (Human Resources (HR) Liaison role) within the Resources Branch (OBS23) has been provided an encrypted drive (non-portable) for storage of personally identifiable information/business identifiable information (PII/BII) in addition to NOAA's Google Suite (maintained per NOAA Chief Information Officer (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 via upload to the appropriate system such as HR Connect or Enterprise Services or on a case-by-case basis via Kiteworks or NOAA email. 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, C-MAN 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).

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

See attached Table at the end of the PIA.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

Moderate

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.

_____ This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

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.

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.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (Check all that apply.)

Identifying Numbers (IN)					
a. Social Security*	X	f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport	X	k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: 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. 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). In addition, all SSNs are purged from the system within 30 days.					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	
d. Sex		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address	X	s. Marital Status	X
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary		j. Proprietary or Business Information	X
c. Work Address	X	g. Work History		k. Procurement/contracting records	X
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	X
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording	X	i. Height		n. Retina/Iris Scans	
e. Photographs	X	j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					
* Video recording is in reference to the video surveillance conducted on buoys.					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run		f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains

In Person	X	Hard Copy: Mail/Fax	X	Online	
Telephone		Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign (<i>Visitors</i>)	X		
Other (specify):					
Foreign Nationals are typically visitors attending buoy workshops or conferences. Foreign nationals accessing NDBC must provide passports (including SSNs) as part of the NOAA foreign national clearance process.					

Non-government Sources					
Public Organizations		Private Sector (Lynker**)	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					
**Lynker is the technical services contractor at NDBC. Lynker is the new vendor for the NDBC technical services, but introduced no change to the system, PII/BII, or personnel.					

2.3 Describe how the accuracy of the information in the system is ensured.

Information received by the system is verified by the respective federal point of contact (POC) with responsibility for processing and protecting the data collected.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB 3206-0182
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. (*Check all that apply.*)

Technologies Used Containing PII/BII Not Previously Deployed (TUCBPNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
---	--

Section 3: System Supported Activities

- 3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(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.			
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.			
There are not any IT system supported activities which raise privacy risks/concerns.			

Section 4: Purpose of the System

- 4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	X
For civil enforcement activities		For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	X
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The information collected and maintained by NOAA8873 is used for administrative purposes such as performance evaluations, logging into the information system, official social media
--

posts, and contact during COOP activities. This information is that of federal employees and contractors.

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. This information is not shared with anyone beyond those that are required to process it within the respective bureau. 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).

Employees' own personnel records (i.e., Standard Form (SF)-50, Performance Evaluations, etc) may be accessed via the e-OPF site.

Customers voluntarily provide contact information when submitting web inquiries via webmaster and in doing so consent to contact from NDBC webmaster to answer their inquiries. Customers may be general public, government, or private sector, including educational institutions.

Foreign nationals (FNs) requesting access to NDBC provide passports (including SSNs) in support of the NOAA foreign national clearance process (application). The passports are transmitted via Kiteworks by the NDBC HR liaison. NASA also requires clearance of foreign nationals since NDBC is a tenant on a NASA installation. Foreign national passport information is delivered in person by the NDBC HR liaison in support of this process. 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).

NDBC outfits data collection platforms (i.e., buoys, C-MAN stations) with cameras that collect visual environmental data. These images are published online to the public and are sometimes used for law enforcement activities if vandalism to the station is detected.

- 5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Insider threat risks are managed by the system in the following ways: NDBC personnel are required to complete the NOAA IT Security and Privacy Awareness Training annually. This training covers proper handling of privacy information. In addition, the Mission Control/IT Branch (OBS24) has a Records Retention POC (federal employee) trained by National Archives and Records Administration (NARA) on records retention policies and purges the information in accordance with the retention schedules.

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X	X	
DOC bureaus			
Federal agencies	X (NASA Security Office)		
State, local, tribal gov't agencies	X		
Public	X		
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.
--	---

- 6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

X	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

- 6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: AWS: Alternate processing site utilizing IaaS/SLA via the NOAA BPA. BII: IT audit logs and internet protocol (IP) addresses. PII: User CAC info (via NOAA Single-Sign On (SSO)). NWAVE Virtual Routing and Forwarding (VRF), 2FA. US Air Force Space Command Iridium: Satellite communications to transmit/receive data from stations/IAA. No PII and/or BII. IP Tables, SSH, transport layer security (TLS).
---	---

