Version Number: 01-2021

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

Privacy Impact Assessment
for the
NOAA6701
Office of Response and Restoration (OR&R) Local Area Network

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

GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892
Date: 2022.01.24 09:15:49 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/NOS/Office of Response and Restoration (OR&R) Local Area Network

Unique Project Identifier: NOAA6701

Introduction: System Description

Provide a brief description of the information system.

The Office of Response and Restoration (OR&R) mission is to "To protect and restore ocean and coastal resources from the impacts of oil, chemicals, marine debris, and other hazards. We provide expert leadership, training, and time-critical services that benefit the environment, public, and economy ". The OR&R vision "The Nation's oceans and coasts are healthy for future generations, protected and restored from pollution and other environmental threats.

ORR Mission(s) Supported

The OR&R organization consists of the following mission and business areas:

1. OR&R Headquarters is the support of managing the business such as funding appropriations development and management, personnel management to include human resources, time management, payroll, and office supplies. OR&R headquarters mission is to work with Congress on appropriations as it applies to all OR&R mission. OR&R headquarters also includes General Counsel, the General Counsel for Natural Resources (GCNR), which provides legal advice to the NOAA Fisheries and the NOAA Ocean Service. General Counsel seeks restoration from responsible parties for injuries caused to our Nation's natural resources by releases of hazardous substances; and physical impacts (i.e., vessel grounding) to unique resources in National Marine Sanctuaries.
2. Emergency Response Division (ERD) responds to oil spills, chemical spills, and significant environment incidents. Under the National Contingency Plan, NOAA has responsibility for providing scientific support to the Federal On-Scene Coordinator (FOSC) for oil and hazardous material spills. When spills occur, NOAA Scientific Support Coordinators (SSCs) coordinate scientific information and provide critical information to the FOSC. ERD scientists are multidisciplinary team that includes oceanographers, modelers, biologists, chemists, and geologists. ERD scientists work in Seattle and support the SSCs during spill events, as well as for drills, exercises, and contingency planning. SSCs are strategically located around the country, often within U.S. Coast Guard (USCG) offices, effectively providing local services to a range of users in public and private sectors. ERD services include:
    a. Supporting emergency response activities
    b. Support environment contingency plans
    c. Develop tools for local decision makers
    d. Provide training

    ERD facilitates spill prevention, preparedness, and response at national and local levels, and provides expertise on such issues as dispersant use, response countermeasures, and alternative response technologies. ERD's scope encompasses the entire U.S. coastline, including the

Great Lakes, Alaska, Hawaii, and U.S. territories. In the last twenty-five years, ERD has responded to almost every major marine spill in the U.S and often sought international environment incidents. In addition, ERD support incidents such as but to limited to downed aircraft, search and rescue, and tracking floating objects.

The Emergency Response Division typically responds to 150-200 incidents annually. Descriptions of some recent responses by ERD are available in our Significant Incidents section. News, photos, and other information about current and historical spill incidents is available at OR&R IncidentNews site at ***incidentnews.noaa.gov***.

3. Assessment Restoration Division (ARD) also support of oil spills, chemical spills, and significant incidents. ARD is responsible for the plan and implement a coordinated, agency-wide damage assessment program to meet the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA), the federal Water Pollution Control Act (Clean Water Act), the Oil Pollution Act of 1990, and the National Contingency Plan. The Damage Assessment Center is responsible to:

    a. Prepare an infrastructure capable of planning and conducting the damage assessment process
    b. Determine injury to natural resources from oil and hazardous substances
    c. Calculate the claim compensation for the public from the potentially responsible parties for those injured resources.

4. Marine Debris Division (MDD) manages waste of consumer materials manufactured or processed disposed or abandoned into the oceans or USA Great Lakes. MDD serves as a centralized program within NOAA to coordinate, strengthen, and promote marine debris activities within the agency and among its partners and the public.

   Research is beginning to show the scope of the issue, and this knowledge, along with new technologies, can lead solutions that are more effective to the problem. Marine debris has many harmful impacts on ecosystems, such as habitat degradation, entanglement, ingestion, and transportation of non-native species. Debris can even affect human health and navigation safety. MDD focuses its efforts to reduce and prevent marine debris decrease not only the quantities but also the impacts of debris, and over time, create an overall change in the behaviors that lead to debris. MDD works with U.S. and international partners to solve the problem of marine debris.

