Version Number: 01-2019

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOAA6101
Office for Coastal Management

Reviewed by: MARK GRAFF, Bureau Chief Privacy Officer

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

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2020.08.13 17:09:24 -05'00' 08/13/2020

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

U.S. Department of Commerce
Privacy Impact Assessment
NOAA6101
Office for Coastal Management

Unique Project Identifier: 06-48-02-00-01-0511-00

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

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

NOAA6101 is a general support system used to ensure that the Office for Coastal Management's (OCM's) programmatic and internal administrative operational needs are met. The system is an integrated collection of subsystems designed to provide general office automation, infrastructure, and connectivity services for the National Oceanic and Atmospheric Administration's (NOAA) Office for Coastal Management (OCM).

(b) System location

Federal Law Enforcement Training Center (FLETC), North Charleston, SC
NOAA Inouye Regional Center (IRC), Honolulu, HI
Stennis Space Center, MS
Ronald V. Dellums Federal Building, Oakland, CA
Silver Spring Metro Center (SSMC), Silver Spring, MD
Microsoft Azure - US East 2, US Central

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

This is a standalone system

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

NOAA6101 groups elements of the system into three areas, each of which serves a distinct and specific function:

- Network Devices -- NOS/OCM Wide Area Network (WAN) and OCM Wide Area Network.
- NOS Domain Servers -- The NOS domain infrastructure components and OCM Local Area Network (File, Print, Application) services.
- Web Application Servers -- OCM application and database hosting services

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

The information is retrieved through an application user interface, except for the data that is kept on the shared drives. Public access of information is provided by web application interfaces.

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

PII is manually entered into the system by the administrator or through a bulk upload from a spreadsheet(s).

Social Security numbers are collected for new NOAA/NOS/OCM employees. These are transmitted to the NOAA Security Office via secure electronic transmission and then destroyed. OCM does not maintain them on the IT system or as hard copy files. Passport numbers are handled in the same way as SSNs. Taxpayer or employer ID information is collected infrequently (see section 5.1 for more details), but is stored only temporarily on the system.

POC information is entered into various applications/web sites as detailed in Section 5 below. This POC information generally consists of name, email, phone number, organization name, and is collected for the following reasons (not exhaustive, and not applicable to each application/site - see Section 5 for specific details):

- preparing collaborative partner project plans
- requesting delivery of data or information
- posting of subject matter expert contact information
- requesting training
- managing task order information
- joining webinars

(g) Any information sharing conducted by the system

Visitor information is shared on a case-by-case basis with the Federal Law Enforcement Training Center in Charleston, SC per the Foreign National Visitor Process. Information is shared within the bureau on a case-by-case basis. Information is shared directly with the public only non-sensitive point of contact information is shared, typically for subject matter experts who have agreed to share this information who have agreed to share this information.

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

The general legislation supporting the system is 5 U.S.C.301, one of the statutes concerning government organization and employees.

From Coastal Zone Management Act - 16 USC 1456; Coordination and cooperation

From Coral Reef Conservation Act - 16 USC 6401

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

From NOAA-12: Marine Mammals, Endangered and Threatened Species/Permits and Authorizations.

From NOAA-13: Personnel, Payroll, Travel, and Attendance Records of the Regional Fishery Management Councils.

From NOAA-21, Financial Services Division.

From COMMERCE/DEPT-2: Accounts Receivable.

From DEPARTMENT-5: Freedom of Information and Privacy Request Records.

From DEPARTMENT-6: Visitor Logs and Permits for Facilities under Department Control.

From DEPARTMENT-7: Employee Accident Reports.

From DEPARTMENT-12: OIG Investigative Records.

From DEPARTMENT-13: Investigative and Security Records

From DEPARTMENT-14: Litigation, Claims, and Administrative Proceeding Records.

From DEPARTMENT -18: Employees Personnel Files Not Covered by Notices of Other Agencies. Includes the following, with all revisions and amendments: 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.

From DEPARTMENT -25: Access Control and Identity Management System. 5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075.

