Version Number: 01-2015

U.S. Department of Commerce
NOAA

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

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2017.12.14 15:53:55 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/NDBC

Unique Project Identifier: NOAA8873

Introduction: System Description

(a) General Description

The National Data Buoy Center (NDBC), a part of the National Oceanic and Atmospheric Administration (NOAA), National Weather Service (NWS), provides comprehensive, reliable systems and marine observations to support the missions of the NWS and NOAA, promote public safety, and satisfy the future needs of our customers. NDBC operates three major buoy arrays as well as a network of coastal marine observing stations. These systems provide critical data on oceanic and atmospheric conditions that is 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 coastal zone surrounding the United States and the open ocean. 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 hosts the Volunteer Observing Ship (VOS) program to acquire additional meteorological and oceanographic observations supporting NWS mission requirements. The VOS is managed by federal employees within the NWS called PMOs (Port Meteorological Officers); their job is to recruit ships to take/report weather observations in the open seas. The NDBC program tracks only metadata on the observations and the ships, no information on the general public. The ships are typically commercial/cruise ships.

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 195 moored buoys and 46 C-MAN stations. 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.

Identifying Numbers:

- Passports of Foreign National visitors are collected via fax and transmitted electronically via Accellion 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 this and other PII/BII.

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, and 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 of NDBC employees (federal) are transferred to NOAA HR in bulk or on a case-by-case basis via Accellion 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.
- 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 (we are now using this form with the PAS added).

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).

c) Information Sharing

Personnel and Foreign National (FN) information is shared/transferred to NOAA Human Resource (HR) and Security offices via Accellion. Foreign national information is delivered to NASA Security in person via the HR liaison. 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 case of a security or privacy breach, information will be shared with the Department of Commerce and possibly the Department of Justice.

d) Legal Authority to Collect PII/BII

Statutory or regulatory authorities for collection and maintenance of the information include:

- 15 USC 1151(Dissemination of Technological, Scientific, and Engineering Information)
- 15 USC 1512 (Powers and Duties of the Department of Commerce)
- 5 USC 2101 to 10210 (Government Organizations and Employees, Part III, Employees)
- 5 USC 301 (Departmental Regulations)
- DAO 207-12 Foreign Visitor and Guest Access Program
- Authorities from DEPT-6: 5 U.S.C. 301; 44 U.S.C. 3101.
- Authorities from DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal

Employment Act of 1972.

- Authorities from DEPT-18: Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.
- Authorities from DEPT-25: 5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075.
- Authorities from NOAA-11: 5 U.S.C. 301, Departmental Regulations and 15 U.S.C. 1512, Powers and duties of Department.
- Authorities from OPM/GOVT-1: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

e) FIPS 199 Security Impact

The NOAA8873 information system is categorized as a Moderate system.

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):					

____X_ This is an existing information system in which changes do not create new privacy risks.

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*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	

d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Performance Plans					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs	X	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

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		Online	
Telephone		Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign *(Visitors)*	X		
Other (specify					

Non-government Sources					
Public Organizations		Private Sector (PAE)**	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): ***Pacific Architects and Engineers (PAE) is the technical services contractor at NDBC. They provide contact information for COOP.*					

2.3 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 (TUCPBNPD)			
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):			

* This issue was addressed in the last PIA. This is the video surveillance of the data center. There are no discs. The video is placed on a network drive and files are automatically deleted once they are past 30 days. This is for correlation of physical entry into the data center in the case of an IT security event. The network drive access is limited to the NOAA IT staff. Signs are posted that video surveillance is in progress once you enter into the area where the camera view reaches.

	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			
To determine eligibility		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)		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, and contact during Continuity of Operations (COOP) activities. This information is that of federal employees and contractors.

Electronic personnel-related forms of NOAA employees only are transferred to NOAA HR in bulk or on a case-by-case basis via DOC Accellion (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.

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 in support of the NOAA FN clearance process (application). The passports are transmitted via Accellion 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. The individual user (HR Liaison role) within the Resources Branch (OBS23) has been provided an encrypted drive (non-portable) for storage of PII/BII.

Proprietary information related to federal acquisition actions are maintained for administrative

purposes.

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	X *		
Federal agencies	X**		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*In case of privacy/security breach

**NASA security office, and Department of Justice in case of breach

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

6.2 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: NOAA WFMO Recruitment Analysis Data System (RADS). NOAA8873 uploads employee PII in specified formats to RADS. The individual user (HR Liaison role) within the Resources Branch (OBS23)

	has been provided an encrypted drive (non-portable) for storage of PII/BII.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 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		Government Employees	X
Contractors	X		
Other (specify):			

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: http://www.ndbc.noaa.gov/contact_us.shtm_ A form for new employees with a PAS is stored in a folder, and attached with this PIA._____.	
X	Yes, notice is provided by other means.	Specify how: **Identifying Numbers**: Written notice is included on all personnel forms that employees (federal) complete. Notice is provided verbally to a foreign visitor by the US sponsor or the DOC staff at DOC International Affairs Office, at the time of the Foreign National's (FN'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 act 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. **System Administration/Audit Data**: NIST SP 800-53A Rev 4 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**: FNs are given the opportunity to decline to provide information during the clearance process with NOAA. If FNs 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 two factor authentication (2FA). If an employee declines to provide, no network access is provided. **General Personal Data**: For the Continuity of Operations (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.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: **System Administration/Audit Data**: NIST SP 800-53A Rev 4 requires information systems to collect audit data in support of IT security.

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**: FNs 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 two factor authentication (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 the Continuity of Operations (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.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: **System Administration/Audit Data**: NIST SP 800-53A Rev 4 requires information systems to collect audit data in support of IT security.

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**: FNs are given the opportunity to update their information during a subsequent clearance process with NOAA where the FN completes a new application. **General Personal Data**: For the Continuity of Operations (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. **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. **Work-Related Data**: Performance/position information is part of the official personnel record for DOC employees and will be updated upon official personnel actions. **General Personal Data**: Customers voluntarily provide email address and contact information at their discretion when contacting the NDBC Webmaster, but we collect information only per each email, rather than keeping a record.
	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 FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): *_01/28/2017* ☐ 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 and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
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 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.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

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 MaaS 360.

NDBC employees are required to utilize DOC Accellion 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 all PII/BII in the system.

Section 9: Privacy Act

9.1 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 and number *(list all that apply)*: *COMMERCE/DEPT-13, Investigative and Security Records* *COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies* *DEPT-6, Visitor Logs and Permits for Facilities under Department Control* *DEPT-25, Access Control and Identity Management System* *NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.* *OPM/GOVT-1, General Personnel Records.*
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

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, General Records Schedule 20-Electronic Records* *NARA, General Records Schedule 24-Information Technology Operations and Management 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 Levels

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.

	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 levels. *(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.*
X	Quantity of PII	Provide explanation: *NDBC employees (federal and contractor) total less than 250 and minimal PII is collected/maintained.*
X	Data Field Sensitivity	Provide explanation: *Some sensitive PII is collected, mainly from foreign visitors.*
X	Context of Use	Provide explanation: *Information is for official use only and contained within DOC and NOAA.*
	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 IAW NIST SP 800-53 Revision 4.*
	Other:	Provide explanation:

Section 12: Analysis

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

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

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

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