5. Business Operations Division (BOD) is the Budget and Financial Management, Employee Resources, Cost Recovery, and Information Technology. BSG is responsible for the day-to-day operations of the Program Office to include budgets, travel, timekeeping, human resources, information technology (IT), records management, and internal policy and processes. The BSG IT team also supports other OR&R divisions' software development.

6. Disaster Preparedness Program (DPP) is a new program to prepare NOS and partners to respond to and recover from pollution events and natural disasters. The Gulf of Mexico Disaster Response Center (DRC) is a facility as a collaboration hub for NOAA offices in the Gulf of Mexico region to develop and coordinate response plans and to develop collaboration capabilities of a better response community.

   The Center provides two major functions in support of the NOAA mission:

    a. First, the Center provides National Ocean Service (NOS) OR&R management and operations a place to give support staff users with work space for day-to-day business

activities; host regional preparedness planning workshops; incident response training activities; and a coordination hub to plan for emergencies. The Center provides NOAA OR&R collaboration users outside of the DRC with the ability to collaborate on business activities.

b. Second, the Center provides NOAA with a facility that can withstand weather conditions and available for standard users, such as Federal, State, and local environment incident responders. Intended to serve as a safe and ready command center during major disaster responses in the Gulf, the DRC also offers facilities for drills, trainings, workshops, and planning activities.

No information/applications that collect, store, transmit PII/BII have been added/removed from the system.

Address the following elements:

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

The NOAA6701 Administrative LAN is a General Support System (GSS), with a server located in Seattle, Washington, which collects and maintains Personally Identifiable Information (PII) as part of the application and hiring of employees (electronic copies of resumes are stored temporarily during the hiring phase), as well as standard HR information (such as Travel authorization and vouchers, passports (temporarily only and then deleted) and international travel forms, information for security badging process, and performance appraisal ranking). The system receives, via secure facsimile transmission, credit card orders for OR&R products identified for recovery of User Fees (Oil Spill Job Aids), which are processed for payment through the pay.gov website by OR&R staff (i.e. no credit card information is resident on the system or its computers) and is only produced in printed form. The printed forms are kept long enough to process payment and then are securely shredded. OR&R employee and contractor data is collected, stored and maintained for internal OR&R Business Continuity, Human Resource, and workforce planning purposes (federal employee/contractor). The storage is in the form of PDF forms or MS Word documents in a secure folder on the OR&R network.

(b) System location

NOAA6701 staff and program offices are located on the Silver Spring Metro Center Campus, Western Regional Center campus, Gulf of Mexico Disaster Response Center, and regional staff located remote offices around the U.S.

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

NOAA6701 interconnects to the following systems:

NOAA6001- Active Directory, and various enterprise management applications.

NOAA0100- Cybersecurity and Incident Response

NOAA0550- Network connectivity

NOAA0700- Authentication services

NOAA0900- g-suite, MaaS360, Microsoft Power BI

NOAA6702- secure connection to AWS environment for administration.

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

NOAA6701 operates with network infrastructure, virtual server infrastructure, physical servers, workstations, and storage area networks, and printers/faxes to support staff in meeting the mission. The NOAA6701 system has internal and external web servers. The internal servers are used for business processes such as the IT help desk, training, tracking budgets, development, etc. The external web sites support our primary mission featuring resources to some of the in house developed applications for supporting responses to oil and chemical spills with tools such trajectory forecasts and modeling (GNOME, ESI, TAP, etc.). In addition, OR&R also hosts sites which are used to report and track status of emergency responses (Responselink, IncidentNews). OR&R has several social media sites (Facebook, Twitter, Flickr) which are used to connect and different audiences like Federal, State, and university partners as well as the public.