From GSA/GOVT-7: Personal Identity Verification Identity Management System.5 U.S.C. 301; Federal Information Security Management Act of 2002 (44 U.S.C. 3554); E-Government Act of 2002 (Pub. L. 107–347, Sec. 203); Government Paperwork Elimination Act (Pub. L. 105–277, 44 U.S.C. 3504 note); Homeland Security Presidential Directive 12 (HSPD–12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

From OPM/GOVT-1: General Personnel Records. 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

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

Moderate

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

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

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

_____This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

__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).

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

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*	X	f. Driver's License		j. Financial Account	
b. Taxpayer ID	X	g. Passport	X	k. Financial Transaction	
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					

*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

Social Security numbers are collected for new NOAA/NOS/OCM employees. These are transmitted to the NOAA Security Office via secure electronic transmission and then destroyed. OCM does not maintain them on the IT system or as hard copy files. Passport numbers are handled in the same way as SSNs. These procedures are detailed in the OCM Standard Operating Procedure-Personnel Security. This SOP will be included/referenced in the NOAA 6101 System Security Plan. Taxpayer or employer ID information is collected infrequently (see section 5.1 for more details), but is stored only temporarily on the system.

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship	X	n. Religion			

u. Other general personal data (specify):
Employee information is collected for emergency/disaster/CoOP related contact needs. General inquiries related to information sharing consist of collecting name and email address in order to respond to the information requests.

Gender, Age, and Citizenship are only collected in hard copy forms for foreign visitors to OCM Charleston office and provided to DHS/FLETC in Charleston.

Various web pages/sites throughout the system collect POC data for information sharing purposes. These are listed below in Section 5.1.

Certain subject matter experts agree explicitly to share contact information (name, phone, email) on OCM's public web site. These are listed below in Section 5.1.

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	X
b. Job Title	X	f. Salary		j. Proprietary or Business Information	X
c. Work Address	X	g. Work History			
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		
k. Other work-related data (specify): Work related data is collected and shared with employees for internal office communication purposes. Additionally, grant information or contract proposals often contain PII/BII, such as budgets/costs; this information is only accessible to those involved in specific work activities, and only on a need-to-know basis. Additionally, all financial transactions take place outside of the OCM system (i.e., NOAA Finance, Grants Online handle financial transactions). General contact information is collected and/or shared on OCM websites for public comments, training, grant proposal preparation, partner points of contact, project and task management, and reference documents. See section 5.1 below for more details.					

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	X	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	
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)
Server logs collect IP addresses, Date and time of access for IT Administration purposes.
Building Entry Readers: Information is captured for physical access to OCM buildings.

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	x
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):					

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

PII in the system is reviewed by OCM staff upon entry and users can review for accuracy and update or request their information be removed from the system.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0648-0121 Management and Oversight of the National Estuarine Research Reserve System 0648-0448 Coral Reef Conservation Program Administration 0648-0145 Deep Seabed Mining Regulations for Exploration Licenses 0648-0646 Socioeconomics of Coral Reef Conservation 0648-0459 Coastal and Estuarine Land Conservation, Planning, Protection, or Restoration 0648-0779 Availability and application of socioeconomic data in resource management in the U.S. Pacific Islands. (Awareness & Application of Long-Term Monitoring Data in the Pacific Islands) 0648-0119 Coastal Zone Management Program Administration 0648-0411 Paperwork Submissions Under the Coastal Zone Management Act Federal Consistency Requirements 0648-0661 Evaluations of Coastal Zone Management Act Programs – State Coastal Management Programs and National Estuarine Research Reserves
	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	x	Building entry readers	X
Video surveillance	x	Electronic purchase transactions	

Other (specify):

Audio recordings: Virtual Conferencing and Webinars - Adobe Connect is being used for virtual meetings and webinars. Recorded webinars are stored on Adobe site, and when appropriate (i.e. trainings and webinars) published for later viewing.

Video Surveillance: Video monitoring occurs in the Charleston, SC office at the front door. The video is streamed to an individual's desk for monitoring, but the data is not recorded, saved, or stored.

Building Entry Readers: Information is captured for physical access to OCM buildings.

Section 4: Purpose of the System

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

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	

Other (specify):

Google Analytics is used for web measurement technologies. All traffic sent to Google Analytics is anonymized per the GSA policy. So, no PII is collected for web measurement technologies.

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).

PII is collected to communicate with OCM customers and stakeholders on topics where they have an explicitly expressed professional interest, or have made a specific request for data or information.

