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 Products System (ORRPS)
NOAA6702

Reviewed by: _____, Bureau Chief Privacy Officer
Mark Graff

[X] 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 13:58:11 -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 Products System (ORRPS)

Unique Project Identifier: NOAA6702 (OMB Exhibit 300 ID Number: 006-000351103 00-48-02-00-02-00)

Introduction: System Description

The National Oceanic and Atmospheric Administration (NOAA), National Ocean Service (NOS), 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 ship, Exxon Valdez or the oil drilling rig of the Deep Water Horizon; chronic releases from contaminated sediments such as the Hudson River Superfund site; and 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 take to improve coastal health.

NOS OR&R operates the Office of Response and Restoration Products System (ORRPS), NOAA6702. ORRPS is comprised of products developed and published by the Divisions within OR&R - Assessment and Restoration Division (ARD), the Emergency Response Division (ERD), Disaster Response Center (DRC) and Marine Debris Program (MDP). The ORRPS incorporates the product systems from these divisions. ORRPS is currently located in the Amazon Web Services (AWS) East/West FedRAMP cloud. The system is a cloud based solution operating the Environmental Response Management Application (ERMA®) subsystem, the Data Integration, Visualization, Exploration, and Reporting (DIVER) subsystem, the Marine Debris website, NOAA Response Asset Directory (NRAD) website, NOAA's Damage Assessment Remediation and Restoration Program (DARRP) website, Response and Restoration website, and the OR&R Intranet website. NOAA6702 has user identification requirements and applications that support assessment and restoration of natural resources, which may require the collection of PII or BII.

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

NOAA6702, ORRPS contains Personally Identifiable Information (PII) that consists of the information needed to establish accounts for non-public users. The PII is non-sensitive in that it contains information provided by the user to obtain an account that includes the user's name, email address, and telephone number and is provided to the account manager through an email request.

NOAA6702 ORRPS contains Business Identifiable Information (BII) that is primarily obtained during an event, such as an oil spill, that is often part of the litigation, and not released to the public until it has completed the OR&R process to validate the information and review the sensitivity of the information, which may require the coordination with Office of General Counsel. Within the Office of General Counsel, the Natural Resources Section provides legal advice to the National Marine Fisheries Service and the National Ocean Service. The purpose of the DARRP Program is to seek restoration from responsible parties for injuries caused to our Nation's natural resources by releases of hazardous substances from thousands of waste sites, numerous oil spills, and physical impacts (e.g., vessel groundings) to unique resources located in National Marine Sanctuaries. Sharing of any PII/BII data with an outside entity would be pursuant a court order.

For Deepwater Horizon (DWH) – OR&R provided a separate site from (2012-2016) for BP to access the information collected by DIVER/ERMA to do their own analysis in preparation for the court action. The datasets (9,000) from NOAA, federal, state, and Non-Governmental Organization (NGO) partners to support these tasks to respond to environmental incidents had restricted access, which required an ERMA/DIVER account to view. In the case of Deepwater Horizon (DWH), the DIVER and ERMA applications maintained a separate database for the information generated during this event. The data has been migrated to NOAA's National Centers for Environmental Information (NCEI) in accordance with OR&R and NOAA's data management and data stewardship policies. NOAA's ERMA and DIVER applications will continue to make NRDA (and other environmental data) available for mapping, query and download from these applications, and will build linkages to the archived data packages for reference and citation.

ORRPS supports Natural Resource Damage Assessment and Restoration cases and projects.

Environmental Response Management Application (ERMA):

ERMA is an online mapping tool designed to aid in spill preparedness and planning, assist in coordinating emergency response efforts and situational awareness for human and natural disasters and support the Natural Resource Damage Assessment (NRDA) process.

The case data may contain BII (oil spill evidence identifying the source of the spill) and PII (contact information for those requesting an account).

Data Integration, Visualization, Exploration, and Reporting (DIVER):
The National DIVER Portal is a login website that encompasses the DIVER Data Warehouse, which contains environmental data, activity data, and restoration project data.

The case data, when a case is active, may contain BII (oil spill evidence identifying the source of the spill; project restoration identifying information) and PII (contact information for those who collected the information and are accessing information).

(b) any information sharing conducted by the system

ERMA:

Homeland Security Infrastructure Program (HSIP)

HSIP map services or shapefile data come from the HSIP Gold. "It is a compilation of over 560 geospatial datasets, characterizing domestic infrastructure and base map features, which have been assembled from a variety of Federal agencies, commercial vendors, and State mission partners. HSIP Gold 2015, in its entirety, is unclassified; it is subject to the handling and distribution rules for "Unclassified For Official Use Only" due to licensing and sharing restrictions set forth by the data source entities.

Case data: In the case of Deepwater Horizon (DWH), the information collected was later used for litigation support. This information, which may include BII, is shared with other agencies, viewable from ERMA when a case is active. While the case data is archived at NCEI, historical data is still viewable by the public.

