Version Number: 01-2019

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) Products Systems (ORRPS)
NOAA6702

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

Jennifer Goode 01/13/2021

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

U.S. Department of Commerce Privacy Impact Assessment
Office of Response and Restoration Products System (ORRPS), NOAA6702

Unique Project Identifier: NOAA6702 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) Whether it is a general support system, major application, or other type of system

NOAA6702 is a general support system. NOS OR&R operates the Office of Response and Restoration Products System (ORRPS) 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), Business Services Group (BSG), Marine Debris Program (MDP), and the Disaster Preparedness Program (DPP). NOAA6702 hosts public and non-public web sites and applications. NOAA6702 does host websites and applications that may collect and/or disseminate PII in the form of images, photographs, video and/or audio recordings No social media sites are operated for OR&R from NOAA6702.

(b) System location

NOAA6702 is located in the Amazon Web Services (AWS) East/West FedRamp cloud.

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

NOAA6702 interconnects with NOAA6701, the Office of Response and Restoration Local Area Network LAN (LAN). This connection provides secure connection for management for NOAA6702 and NOAA6701 provides the logistics, support, development, etc. for NOAA6702.

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

NOAA6702 is an Internet connected system that is in a virtual environment in the AWS cloud. The cloud allows OR&R to utilize the "Elastic" capabilities of the cloud to rapidly ramp up response tools such as ERMA and DIVER for large responses and downsize when the disaster is over. NOAA6702 hosts the applications including Environmental Response Management Application (ERMA®) subsystem and the Data Integration, Visualization, Exploration, and Reporting (DIVER) subsystem application as part of the system boundary. The other websites currently hosted in ORRPS, include the Marine Debris Program web site and Blog, NOAA Response Asset Directory (NRAD), NOAA's Damage Assessment Remediation and Restoration Program (DARRP), Office of Response and Restoration public web page and Blog, and the OR&R Intranet. These applications allow OR&R to fulfill its mission responding to disasters that affect our nation's coasts and water ways and restore the environment to its pre-disaster state.

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

Data is retrieved using Government Furnished Equipment (GFE) to open, review, verify, and securely delete the information for NOAA personnel updating and maintaining the applications in NOAA6702. General public users do not require accounts to access public sites including public outreach, communication, employee/partner recognition which may include photographs, video and/or audio recordings, and biographies. Non-NOAA partners who require access to applications that are not publicly available use username and passwords. All the sites which are hosted utilize SSL/TLS certificates for enhanced security through the user's browser.

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

Information in NOAA6702 is mostly collected through online web applications, forms. Any information that is collected through an e-mail link is then collected and maintained by NOAA6701 in its support role for NOAA6702. Applications such as ERMA in NOAA6702 share data with other federal agencies such as the Coast Guard, DOI, and DHS. Homeland Security Infrastructure Program (HSIP) data comes from a Department of Homeland Security (DHS) mapped server (mapping system similar to ERMA). 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.

(g) Any information sharing conducted by the system

NOAA6702 information sharing related to PII/BII is limited and not shared outside of the bureau. Applications such as ERMA in NOAA6702 share data with other federal agencies such as the Coast Guard, DOI, and DHS. Homeland Security Infrastructure Program (HSIP) data comes from a Department of Homeland Security (DHS) mapped server (mapping system similar to ERMA). ERMA Receives ship location information from Nationwide Automatic Identification System (NAIS) from the Coast Guard's secure server. PII is shared with the Department of Commerce and other Federal bureaus in case of security/privacy breach.

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

(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.

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

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

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify): 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 business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

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		q. Military Service	
d. Gender		k. Telephone Number		r. Criminal Record	
e. Age		l. Email Address		s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

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

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs	X	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify): The NOAA6702 system enables OR&R in providing public outreach, communication, and employee/partner recognition on our public web sites which may include photos, biographies, and award 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	d. Queries Run	X	f. Contents of Files	X
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 Describe how the accuracy of the information in the system is ensured.

Manual review of the data is used to verify data.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
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			
For a Computer Matching Program		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	X
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	X
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.

The NOAA6702 system enables OR&R in providing public outreach, communication, and employee/partner recognition on our public web sites which may include photos, biographies, and award recognition.

For web measurement and customization technologies (multi-session) NOAA6702 is required to collect and maintain data on public facing web sites which 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.

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 NOAA6702 include unintentional disclosure, information system breaches, insider threats, etc. NOAA6702 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. NOAA6702 systems are monitored and audit logs are fed to the NOAA-Computer Incident Response Team N-CIRT for monitoring. NOAA6702 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	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/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: 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: 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. 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 a facilitated by a trust relationship between the DOI Response Database and NOAA DIVER application. The NOAA6702 system enables OR&R in providing public outreach, communication, and employee/partner recognition on our public web sites which may include photos, biographies, and award recognition
	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	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 only contains non-sensitive PII which may include images, photographs, video and/or audio recordings, 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://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	
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 through online forms, web applications and email. Users can choose to not provide PII will not get an account and that is their option. Users must give consent to before the use of images, photographs, video and/or audio recordings, of themselves are shared on web sites. 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 consent to particular uses of their PII/BII.	Specify how: Email address, phone number, and name are required 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. Users must give written consent to before the use of images, photographs, video and/or audio recordings, of themselves are shared on web sites. 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.
	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: Users can reach account administrators through the Contact: link in the site footer.
	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: Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access to NOAA6702 is monitored with both physical and logical access controls. In addition user permissions and for role based access and logging is managed through the AWS CloudTrail. All logs for NOAA6702 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): 06/14/2019 ☐ 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.
	Contracts with customers establish DOC 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. *(Include data encryption in transit and/or at rest, if applicable).*

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 NOAA6702 applications and websites are allowed to view.

The NOAA6702 applications and websites are 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 and other applications 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 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)*: 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, 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, Civilian Personnel 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. 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):			

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.)*

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. User images, photographs, video and/or audio recordings may be traceable to an individual.
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. User images, photographs, video and/or audio recordings are only used with consent.
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. User images, photographs, video and/or audio recordings are only used with consent.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Only account administrators can access 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 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.)

NOAA6702 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 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.