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

All internal data is retrieved using Government Furnished Equipment (GFE) suing to appropriate application to open, review, verify, and securely delete the information. Internal data is security is provided by defense in depth with layered security for internal data. (Physical access, Firewalls, Active Directory, Access Controls, etc.) Web sites that are only accessible to internal users include (Jira, Training, Cost Recovery, GitLab, Trac, and Agreements). General public will only have access to the public to response tools that are made available on public web sites. (GNOME, GOODS, CAMEO Chemicals, Incident News) NOAA6701 public web sites may include images, photographs, video and/or audio recordings, biographies, and award recognition. OR&R has several social media sites (Facebook, Twitter, Flickr) which are used for public outreach, communication, and employee/partner recognition. Public data is hosted on publicly accessible web sites which are all hosted with SSL/TLS certificates for enhanced security

(f) How information is transmitted to and from the system

All sensitive information is transmitted through secure e-mail (Kite Works), facsimile, or data is manually entered into online web applications such as E2 Travel Manager, HR-connect, CBS, etc. Google mail and G-Suite is used by NOAA6701 for email and data sharing as NOAA preferred provider. Internal data is security is provided by defense in depth with layered security for internal data. (Physical access, Firewalls, Active Directory, Access Controls, etc.). Public data is hosted on publicly accessible web sites which are all hosted with SSL/TLS certificates for enhanced security. OR&R Outreach Office manages its social media sites from NOAA6701 workstations.

(g) Any information sharing

The PII in NOAA6701 includes information on OR&R employees HR documents such as

resumes or information for security badges and travel documents like travel vouchers or passports may be collected. For non-NOAA and public (users who subscribe to ORR newsletters or take training classes offered by ORR) Name, address, email address and organization/affiliation data may be collected. For those who take surveys and in order to follow-up on the surveys to those who consent information (including age, level of education, numbers of adults and children in family, name and home address) may be collected. ResponseLink the primary site utilized by OR&R to communicate with partners and other federal agencies issues username/password to access the site. Email and phone numbers are also gathered to enable communication during an Oil or Chemical spills when OR&R is requested to respond by one of the external partners. All these data types are stored in word or pdf documents. The NOAA6701 system enables OR&R in providing public outreach, communication, and employee/partner recognition on our public web sites as well as several social media accounts (Facebook, Twitter, Flickr) which may include photos, biographies, and award recognition.

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

- U.S. DOC/NOAA NRDA Regulations (OPA) NRDA Regulations 15 C.F.R. 990; Oil Pollution Act of 1990. Establishes legal authorities for NRDA
- U.S. DOC/NOAA Guidance Documents
- Pre-assessment Phase: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment Remediation and Restoration Program, NOAA, August 1996
- Injury Assessment: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment Remediation and Restoration Program, NOAA, August 1996
- Specifications for Use of NRDAM/CME Version 2.4 to Generate Compensation Formulas: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment Remediation and Restoration Program, NOAA, August 1996
- Primary Restoration: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment and Restoration Program, NOAA, August 1996
- Restoration Planning: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment and Restoration Program, NOAA, August 1996.
- Other relevant Guidance Documents may be accessed at the NOAA DARRP Website.
- The general legislation supporting the system is 5 U.S.C.301, one of the statutes concerning government organization and employees.
- -5 U.S.C. § 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.
- -15 U.S.C. § 1512 is an Organic Law which confers general powers and duties authority to executive agencies, vesting jurisdiction and control of departments, bureaus, offices and branches.
- 28 U.S.C. 3101-3105, Debt Collection Act of 1982 (Pub. L. 97-365); 26 U.S.C. 6402(d); and 31 U.S.C. 3711.

- Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966.
- Executive Orders 10450, 11478, 12065, 5 U.S.C. 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.
- 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.
- For the Entity Management functional area of SAM, the authorities for collecting the information and maintaining the system are the Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204 and 2 CFR, Subtitle A, Chapter I, and Part 25, as well as 40 U.S.C. 121(c). For the exclusions portion of the Performance Information functional area, the authorities are FAR Subparts 9.4 and 28.2, Executive Order 12549 (February 18, 1986), Executive Order 12689 (August 16, 1989).
- E-Government Act of 2002 (Pub. L. 107–347) Section 204; Davis-Bacon and Related Acts: 40 U.S.C. 3141–3148, 40 U.S.C. 276a; 29 CFR parts 1, 3, 5, 6 and 7; Section 5 of the Digital Accountability and Transparency Act (DATA Act), Public Law 113–101.

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

FIPS 199 Security Categorization: Moderate (M, M, M).

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*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport	X	k. Financial Transaction	X
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m. Medical Record	
e. File/Case ID	X				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: Employee's official Government Passports are required to obtain foreign travel authorizations for employees. The Passport information is transmitted securely via KiteWorks before being deleted from the travel teams' NOAA6701 computer. Credit card information is received via secure fax, entered into the pay.gov web site by OR&R staff to process payment, then the paper form is securely shredded.					