Ship positions: Nationwide Automatic Identification System (NAIS). Source Coast Guard

In ERMA, the user can search the Nationwide Automatic Identification System (NAIS) for an Automatic Identification System (AIS) enabled ship by name or MMSI number to determine the last known or reported location of the ship.

DIVER:

Case data: In the case of Deepwater Horizon (DWH), and other cases, information collected, which may include BII, is used for litigation support. This information is shared with other agencies, viewable from DIVER when a case is active. While the case data is archived at NCEI, historical data is still viewable by the public.

If there is a security or privacy breach, information will be shared within the bureau, with the Department and with other federal agencies as applicable.

(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
    - 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.
- Authorities from NOAA-11: 5 U.S.C. 301, Departmental Regulations and 15 U.S.C. 1512, Powers and duties of Department.
- 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.

(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.

NOAA6702 addresses OR&R applications, such as ERMA and DIVER applications in its boundary.

__ _ This is a new information system.

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

_____ This is an existing system for which a Privacy Impact Assessment had not been done, and for which there are privacy risks.

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

X This is an existing information system in which changes do not create new privacy risks and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later).

Section 2: Information in the System

NOAA6702 contains **PII** that is work-related and system administration information. **BII** is contained in the case data collected for a NRDA incident, when a case is active.
NOAA6702 data is encrypted at rest and in transit.
In DIVER, descriptive fields such as the project's name, phase, location, type (i.e., planning or project), and the activity under which the project is being undertaken are associated with the Project ID (BII information is data contained within the project, not the Project/File ID).
The DIVER application also imports data from an external DOI application. The connection to the DOI application encrypts the data while in transit.

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

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify): In NOAA6702, descriptive fields such as the project's name, phase, location, type (i.e., planning or project), and the activity under which the project is being undertaken are associated with the Project or File/Case ID.					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

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

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	
b. Job Title		e. Email Address	X	h. Work History	

c. Work Address		f. Business Associates			
i. Other work-related data (specify):					

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	
g. Other system administration/audit data (specify): User ID is logged in NOAA6702 (ERMA and DIVER) when files are uploaded. Displayed as user name on the screen.					

Other Information (specify)
NOAA6702 ORRPS supports Natural Resource Damage Assessment and Restoration cases and projects. ERMA is an online mapping tool designed to aid in spill preparedness and planning, assist in coordinating emergency response efforts and situational awareness for human and natural disasters and support the Natural Resource Damage Assessment (NRDA) process. The case data, when a case is active, may contain BII (oil spill evidence identifying the source of the spill) and PII (contact information for those who collected the information).
The National DIVER Portal is a login website that encompasses the DIVER Data Warehouse, which contains environmental data, activity data, and restoration project data. The case data, when a case is active, may contain BII (oil spill evidence identifying the source of the spill; project restoration identifying information) and PII (contact information for account users, including those who collected the information).

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		Hard Copy: Mail/Fax		Online	X
Telephone		Email	X		
Other (specify): Name, phone number, and email from account request form from users that require an account. Public users do not require an account.					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal	X	Foreign			
Other (specify Case data: NRDA activities					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	

Third Party Website or Application			
Other (specify):			

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		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

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

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	X
For litigation	X	For criminal law enforcement activities	X
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)	X	For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

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

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 (researchers who are participating in data collection and analysis for response and or restoration efforts) users who request an account on the system and are approved for a valid business need.

Administrative information is used to designate the role for access to information and the decision to allow modification to the information based on the role assigned.

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

Information sharing is an initiative to provide information, which may include PII/BII, for organizations that need it for litigation actions pursuant a court order. Interagency data flows: USCG and NOAA HSPO among others use DIVER/ERMA for responses to spills and responses. However, there is currently no such data in the system; projects that were completed are archived in NCEI.

OR&R provides information requested by other agencies from information collected during NRDA in support of their missions. BII collected is based on the target of the assessment and response activities and how the damage is litigated.

ERMA is used by the NOAA Homeland Security Program Office (HSPO) as a tool to provide their Common Operating Picture. HSPO uses the maps and data layer information from ERMA for agency situational awareness and response related to an event impacting NOAA, People, Mission and Infrastructure.

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

*In case of breach. **The PII/BII in the system will not be shared except pursuant to a court order.