Other PII is collected for OCM staff employment and personnel records (federal/contractor) and OCM visitor access information (federal/contractor/member of the public/foreign national).

BII is collected and maintained for purposes such as contractual agreements and grants.

Details are found below.

NOAA's Office for Coastal Management Business Operations Division collects data containing personally identifiable and business identifiable information (BII) for internal government operations / administrative processes. The processes include:

- Employee / Contractor information needed for personnel, performance evaluation, merit rewards, training, travel, accident reporting, etc. This type of PII information is reviewed and updated annually by staff.
- Employee / Contractor / Visitors / Foreign National information required by DOC and/or OPM for security purposes and/or background checks. Passport numbers are collected for foreign visitors, sent as appropriate for security checks, and removed from the system. All information is required per DOC PII Policy and Foreign National Processing guidance, as well as the Federal Law Enforcement Training Center (FLETC) Foreign National Visitor Process.
- Employee / Contractor emergency contact information for use in call trees and Continuity of Operations Plan (CoOP), which includes names, phone numbers, and addresses
- Applicant information submitted in response to requests for proposals and/or in response to a solicitation. External grant applications/proposals are not typically collected by OCM. Per the NOAA Grants Management Office policy, proposals almost always run through the Grants.gov submission process and end up in the Grants Online system. In rare cases, applicants without access to the Internet [e.g., US Territories] are permitted to submit paper applications. When this happens, OCM scans the proposals and loads them into Grants Online. Any subsequent sharing of grant proposals via email for review must be done via a secure file transfer process (e.g., Grants Online, Accellion/Kiteworks if emailing internally or externally to NOAA, a secure Google Drive or a network location for internal NOAA reviewers, or a password protected website for internal and external NOAA reviewers). Once reviews are complete and awards are made, proposals are removed from the OCM system and the Grants Online system is the official repository.

Typical personal or business identifiable information collected for grant applications includes:

- proposer's name
- email
- phone #
- organization name
- organization DUNS #
- employer identification number or taxpayer identification number

For acquisitions, the business identifiable information collected typically includes:

- proposer's name
- email
- phone #
- organization name
- organization DUNS #
- Cost proposal information is also collected, and would be considered BII, as it is often proprietary.
- Management and technical approaches found in vendor proposals is often considered BII.

Other PII that is being collected and/or made available via Internet / Web sites or applications include the following.
(Any personal information on any of the following sites is entirely voluntary and can be removed by request at any time.)

- CAMMP: Version 2 (V2) is currently (June 1, 2020) under development with a release date in August 2020. Version 1 (V1) will be no longer accessible when V2 is released.
    - V2: Application that allows for collaborative project planning with partners (state CZM and NERRS). Data collected includes names, title, email, and budget.)
    - V1: Application that allows for collaborative project planning with partners (state CZM and NERRS). Data collected includes names, title, email, and budget.)
- Coastal Zone Management Act Program Changes is an application where proposed State CZM Program changes are posted for public comment. Information collected includes name, affiliation, email address, city, state, zip, comments. Email address is collected to verify a user exists and a two step authentication process is in place to make sure the user receives an email before comments are posted.
- Coral Database: Application that collects internal NOAA staff proposals to the NOAA Corals matrix program.

- Data Access Viewer (DAV): Application that receives requests for data from the public. Email addresses are stored to provide a method of contacting the requester when the data is ready for pickup on the OCM FTP site.
- Digital Coast: Publishes contact information of trainers for some trainings listed on the Digital Coast Training page. Information includes name, email, and location. Permission is acquired (via a form) from each trainer before listing their information on the site.
- Estuaries Education: Website that publicly lists some partner organization POCs (name, organization, email, phone number), along with OCM POCs. POC information is entirely voluntary and can be removed at any time upon request.
- Green Infrastructure Database is a catalog of literature resources documenting the effectiveness of using green infrastructure to reduce impacts from coastal hazards. Information published includes study authors as typical with standard citations.
- NERRs and State Coastal Zone Management (CZM) Performance Measures Databases are authenticated applications for NERRs and CZM partners to document grant performance measures in a standardized way, and to work collaboratively with OCM staff. Information collected includes name, organization, email, and phone number.
- National Estuarine Research Reserves (NERRS): Website that publicly lists some partner organization POCs (name, organization, email, phone number), along with OCM POCs. POC information is entirely voluntary and can be removed at any time upon request.
- OCM Intranet (Inet): Contains current information on staff, including phone numbers, names, email addresses, and emergency contacts. The system is used to maintain up to date records on staff contact information.
- OCM Staff Info - Contact information for OCM staff. Information published includes name, email and phone number.
- Ocean Law Search: Web site related to underwater cultural heritage that makes various public laws, statutes, articles, and court case summaries available via an online searchable interface. All of the information available is publicly accessible and has been assembled to focus on underwater cultural heritage. Some of the documents available contain names and addresses of legislators, attorneys, plaintiffs, or witnesses.
- PRiMO: Web site that publicly lists some partner organization POCs (name, organization, email, phone number, photos), along with OCM POCs. POC information is entirely voluntary and can be removed at any time upon request.
- Task Order Management Information System (TOMIS): Version 2 (V2) is currently under development with a release date in July 2020. Version 1 (V1) will be no longer accessible when V2 is released.
    - V2: Application that collects and maintains POC information (name, email, phone, company name) for use in administering various contractor tasks and deliverables. Note, contractor evaluations will not be migrated to the new site