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	X	l. Email Address	X	s. Marital Status	

f. Race/Ethnicity		m. Education	X	t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify): Numbers of adults and children in family					

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

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X	f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs	X	j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify): Photographs are used for outreach and recognition					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	f. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify): User ID, IP Address, and Date/Time of Access is automatically collected by the System for auditing purposes only.					

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	X
Telephone	X	Email	X		
Other (specify): Subscription information for newsletters including name, email address, organization/affiliation are for contact purposes only. Information is collected during surveys conducted by interview of members of the public, and deleted once surveys are mailed. Information is maintained in a list that is accessible to ORR users with appropriate permissions to view and update the contact lists as necessary. OR&R social media sites, (Facebook and Twitter) may have PII from users posting to these sites. That data is subject to the privacy policies of the respective					

systems.

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

Non-government Sources					
Public Organizations	X	Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): **Proposal & Acquisition.** BII information obtained and utilized during the proposal and acquisition obtained through deliverable package and contain specific company information. BII information on secure network folders during the execution of award of the contract and other information from business not receiving awards deleted, when appropriate					

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

Users are required to provide information to OR&R for contact purposes. The user inputting the data is required to ensure the accuracy of this information. Manual review is used to verify data accuracy entered into documents and forms. Form input validation ensures the data is of a valid type and not malicious however it does not ensure the accuracy of the data input.

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. 0648-0644 Shipboard Observation Form for Floating Marine Debris 0648-0718 NOAA Marine Debris Program Performance Progress Report.
	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	
Video surveillance	X	Electronic purchase transactions	
Other (specify): The DRC utilizes a video surveillance system, which is managed by the DRC staff. Signs indicating that the facility is being monitored by video are posted. The facility does not have security guards and is open 8AM to 5:00PM. This is a stand-alone system which records onto disks which are overwritten every 60 days (or when full). Only the DRC manager and the one IT staff have access to the disks.			
	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	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation	X	For criminal law enforcement activities	
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)	X
Other (specify): In order to determine a potential contractor's ability to fulfill contract a request for proposal (RFP) proprietary information (BII) may be collected to review proposals.			

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).

Office of Response and Restoration collects PII as part of the application and hiring of

employees (electronic copies of resumes are stored temporarily during the hiring phase and then deleted), as well as standard HR information (such as Travel authorization and vouchers, passports and international travel forms, information for security badging process, and performance appraisal ranking). OR&R' employee and contractor data is collected, stored and maintained for internal OR&R Business Continuity, Human Resource, and workforce planning purposes (federal employee/contractor). The storage is in the form of PDF forms or MS Word documents in a secure folder on OR&R network (members of the public and Federal employees).

User name, phone number, and work email addresses are collected during the account request process. The username given is the root of the user's email address, and the email address must be a work email account. Email address is used for correspondence about planned system outages, etc., and for password reset requests. This PII is collected from federal employees and contractors, and academia users who request an account on the system and are approved for a valid business need.

BII is collected from those responding to solicitations and in resulting contracts, from members of the public.

Information about responsible parties and information about labor expended during response activities are collected to support litigation by General Counsel.

Last successful login time is used to gauge automatic account deactivation.

ORR conducts public surveys, which gather age, numbers of adults and children in the family and level of education, as well as names and addresses of the public in order to mail follow-up surveys to them.

The NOAA6701 system enables OR&R in providing public outreach, communication, and employee/partner recognition on our public web sites as well as several social media accounts (Facebook and Twitter) which may include photos, biographies, and award recognition

Public facing web sites are required to use Google Analytics, organized by the Office of Management and Budget (OMB), "Guidance for Online Use of Web Measurement and Customization Technologies" (OMB M-10-22). This cookie does not collect personal identifying information and is considered a Tier 2 service in the OMB guidance.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:
"All public facing websites and digital services should be designed around user needs with data-driven analysis influencing management and development decisions. Agencies should use qualitative and quantitative data to determine user goals, needs, and behaviors, and continually test websites and digital services to ensure that user needs are addressed.
A. All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs.

B. GSA will maintain a public listing of the domains participating in the DAP and track agency compliance on the DotGov Dashboard and
C. Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".
The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

No SSNs are collected or stored within NOAA6701. NOAA6701 does gather employee's Government passport information in order to obtain foreign travel approval from the State Department. The passport data is scanned by the travel preparer then uploaded to KiteWorks to securely transfer the information before being deleted from the workstation.