	The PII and BII 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: For active case data that is held locally in ERMA, Access Control, Encryption, Virtual Private Network, Amazon Web Services (AWS) Cloud Environment, Homeland Security Infrastructure Program (HSIP) data comes from a Department of Homeland Security (DHS) mapped server (mapping system similar to ERMA). Receives ship location information from Nationwide Automatic Identification System (NAIS) from the Coast Guard's secure server. Encryption of data in transit is used for system connections (PII/BII information). **(Response) Specific**: Department of interior (DOI) provides DIVER with public data that it collects for the Response. DOI maintains the administrative record in their websites, but DIVER uses the data from DOI after it is transformed into the DIVER schema and then provides the data to view in the DIVER application. DOI information provides information specific to the Response case data that DOI collected. The DIVER Explorer application integrates data from multiple sources. Most data are ingested directly through the DIVER application. One exception to that is the DOI Response Database. DOI provides a complete dump of their Response-related assessment data warehouse and the DIVER team manually integrates this into the warehouse. The DIVER connects to a DOI database using an Extract, Transform, Load (ETL) process that reformats the data to conform to the DIVER schema, using encryption in transit to pull sample and visual observation data. NOAA6702 doesn't share data or directly connect the systems. The DOI dataset includes URL links to associated files and photographs which are made available through the DIVER Explorer user interface. These associated files are not generally publicly available. However, they are surfaced through DIVER Explorer to authorized users of the DIVER application. This is facilitated by a trust relationship between the DOI Response Database and NOAA DIVER application.

	The DIVER application data flow is managed by data managers on a workspace and record level basis.
	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: https://oceanservice.noaa.gov/privacy.html https://response.restoration.noaa.gov/privacy-act-statement https://portal.diver.orr.noaa.gov/web/national/request-user-account https://marinedebris.noaa.gov/privacy-policy https://intranet.orr.noaa.gov/privacy-policy https://www.darrp.noaa.gov/privacy-policy https://erma.noaa.gov/ERMA/RequestAccount?sitename=atlantic.	
X	Yes, notice is provided by other means.	Specify how: Notice is provided on the user account sites.
	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: Users can choose to not request an account. Organizations provide BII based on an agreement with the agency in place (ERMA currently has an informal agreement with USGS; a formal agreement is in process)
	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	Specify how: Email address, phone number, and name are required

	consent to particular uses of their PII/BII.	for account maintenance and communication. Individuals cannot create an account without consent to these uses. Individuals may not consent, in the form of an incomplete account request, but this results in an account not being created. The draft USCG agreement for NAIS data does not specify BII, but does say that sensitive information is for official use only and should be protected as such. The NAIS data is restricted from public access which is limited to federal government users. Other BII collected, such as in response to a spill, is done under one of the citations in paragraph c.) such as the Oil Pollution Act of 1990 where a responsible party agrees to provide data to the federal gov't.

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: Users reach account administrators through the "Contact" link in the site footer. 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.)*

	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: All account modification issues are logged and monitored
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 5/24/2018 This is a new system. The A&A package was 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.

	Contracts with customers establish ownership rights over data including PII/BII.
	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.

Names of account holders and their respective phone numbers and email addresses are accessible only through a role-based security system where only account administrators of ERMA and DIVER can view.

The ERMA and DIVER software is designed to restrict access to data based on specifically granted permissions. These permissions may be granted at several levels:

- Restricted by source system IP address in combination with an authentication "token"/key.
- Restricted to authenticated users with a specific level of granted access.
- ERMA and DIVER designate most data with specific sets (datasets) of "contexts", using an event name, privilege level, and visibility level. In order to view a resource, users must be granted access to all three applicable contexts for a resource. For DIVER it's a workspace, privilege level, and sharing status.
- Low-level access to data (the database and related files) is restricted to the core application, and is not accessible from outside of the application, except by system administrators.
- All underlying system files are encrypted, ensuring that drives taken out of service are not accessible.
- Other system resource data are accessible to only ERMA designated system administrators; and System Administrators, Program Administrators, and Data Managers for DIVER.

Section 9: Privacy Act

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

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

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: COMMERCE/NOAA-11, Contact information for members of the public requesting or providing information related to NOAA's mission.

	DEPT-13, Investigative and Security Records. DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies.
	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. The information is retained by ERMA and DIVER as part of the legal process for supporting litigation actions.
	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		Overwriting	X
Degaussing	X	Deleting	
Other (specify): Information is not deleted, but all information is archived or made inactive. Hard drives containing information that are no longer serviceable are overwritten and degaussed.			

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.

ERMA and DIVER designate most data with specific sets (refers to datasets and user roles of access (event name, privilege level, and visibility level) of "contexts", using an event name, privilege level, and visibility level. In order to view a resource, users must be granted access to all three applicable contexts for a resource. For DIVER it's a workspace, privilege level, and sharing status.

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	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: Only name, phone number, and work email are recorded for accounts requiring login access.
X	Quantity of PII	Provide explanation: Only name, phone number, and work email are recorded for Government, State, Trustees, Contractors, and Academia accounts requiring login access. These accounts number less than 500.
X	Data Field Sensitivity	Provide explanation: User name, phone number, and email address are provided by the user to obtain an account voluntarily. Primarily used for account management. The information is non-sensitive PII.

X	Context of Use	Provide explanation: Only name, phone number, and work email are recorded for account user ID. Used to contact user for account set up and notifications for outages.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Only account administrators can see the PII. Concept of least privilege; secure network and database; encrypted storage and transmission. Information is stored in AWS as a FedRAMP approved site.
	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. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.