or database.

- V1: Application that collects and maintains POC information (name, email, phone, company name, contractor evaluations) for use in administering various contractor tasks and deliverables. After migration to V2, the V1 DB will be backed up, encrypted and taken offline. Contractor evaluations will be deleted and will not be backed up as part of the database archiving process.

- Training Manager System: Web site that collects information on training courses, hosts, and participants of OCM training programs. Information that is collected is not shared publicly. Fields collected include (name, organization, address, city, state, zip, email, phone).
- Virtual Conferencing and Webinars - Adobe Connect is being used for virtual meetings and webinars. Recorded webinars are stored on Adobe site. Attendee information is anonymized when saved for republishing.
- Still images and video on web sites, online newsletters, video streaming, to fulfill OCM's mission to provide coastal information to interested stakeholders and the general-public. Images and video with identified individuals are searchable when included on web pages with descriptive text of the person in the image or video. People who are identified in images and videos will be required to submit the POC Consent Form.

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.)

Threats

- If users print information from the system, there is a chance that privacy data will be viewed if the document is left in plain sight.
- There is a potential for unauthorized access to the system, which would expose non-sensitive PII to an unauthorized user.

Controls

- Users take privacy training at least annually in the required annual security awareness course.
- Users take Controlled Unclassified Information (CUI) course annually
- Users sign rules of behavior to ensure they understand their responsibilities.
- OCM follows records retention schedules as noted in Section 10 below. Manual review and manual purging of records occurs per these schedules or as noted in

Section 10. In addition, as stated in Section 7, individuals with PII in the system can request a review and/or removal of individual PII at any time. Please see Section 7 for specific details.

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			
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			X (only non-sensitive, point of contact information is shared, typically for subject matter experts who have agreed to share this information)
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

* DHS FLETC for verification of foreign visitor identity.

	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 Act statement and/or privacy policy can be found at: • CAMMP (https://coast.noaa.gov/cammp/) (V2 will have User Management Privacy Act Statement on login page) • Coastal Management Fellows Contacts (https://coast.noaa.gov/fellowship/Directory/alphabetical.html) (Privacy Policy link in footer) • Coastal Zone Management Program Change Public Comments Form (https://coast.noaa.gov/czmprogramchange/#/public/change-view/1230) (Privacy Act Statement linked on top of public comments form) • CZM Performance Measure tracking system (https://coast.noaa.gov/czmpm/ - access is restricted) (Privacy Act Statement is provided on the login page.) • Corals DB (https://inet.coast.noaa.gov/coral/) (Privacy Act Statement on login page) • Data Access Viewer (https://coast.noaa.gov/dataviewer/) (Privacy Act Statement on request submission form) • Digital Coast Training Section Host This Course form (https://coast.noaa.gov/digitalcoast/training/ecosystem-services.html) (Privacy Act Statement link to contact us statement) • Estuary Education Volunteer Contacts (https://coast.noaa.gov/estuaries/news/volunteer.html) (Privacy Act Statement included on consent form) • Green Infrastucture Effectiveness Database (https://coast.noaa.gov/gisearch/#/search) (Privacy Policy in Footer) • National Estuarine Research Reserves - Reserve Profiles (https://coast.noaa.gov/nerrs/reserves/wells.html) (Privacy Policy in Footer) • NERRs Intranet (https://coast.noaa.gov/nerrsintranet/) (Privacy Act Statement is provided on the login page.) • NERRS Performance Measure tracking system (https://coast.noaa.gov/nerrspm/) (Privacy Act Statement is provided on the login page.) • Ocean Law Search (https://coast.noaa.gov/oceanlawsearch/#/search) (Privacy Policy in footer) • OCM Contact Form (https://coast.noaa.gov/contactform/) (Privacy Act Statement linked at bottom of form)

