Version Number: 01-2019

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
Date: 2020.08.04 11:43:13 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer — Date: 08/03/2020

U.S. Department of Commerce Privacy Impact Assessment
NOAA/National Data Buoy Center (NDBC)

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

Introduction: System Description

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

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

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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

General Support System (GSS)

(b) System location

Stennis Space Center, Mississippi Silver Spring, Maryland

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

Amazon Web Services (AWS) –NOAA0201 WOC: Data Processing servers are IaaS within the FedRAMP GovCloud/SLA (NOAA BPA) US Air Force Space Command Iridium: Satellite communications to transmit/receive data from stations/IAA

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

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

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

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

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

NOAA8860—WCCIS: Provides OneNWSNet connection to NDBC/None

NOAA8865—NTWC: Access to raw tsunami data/ISA

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

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

(e) 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.

(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 (Coastal WxBuoy, C-MAN, DART, TAO).
NDBC partner data is also ingested via file transfer protocol (FTP) and application programming interface (API). **POA&M 105542 is to secure FTP at NDBC.**

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

(g) Any information sharing conducted by the system

Information sharing is outlined in section "c" for interconnections and section "e" for users, the weather community, and the public sector. The data collected and shared by the system is public weather data.

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

- 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
- 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 Records
- DEPT-6, Visitor Logs and Permits for Facilities under Department Control
- NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.
- DEPT-13, Investigative and Security Records
- OPM/GOVT-1, General Personnel Records

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

system

NOAA8873 FIPS 199 Security Impact Category: 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.

____ 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).

X___ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

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): DoD ID Number (CAC Authentication)					

*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).

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. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address	X	s. Physical Characteristics	
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			
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		
k. Other work-related data (specify):					

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.*					

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 POC with responsibility for processing and protecting the data collected.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	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 (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): Video surveillance is conducted on buoys equipped with buoycams to collect visual environmental data. Video surveillance is also conducted at the entry and inside the NOAA8873 data center for IT Security purposes.			

	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)		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 (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., SF-50, Performance Evaluations, etc) may be accessed via the Electronic Official Personnel Folder (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 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. 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, CMAN 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.)

NDBC personnel are required to complete the NOAA IT Security 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 NARA on records retention policies.

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			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	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 in addition to NOAA's Google Suite (maintained per NOAA CIO requirements).
	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.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 ISSO when giving their DoD ID numbers. 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 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, CMAN stations). **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. There is no expectation to privacy for cameras collecting environmental data positioned on data collection platforms (buoys, CMAN stations).
X	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. There is no expectation to privacy for cameras collecting environmental data positioned on data collection platforms (buoys, CMAN stations).
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. 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, CMAN 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): 01/30/2020 ☐ 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 MaaS 360.

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. *(list all that apply)*: *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 Records* *DEPT-6, Visitor Logs and Permits for Facilities under Department Control* *NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.* *DEPT-13, Investigative and Security Records* *OPM/GOVT-1, General Personnel Records*
	Yes, a SORN has been submitted to the Department for approval on (date).
	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 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 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 minimalize 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.