Version Number: 01-2017

U.S. Department of Commerce

National Oceanic and Atmospheric Administration (NOAA)
National Ocean Services (NOS)
Office of Response and Restoration (OR&R)

Privacy Impact Assessment
For the
Office of Response and Restoration (OR&R) Local Area Network (LAN) System (ORR LAN)
NOAA6701

Reviewed by: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2019.05.20 17:17:12 -04'00', Bureau Chief Privacy Officer

Mark Graff

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

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

for Catrina D. Purvis

KRISTEN LEFEVRE Digitally signed by KRISTEN LEFEVRE Date: 2019.05.24 13:49:22 -04'00' 05/24/2019

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

U.S. Department of Commerce Privacy Impact Assessment
National Oceanic and Atmospheric Administration (NOAA)
Office of Response and Restoration (OR&R) Local Area Network (LAN) System (ORR LAN)

Unique Project Identifier: DOC Consolidated IT Infrastructure: 006-00-02-00-01-0511-00-404-139 (CSAM: 1283)

Introduction: System Description

The Office of Response and Restoration (OR&R) is the focal point in NOAA for preventing, planning for, and responding to oil spills, releases of hazardous substances, and hazardous waste sites in coastal environments and restoring affected resources. OR&R protects and restores coastal resources through the application of science and technology. On behalf of the public, OR&R addresses environmental threats from catastrophic emergencies such as the oil spills of the Exxon Valdez or oil pipeline of the Deep Water Horizon; chronic releases from contaminated sediments such as the Hudson River Superfund site; vessel groundings in sanctuaries such as coral reefs in the Florida Keys. By working in partnerships, OR&R empowers communities and decision makers to be coastal stewards by transferring the results of its experience through training, guidance, and decision-making tools that emphasize actions to improve coastal health.

(a) A general description of the information in the system

The NOAA6701 Administrative LAN is a General Support System (GSS), with the 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.

PII may include information needed to establish accounts for non-NOAA and public users who subscribe to ORR newsletters, take training classes offered by ORR (Name, address, email address and organization/affiliation and for those who take surveys in order that we may mail follow-up surveys to those who consent (including age, level of education, numbers of adults and children in family, name and home address).

Information is automatically collected by the system for auditing purposes only when users access NOAA6701 systems. The audit logs generated during the access of NOAA6701 are shared with the NOS web administrators for evaluation purposes. The information that is stored in this system consists of the following: User ID, IP Address, and Date/Time of Access.

No SSNs are collected in NOAA6701. SSNs have been deliberately removed from ORR's administrative processes. Sensitive PII, such as SSN or financial information, is entered by the employee/preparer on printed form for NOAA Badging or directly into NFC, Travel, or Workforce management application outside of the boundary of NOAA6701 (and not maintained within the system). Foreign Travel requests through the State Department do require the travel team to upload Government Passport information via Accellion. Employees are discouraged from downloading and storing sensitive information on their work computers such as copies of their performance (EOPF) files, passports, forms for acquiring/updating passports, or any personal financial information. OR&R provides monthly training sessions on IT issues including handling of sensitive information and PII. All staff have access to the OR&R intranet site that includes the training on PII. We also provide training on the use of Accellion and "discourage" the practice of storing PII on a work computer.

Business Identifiable Information (BII) is primarily collected during the pre and post activities associated with the acquisition and management of contracts. The storage is in the form of PDF forms or MS Word documents.

(b) Any information sharing conducted by the system:

- *BII is not shared outside the bureau.*
- *PII is shared with the State Department via Accellion for official foreign travel clearances*
- *Human Resources: NOAA (WFMO) ORR utilizes NOAA's WFMO and does not operate a separate HR division*
- *Travel authorizations: NOAA Travel (E2) ORR utilizes NOAA's Travel system and does not operate a separate Travel division. Passport information is securely transmitted to the Department of State to obtain foreign travel clearances for employees travelling abroad for official duties.*
- *Budget: Commerce Business Systems (CBS) ORR utilizes NOAA's Budget and Finance system and does not operate a separate Budget/Finance division.*
- *Public surveys: not shared outside the bureau.*
- *PII is shared with the Department of Commerce and other Federal bureaus in case of security/privacy breach.*

(c) A citation of the legal authority to collect PII and/or BII

- 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.
- Authorities from DEPT-2: 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.
- Authorities from DEPT-9: Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966.
- 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: 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 GSA-GOVT-9: 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).
- Authorities from GSA-GOVT-10: 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.

(e) The Federal Information Processing Standard (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		b. New Interagency Uses	
c. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
d. 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, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 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*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID	X	g. Passport	X*	k. Financial Transaction	X
d. Employee ID	X	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:					

* Employee's official Government Passports are required to obtain foreign travel authorizations for employees. The Passport information is transmitted securely via Accellion 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	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	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education	X	r. Mother's Maiden Name	
s. Other general personal data (specify): Numbers of adults and children in family.					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
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		d. Photographs		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	X	f. Contents of Files	X
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	
Telephone		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.					

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 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

To determine eligibility		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	X	For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	
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 fulfil 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.

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.

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 Accellion to securely transfer the information before being deleted from the workstation.

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		
DOC bureaus	X		
Federal agencies	X		
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.

	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:
X	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 Policy can be found at: https://oceanservice.noaa.gov/privacy.html. The public account request with PAS is at https://response.restoration.noaa.gov/subscribe ***Federal and contractor account request forms and a public survey with PASs are included in the email with this PIA.***	
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: 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	Specify why not:

	pertaining to them.	

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.
	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:NOAA6701 utilizes the NOS Microsoft Active Directory to assign user access and employ auditing measures for access to system resources
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): __05/24/2018_____ ☐ 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.
	Other (specify):

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

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 Accellion secure email system or fax machines are used to transmit PII/BII data.

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)*: DEPT-2, Accounts Receivable, DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons, DEPT-13, Investigative and Security Records, 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, 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: 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 1, Civilian Personnel Records. In accordance with GRS 20, item 3, 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 20. 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. • 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 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: 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 Accellion 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 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.

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

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