	• OCM Intranet (https://inet.coast.noaa.gov/ - access is restricted) (Privacy Act Statement is linked at top of employee update form) • OCM Partner Contact Information Sharing Consent Form (https://drive.google.com/drive/folders/0Bx8TMwCZRex9Zi1DV1ZCV2pyY0E - access is restricted) (Privacy Act Statement is the on form provided to partners when they consent to publishing their information on OCM website(s)) • OCM Staff Directory (https://coast.noaa.gov/about/staff/) (Privacy Policy in footer, Staff sees Privacy Act Statement in INET when updating contact info annually) • PRiMO leadership page (https://coast.noaa.gov/primo/about/leadership.html) (Privacy Policy in footer, POC consent form for users on page) • Still Images and Video on websites (Privacy Policy link in footer, POC consent form for people identified in images and videos.) • TOMIS V2 (https://coast.noaa.gov/tomis/) (Privacy Act Statement on login) • Training Management System (https://coast.noaa.gov/trainingmanager/login/) (Privacy Policy in footer, POC consent form with Privacy Act Statement linked in course participants section) • Virtual Conferencing and Webinars (via Adobe Connect) (Adding Privacy Act Statement link to Adobe Connect Registration page with confirmation checkbox) The privacy policy is linked in footers of every page and can be found at: https://coast.noaa.gov/PrivacyPolicy/privacyPolicy.html .	
X	Yes, notice is provided by other means.	Specify how: Subject matter experts often provide contact information via the OCM public website. Prior to making the POC information public, the subject matter experts are asked to fill out a form acknowledging that they will be providing this information on a public web site and that they agree to do so. A Privacy Act Statement is also made available on the form. Visitors to the OCM web presence can request information by providing minimal PII through an information request contact form. Individuals are under no obligation to provide this information, and the details of how this information is handled are readily available via the OCM Privacy Policy and a Privacy Act statement. OCM staff members (employees) are provided notice of how PII is used (i.e., emergency contact information in case of natural disasters) upon hire

		and when annually updating personal information in the OCM INET employee update form. Partners/grantees may provide contact information (PII) to participate in the NERRs Intranet site established for collaboration and to enter data into grantee performance measurement tracking systems. Vendors and grantees are notified via solicitations and calls for proposals that BII will be collected as necessary to effectively evaluate proposals.
	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: Subject matter experts often provide contact information via the OCM public website. Prior to making the POC information public, the subject matter experts are asked to fill out a form acknowledging that they will be providing this information on a public web site and that they agree to do so; all have the opportunity to decline to provide PII as it is an "opt in" scenario. A Privacy Act statement is also made available. Visitors to the OCM web presence can request information by providing minimal PII through an information request contact form. Individuals are under no obligation to provide this information, and the details of how this information is handled are readily available via the OCM Privacy Policy and a Privacy Act statement. Staff members provide PII upon hire as a condition of employment. A Privacy Act statement concerning usage of this information is made available to OCM staff members. They may decline to provide PII but this may affect their employment status. <u>Site specific details:</u> CAMMP – Staff and partners are required to have accounts to access internal documents and update task order status. Partners/grantees may provide contact information (PII) to participate in grants application