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.)

Potential threats to privacy for NOAA6701 include unintentional disclosure, information system breaches, insider threats, etc. NOAA6701 users are required to take annual IT Security awareness training including protecting PII. OR&R has additional PII training for users several times a year. NOAA6701 systems are monitored and audit logs are monitored by the NOAA-Computer Incident Response Team N-CIRT. NOAA6701 is assessed annually by independent assessors to validate the security controls in place to protect the Confidentiality, Integrity, and Availability of the information system.

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		X
Federal agencies	X		X
State, local, tribal gov't agencies			
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: NOAA6701 has interconnections with NOAA6001, NOAA6702, NOAA0100, NOAA0550, NOAA0700 and NOAA0900. Network traffic and data at rest are encrypted with FIPS 140-2 compliant algorithms to protect sensitive data from unauthorized disclosure. File servers log access to files and folders to alert admins to unauthorized attempts to access data.
	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): General public will only have access to the public outreach, communication, and employee/partner recognition on our public web sites which may include photos, biographies, and award recognition.			

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://response.restoration.noaa.gov/privacy-policy.html	
X	Yes, notice is provided by other means.	Specify how: ORR staff members (employees) are provided notice via email of how PII is used (i.e., emergency contact information in case of emergency or disasters) upon hire as well as via ORR Privacy Policy. Visitors to the ORR web sites, users who request email list subscriptions, and those requesting training opportunities can receive notice on the information request contact form. Acquisition and contracts: Businesses are given notice on solicitations and on contracts. Surveys: respondents are asked face to face, to participate in an onsite interview and if they agree, to be mailed a full survey.
	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: Visitors to the ORR web sites, users who request email list subscriptions, and those requesting training opportunities can request information by submitting an email through an information request contact form. Individuals are under no obligation to provide any identifying information, and the details of how this information is handled are readily available via the ORR Privacy Policy and a Privacy Act statement. Staff members are notified upon request in writing for collection of identifying information. They may decline to provide the information via email or verbally, to their supervisors, but that in some instances it may affect their employment. Vendors are also under no obligation to provide any identifying information. BII can be declined to be provided as part of the acquisition package but could impact evaluation of the bid. Surveys: individuals approached for interviews may decline (face to face).
	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: For those requesting an account, there is only one use for the information. By providing the information, the account requestor agrees to the use. Applicants or employees can choose to not provide information but this may affect their employment. Vendors: There is only one use for solicitations; not responding constitutes withholding consent, but could impact evaluation of the bid. Survey respondents may decline to participate at all, when asked (face to face) or they may complete a screening interview but then decline to provide their names and addresses for the full survey.
	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: Those requesting updates to their information can contact ORR directly by email or phone as listed in the ORR Web site and Privacy policy located at: https://response.restoration.noaa.gov/about. Surveys: Individuals whose addresses change before they receive a mail survey may contact the NOS program manager by email.
	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.)*

X	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:** Access to NOAA6701 is monitored with both physical and logical access controls. In addition, user permissions and for role-based access and logging is managed through the NOAA6001 Active directory. All logs for NOAA6701 are forwarded to the NOAA Arcsight centralized log management tool.
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): 10/28/2021 ☐ 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.
	Other (specify):

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).*

NOAA6701 utilizes the National Ocean Service (NOS) Microsoft Active Directory to enforce user identification and authorization to access the information system. All users are vetted and background investigations are performed before access to the information system is granted. Least privilege is employed in the system and only those users authorized access to information are allowed access to the data. Data in the information system is encrypted and all PII or BII data is encrypted with a FIPS140-2 encryption method while at rest. OR&R utilizes laptop computers for end users and we encrypt all laptops with the NOS enterprise McAfee Endpoint encryption solution. The DOC KiteWorks secure email system or fax machines are used to transmit PII/BII data.