	GOES—NOAA/NESDIS: Satellite communications to transmit/receive data from stations/ISA. No PII and/or BII. IP Tables, SSH, TLS. HF Radar—University of California: NDBC hosts website to deliver radar data/ISA. No PII and/or BII. SSH, TLS. Git Satellite, LLC: Iridium communications to transmit/receive data from stations/Contract. No PII and/or BII. IP Tables, SSH, TLS. NOAA0100—NOAA Cyber Security Center: Enterprise security tools/Memorandum. BII: IT audit logs, IP addresses, and system vulnerability information. PII: User ID and CAC info. SSH, TLS, 2FA NOAA0201—NOAA WOC: Hosts NDBC's main website/SLA. PII: Public users' info if requesting contact from NDBC via webmaster. SSH, TLS, 2FA. NOAA3100—PMEL: NDBC hosts OSMC database and website to deliver weather data/ISA. PII: User ID (limited to one (1) OSMC personnel). SSH, TLS. NOAA0550—NOAA Enterprise Network (NWAVE)/SLA. BII: IT audit logs and IP addresses. PII: User ID and CAC info (limited to NDBC IT admins). NWAVE VRF, SSH, TLS, 2FA. NOAA8860—WCCIS: Provides internet connection to NDBC/None. BII: IP addresses. NWAVE VRF, SSH, TLS. NOAA8865—NTWC: Access to raw tsunami data/ISA. PII: CAC info (via NOAA SSO). SSH, TLS, 2FA.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. (*Check all that apply.*)

Class of Users			
General Public	X*	Government Employees	X
Contractors	X		
Other (specify):			
*The general public has very limited access to the system, which is limited to public, non-PII/BII buoy data and official social media posts.			

Section 7: Notice and Consent

- 7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.ndbc.noaa.gov/contact_us.shtml
X	Yes, notice is provided by other means. Specify how: Identifying Numbers: Written notice is included on all personnel forms that employees (federal) complete. NDBC employees (federal and contractor) are notified in person by the NDBC Information System Security Officer (ISSO) when giving their DoD ID numbers. Notice is provided verbally to a foreign national by the US sponsor or the DOC staff at DOC International Affairs Office, at the time of the foreign national's appearance at the office, that completion of the information on the Foreign National Visitor and Guest Access request form is required for obtaining authorization for a visit. General Personal Data: Notice is provided to customers initiating web inquiries via webmaster by a privacy statement on the web site. For NDBC COOP activities, employees are asked permission in person by their supervisors when collecting the applicable information. Work-Related Data: Written notice is included on all personnel forms that employees complete. For DOC performance/award documents, employees are informed by their supervisors in person or via email that the evaluations are in process.

		Employees have access to view the official documents. Distinguishing Features/Biometrics: NDBC employees (federal and contractor) give written consent for use of photographs via the DOC Photo Release Form maintained by the HR liaison. There is no expectation to privacy for cameras collecting environmental data positioned on data collection platforms (buoys, C-MAN stations). System Administration/Audit Data: NIST SP 800-53A Rev 5 requires information systems to collect audit data in support of IT security activities. NDBC employees (federal and contractor) are given notice via the NOAA IT Security Awareness Training.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Identifying Numbers: Foreign nationals are given the opportunity to decline to provide information during the clearance process with NOAA. If foreign nationals decline to provide the information (by not providing it), then access to NOAA sites (including NDBC) are denied. HSPD-12 requires personnel log into the information system using 2FA. If an employee declines to provide, no network access is provided. General Personal Data: For COOP activities, NDBC personnel can inform their supervisor in person or in writing that they decline to provide PII/BII. Customers voluntarily provide information when submitting web inquiries via webmaster, so that they may be contacted. Work-Related Data: Performance/position information is part of the official personnel record
---	---	---

		for DOC employees, with notice given on the forms completed as part of the hiring process. Individuals may have chosen not to provide information, by not completing the forms, but this would affect their employment status. . Distinguishing Features/Biometrics: NDBC employees (federal and contractor) give written consent for use of photographs via the DOC Photo Release Form maintained by the HR liaison. If personnel decline participation, no DOC Photo Release Form is filed with the HR liaison. There is no expectation to privacy for cameras collecting environmental data positioned on data collection platforms (buoys, C-MAN stations). System Administration/Audit Data: NIST SP 800-53A Rev 5 requires information systems to collect audit data in support of IT security. Users may decline, but it will impact their access to the system which could impact employment.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Identifying Numbers: Foreign nationals are given the opportunity via the NOAA forms to consent to the use of their information in support of the clearance process during the application process with NOAA. Personnel may choose not to log in to the information system, but HSPD-12 requires personnel to log in using 2FA. This is the only use for this information. Work-Related Data: Performance/position information is part of the official personnel record for DOC employees. Employees may choose not to consent to a particular use, in writing, to their supervisors, but this may affect their employment status.
---	--	--