		preparation systems. Partners can decline to provide this information as it is an "opt in" scenario. Coastal Management Fellowship Contacts – No data entry, this is a directory of names. A fellow could request to have their information removed from the site. They can also decline to publish their info in the POC sharing consent form. Coastal Zone Management Act Program Changes – Visitors to the site have the ability to submit public comments. This is voluntary or "opt in" for the users. The users are required to submit basic PII contact information and an email address for validating the comment. The details of how this information is handled are readily available via the OCM Privacy Policy and a Privacy Act statement at the top of the form. Coral Database – Restricted access site. If user information is not provided, users can't login to the site to manage projects. Data Access Viewer (DAV) – Downloading data only requires the user to submit an email address. That email address could be a temporary or anonymous account. Digital Coast – Registration for live online courses and webinars require contact information. Courses are provided afterward in an on-demand self-guided version if people don't want to register. (Example: see additional information section https://coast.noaa.gov/digitalcoast/training/risk-communication.html). Estuaries Education – No data entry allowed. Education Volunteer Coordinator's contact info is provided, but some states have generic contact info (i.e.: Delaware – info@nerra.org). If a volunteer coordinator wishes to remove their contact info, they can use a generic contact email address. Green Infrastructure Database - No data entry. All information listed in this database is from publicly available literature. National Estuarine Research Reserves (NERRS) –

		No data entry. NERRS staff and contributors are listed in the reserve site profile. Staff and Contributors could request to have their information removed from the contact us link at the bottom of every page. NERRs Performance Measures Database – Restricted access site. Information used for access to performance measurement tracking and administrative purposes. Partners/grantees may provide contact information (PII) to participate in grantee performance measurement tracking systems. Partners can decline to provide this information as it is an "opt in" scenario. Ocean Law Search – No data entry available. Site consists of publicly available legal documents. OCM Intranet (Inet) – Staff are required to have accounts to access internal documents. If they decline to provide information, users cannot use the system. OCM Staff Info – No data entry available, staff directory is from INET staff contact database. PRiMO – No data entry, partners can request to have their information removed from the site. They can also decline to publish their info in the POC sharing consent form. State Coastal Zone Management (CZM) Performance Measures Database - Restricted access site. Information used for access to performance measurement tracking and administrative purposes. Partners/grantees may provide contact information (PII) to participate in grantee performance measurement tracking systems. Partners can decline to provide this information as it is an "opt in" scenario. Still images and video – A subject in a picture or video can request to have the image or video removed. The request can be made via the Contact Us form which is in the footer of every page. They can also refuse when asked to submit the POC consent form. Task Order Management Information System

		(TOMIS) – Staff and contractors are required to have accounts to access internal documents and update task order status. Vendors and/or grantees provide BII when submitting proposals of various types. Proposers may decline to provide BII, by not including it in their proposals; however, that declination effectively removes them from consideration of contract or grant awards, as there are certain types of information that contain BII that are essential to a full and valid competition. Training Manager System – This is a restricted site. Course registrants are required to submit minimal information to take a course. Non-OCM course participants are required to submit the PII Disclosure Agreement form. Virtual Conferencing and Webinars (Adobe Connect) – Virtual Conferences require minimal PII to register for courses and webinars. If a user declines to register, the courses are typically provided for on-demand viewing after the course/webinar has completed.
	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: Subject matter experts who may be asked or offer to provide contact information are informed of exactly how and where on the OCM web site their contact information will be made available. A Privacy Act statement for this type of scenario is also available. Visitors to the OCM web presence can learn how PII is used via the OCM Privacy Policy and make the choice to opt in to the particular stated uses. A Privacy Act statement for this type of scenario is also available. Staff members provide PII upon hire as a condition of employment. They may consent to only particular

		uses, but this may affect their employment. A Privacy Act statement for this type of scenario is also available. Partners/grantees who provide contact information (PII) to participate in the NERRs Intranet site established for collaboration or to enter data into grantee performance measurement tracking systems opt in to providing PII for the particular stated uses. For vendors and grantees, the only usage of the BII is during proposal review and subsequent consultation with vendors or grantees. The BII is not shared or disseminated beyond this scope. <u>Site specific details:</u> CAMMP – Staff and partners are required to have accounts to access internal documents and prepare grant applications. Partners/grantees may provide contact information (PII) to participate in grants application preparation systems. Partners can decline to provide this information as it is an "opt in" scenario. User consent for PII is limited to the CAMMP application. Coastal Management Fellowship Contacts – No data entry involved in this. The fellow's contacts and project descriptions are consented by accepting the Fellowship, just as an employee would with employment. Coastal Zone Management Act Program Changes – Visitors to the OCM web presence can learn how PII is used via the OCM Privacy Policy and make the choice to opt in to the particular stated uses. A Privacy Act statement for this type of scenario is also available. Coral Database – This is a restricted access NOAA staff only application. Staff members provide PII upon hire as a condition of employment. They may consent to only particular uses, but this may affect their employment. A Privacy Act statement for this type of scenario is also available. Data Access Viewer (DAV) – Visitors to the Data Access Viewer are required to submit their email