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-2, Accounts Receivable, COMMERCE/DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons, COMMERCE/DEPT-13, Investigative and Security Records, COMMERCE/DEPT-18, Employees Personnel Files not covered by Notices of Other Agencies, NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission, GSA/GOVT-9, System for Award Management, GSA/GOVT-10, FAR Data Collection System
	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: The retention period for these records is guided by the General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the federal government. The underlying paper records relating to employees are covered by GRS 2.2 Employee management administrative records and GRS 2.4 Employee Compensation and Benefits Records. In accordance with GRS (Transmittal 31), electronic versions of records scheduled for disposal under other records schedules may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. Guidance for these records in the NOAA Records Schedules refers disposition to GRS (Transmittal 31). NOAA Records Schedules Chapter 100 – General Chapter 200 – Administrative and Housekeeping Chapter 1600 – National Ocean Service (NOS) Functional Files describes records created and maintained in the National Ocean Service (NOS) on the ocean and coastal zone management services and information products that support national needs arising from increasing uses and opportunities of the oceans and estuaries. 1605 – Office of Response and Restoration Records relating to the prevention and mitigation of risks to coastal resources and restoration of habitats from oil and hazardous materials; support for the cleanup of spills occurring in U.S. coastal and navigable waters; training and outreach programs; and software for spill responders and planners and coastal management decision making. 1605-01 - Incident Response and Waste Site Financial Records. 1605-02 - Query Manager Databases (QM). 1605-03 - Coastal Resource Coordinator Records. 1605-04 - HAZMAT Response Records. 1605-05 - Electronic Copies-All Offices.

	1605-06 - Defunct. 1605-07 – Defunct. 1605-08 – Defunct. 1605-09 - NRDA Administration Record Files - Pre Settlement. 1605-10 - NRDA Pre-Settlement Case Files. 1605-11 - NRDA Pre-Settlement Working Files. 1605-12 - Infant and Orphan Case Files. 1605-13 - Multi-case Evidence Tracking Records. 1605-14 - Cost Accounting and Documentation Files. 1605-15 - Rulemaking Administrative Record. 1605-16 - Rulemaking Working Files – consolidated into 1605-15. Chapter 2300 General Information Technology Management Records states "This schedule includes records related to developing, operating, and maintaining computer software, systems, and infrastructure improvements; complying with information technology policies and plans; and maintaining data standards" Chapter 2400 Information Systems Security Records states "This schedule covers records created and maintained by Federal agencies related to protecting the security of information technology systems and data, and responding to computer security incidents" • U.S. DOC/NOAA NRDA Regulations (OPA) NRDA Regulations 15 C.F.R. 990 • U.S. DOC/NOAA Guidance Documents • Preassessment Phase: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment Remediation and Restoration Program, NOAA, August 1996 • Injury Assessment: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment Remediation and Restoration Program, NOAA, August 1996 • Specifications for Use of NRDAM/CME Version 2.4 to Generate Compensation Formulas: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment Remediation and Restoration Program, NOAA, August 1996 • Primary Restoration: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment and Restoration Program, NOAA, August 1996 • Restoration Planning: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment and Restoration Program, NOAA, August 1996. Other relevant Guidance Documents may be accessed at the NOAA DARRP Website
	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	X	Deleting	
Other (specify):			

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: Names, emails and addresses are collected, allowing identification of individuals
X	Quantity of PII	Provide explanation: OR&R has a limited quantity of PII/BII necessary for HR actions, management, contract management, and interactions with non-NOAA personnel for training, surveys, and mailing lists.
X	Data Field Sensitivity	Provide explanation: No SSN, credit card information, or passport information is collected or maintained in NOAA6701 (passport information is scanned and transmitted via KiteWorks and then deleted).
X	Context of Use	Provide explanation: PII/BII that is collected and maintained is mostly for employment purposes, contract management, communications, training, and surveys.
X	Obligation to Protect Confidentiality	Provide explanation: 5 USC 552(b)(4) and the FAR, in accordance with 41 CFR 13.
X	Access to and Location of PII	Provide explanation: Only authorized or privileged users can access the PII/BII. NOAA6701 employs the concept of least privilege; secure network; transmission, and encrypted data storage.
	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.)

NOAA6701 OR&R has reduced the amount and types of PII that are collected and maintained in the system. No sensitive PII such as SSN, credit card data, etc. is collected within the system. We have modified our business processes to reduce the risk of an unauthorized access, alteration, or disclosure of PII with technical, physical, and administrative safeguards. Administrative safeguards include training personnel on information handling best practices. Physical safeguards include ensuring paper digital records are secured and access controlled physically and logically. Technical controls include the use of encrypted DOC Kite Works email, encrypting computers and requiring Common Access Cards (2FA) for system access.

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.