		General Personal Data: For COOP activities, there is only one use. Customers voluntarily provide information when submitting web inquiries via webmaster and in doing so consent to contact from NDBC webmaster to answer his/her inquiry. This is the only use of the information. Distinguishing Features/Biometrics: NDBC employees (federal and contractor) give written consent for use of photographs via the DOC Photo Release Form maintained by the HR liaison. Cameras collecting environmental data positioned on data collection platforms (buoys, C-MAN stations) is not voluntary and is meant to be a law enforcement deterrent to prevent vandalism. Individuals may avoid this collection by not approaching or interfering with remotely moored and stationed buoys. System Administration/Audit Data: NIST SP 800-53A Rev 5 requires information systems to collect audit data in support of IT security. Users may decline, but it will impact their access to the system which could impact employment.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Identifying Numbers: Foreign nationals are given the opportunity to update their information during a subsequent clearance process with NOAA where the foreign national completes a new application. General Personal Data: For COOP activities, NDBC personnel are asked via email from either the NDBC HR liaison or the NDBC ISSO to review/update PII/BII annually in person. Customers voluntarily provide email address and contact information at their discretion when
---	---	---

		contacting the NDBC Webmaster, but the data is not reviewed or updated. Distinguishing Features/Biometrics: NDBC employees (federal and contractor) give written consent for use of photographs via the DOC Photo Release Form maintained by the HR liaison. There is no expectation to privacy for cameras collecting environmental data positioned on data collection platforms (buoys, C-MAN stations). Work-Related Data: Performance/position information is part of the official personnel record for DOC employees and will be updated upon official personnel actions.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. (*Check all that apply.*)

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Windows file system auditing monitors, tracks, and records changes to the files containing PII/BII and a report is sent to the NDBC ISSO daily.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): <u>01/31/2025</u> ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish DOC ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
X	Other (specify):

	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).
--	---

- 8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.
(Include data encryption in transit and/or at rest, if applicable).

All NDBC employees and contractors undergo a national agency check with inquiries (NACI) security check when employed or contracted. This involves a check of Federal and local law enforcement records to help ensure the trustworthiness of the employee.

The user electronically signs the Rules of Behavior (ROB) via the NOAA IT Security Awareness training indicating that they have read and understand the ROB. The ROB outlines privacy and the PII definition, storage, sharing, and reporting of PII incidents.

To protect data contained on mobile devices, all NDBC laptops are fully encrypted using the NOAA enterprise supplied encryption software. In addition, all NDBC government issued phones are protected via mobility as a service (MaaS) 360 via NOAA's Unified Messaging Services (UMS).

NDBC employees are required to utilize DOC Kiteworks for the transmission of any sensitive data.

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's requirements).

Section 9: Privacy Act

- 9.1 Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?

 X Yes, the PII/BII is searchable by a personal identifier.

 No, the PII/BII is not searchable by a personal identifier.

- 9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (A new system of records notice (SORN) is required if the system is not covered by an existing SORN).

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i> OPM/GOVT-1, General Personnel Records OPM/GOVT-2, Employee Performance File System Records COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies COMMERCE/DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs COMMERCE/DEPT-25, Access Control and Identity Management System COMMERCE/DEPT-6, Visitor Logs and Permits for Facilities under Department Control COMMERCE/DEPT-13, Investigative and Security Records NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission COMMERCE/DEPT-20, Biographical Files and Social Networks COMMERCE/DEPT-27, Investigation and Threat Management Records GSA/GOVT-9, System for Award Management (SAM)
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NARA, GRS 3.1-General Technology Management Records NARA, GRS 3.2-Information Systems Security Records NARA, GRS 6.3-Information Technology Records
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X

Other (specify):

Destruction of hard drives

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

X	Identifiability	Provide explanation: Customers voluntarily provide only as much information as they feel necessary when submitting web inquiries via NDBC webmaster. All other PII is that of an employee or foreign national and requires consent for collection.
X	Quantity of PII	Provide explanation: NDBC employees (federal and contractor) total less than 200 and minimal PII is collected/maintained.
X	Data Field Sensitivity	Provide explanation: Limited sensitive PII is collected from a foreign national.
X	Context of Use	Provide explanation: Information is for official use only and disclosed upon consent.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Security and privacy controls for protecting PII/BII are in place and functioning for NOAA8873 in accordance with NIST SP 800-53A Revision 5.

	Other:	Provide explanation:
--	--------	----------------------

Section 12: Analysis

- 12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

NDBC chooses to minimize the amount of PII/BII collected due to the lack of a comprehensive information system encryption method. While NDBC administrators have established encrypted drives and folders for individual users, the classification of the majority of NDBC data does not warrant encryption of the entire information system.

- 12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

- 12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Type of Information Collected	Applicable SORNS	Programmatic Authorities
Personnel Actions Including Training	OPM/GOVT-1	5 U.S.C. 1302, 2951, 3301, 3372, 4118, 5379, 8347
	COMMERCE/DEPT-18	Executive Orders 9397, as amended by 13478, 9830, and 12107; 13164; 12564; and 11246
		44 U.S.C. 3101
		41 U.S.C. 433(d)
		5 CFR Part 537
		Public Law 100-71
		26 U.S.C. 3402
Employee Performance Info	OPM/GOVT-2	Executive Order 12107
		5 U.S.C. Sections 1104, 3321, 4305, and 5405
Emergency Preparedness/COOP	COMMERCE/DEPT-18	Executive Order 12656
		Federal Preparedness Circular (FPC) 65, July 26, 1999
Security Investigations (Security Clearance actions)	COMMERCE/DEPT-13	Executive Orders 10450, 11478
		5 U.S.C. 7531-332
		28 U.S.C. 533-535
		Equal Employment Act of 1972
Badging & CAC Issuance	COMMERCE/DEPT-18	Electronic Signatures in Global and National Commerce Act, Public Law 106-229
		5 U.S.C. 301
Biographical Info / Social Networks	COMMERCE/DEPT-20	5 U.S.C. 301
		15 U.S.C. § 1516
		E.O. 11625
		Presidential Memorandum to the Heads of Executive Departments and Agencies on Transparency and Open Government, January 21, 2009
		OMB Open Government Directive, M-10-06, December 8, 2009
		OMB Guidance for Online Use of Web Measurement and Customization Technologies, M-10-22, June 25, 2010

System Administration/Audit Data (SAAD)	COMMERCE/DEPT-25	5 USC 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
		Electronic Signatures in Global and National Commerce Act, Public Law 106-229
		28 U.S.C. 533-535
Building Entry/Access	COMMERCE/DEPT-25	5 USC 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
Foreign National Information	COMMERCE/DEPT-27	28 U.S.C. 533-535
		44 U.S.C. 3101
		5 U.S.C. 301
		Executive Orders 13526, 12968, 13356, 13587
		Public Law 108-458 (Intelligence Reform and Terrorism Prevention Act of 2004)
		Intelligence Authorization Act for FY 2010, Public Law 111-259
		31 U.S.C. 951-953
		8 U.S.C. 1324a
		15 Code of Federal Regulations (CFR) Parts 730-774, Export Administration Regulations
		NOAA Administrative Order (NAO) 207-12 "Technology Controls and Foreign National Access"
		Department Administrative Order (DAO) 207-12 Version Number: 01-2017 "Foreign National Visitor and Guest Access Program
Visitor Logs & Permits for Facilities	COMMERCE/DEPT-6	5 U.S.C. 301
		44 U.S.C. 3101
Contact Information for the Public	NOAA-11	5 U.S.C. 301, Departmental Regulations
		15 U.S.C. 1512, Powers and duties of Department
Info Collected Electronically in	COMMERCE/DEPT-23	15 U.S.C. § 272

Connection w/ DOC Activities, Events & Programs		
		15 U.S.C. § 1151
		15 U.S.C. § 1512
		15 U.S.C. § 1516
		15 U.S.C. § 3704b
		47 U.S.C. § 902
		E.O. 11625
Procurement/Contracting	GSA/GOVT-9	FAR Subparts 4.11, 52.204
		2 CFR Subtitle A
		40 U.S.C. 121(c)
		FAR Subparts 9.4 and 28.2
		Executive Orders 12549, 12689