		address for sending the data. They are also provided with an option to sign up for email lists. Digital Coast –Subject matter experts who may be asked or offer to provide contact information are informed of exactly how and where on the OCM website their contact information will be made available. The consent is provided by the POC consent form. A Privacy Act statement for this type of scenario is also available on the consent form. Estuaries Education – Subject matter experts who may be asked or offer to provide contact information are informed of exactly how and where on the OCM web site their contact information will be made available. They consent to that use via the POC Sharing Form. A Privacy Act statement for this type of scenario is also available. Green Infrastructure Database - There is no data entry or PII created to end users. This is a database of publicly available scholarly papers. National Estuarine Research Reserves (NERRS) – NERRS does not provide data entry capabilities. There are reserve profiles that list staff and contributors to the profile. Anyone listed on the Reserve Profiles can request that their info be removed through the Contact Us form linked in the bottom of every page. NERRs Performance Measures Database – Partners/grantees who provide contact information (PII) to participate in the NERRs Intranet site established for collaboration or to enter data into grantee performance measurement tracking systems opt in to providing PII for the particular stated uses. Ocean Law Search – There is no data entry or PII created to end users. This is a database of publicly available legal documents. OCM Intranet (Inet) – This is a restricted access for NOAA staff only application. Staff members provide PII upon hire as a condition of employment. They may consent to only particular

		uses, but this may affect their employment. A Privacy Act statement for this type of scenario is also available. OCM Staff Info – This is a staff contact directory. Staff members provide PII upon hire as a condition of employment. PRiMO – Partners and Subject matter experts who may be asked or offer to provide contact information are informed of exactly how and where on the OCM web site their contact information will be made available. A Privacy Act statement for this type of scenario is also available. State Coastal Zone Management (CZM) Performance Measures Database - Partners/grantees who provide contact information (PII) to participate in the State CZM Performance Measurement Database site established for collaboration or to enter data into grantee performance measurement tracking systems opt in to providing PII for the particular stated uses. Still images and video – Employees and partners identified in still images or videos will be asked to submit the POC consent form. Task Order Management Information System (TOMIS) – Employees, partners and contractors who provide contact information (PII) to participate in the TOMIS site established for collaboration or to task order management systems opt in to providing PII for the particular stated uses. Training Manager System – This is a restricted access for NOAA staff only application. Staff members provide PII upon hire as a condition of employment. They may consent to only particular uses, but this may affect their employment. A Privacy Act statement for this type of scenario is also available. Virtual Conferencing and Webinars (Adobe Connect) – Visitors to the OCM web presence can learn how PII is used via the OCM Privacy Policy and make the choice to opt in to the particular

		stated uses. Virtual Conferencing require minimal PII to register for courses and webinars. If a user declines to register, the courses are typically provided for on-demand viewing after the course/webinar has completed. Attendees are also notified that the session is being recorded and will be posted to the internet.
	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: Subject matter experts who provide contact information on the OCM website can review, update, or delete their PII upon request at any time. Web site visitors who provide PII via a request for information can request to review, update or delete the PII provided at any time. Staff members can update PII during performance reviews or via secure Intranet. Partners/grantees who provide contact information (PII) to participate in the NERRs Intranet site established for collaboration or to enter data into grantee performance measurement tracking systems can review, update, or delete their PII upon request at any time. Vendors or grantees can review/update BII at any time upon request to the NOS proposal contact. <u>Site specific details</u>: CAMMP – Users can review their account information and grant application preparation materials in their user profile. Coastal Management Fellowship Contacts – Fellows can review the information on the web page and request modifications via the contact us page linked at the bottom of every page.

		Coastal Zone Management Act Program Changes – These are public comments relating to rule/law changes. As a result, users cannot change information they entered. NOAA staff moderate all comments prior to publishing. If a user submitted something they wanted to change, they could contact the comment moderators to have them reject publishing the comment. Coral Database – Users can review and update their account information in their user profile at any time. Data Access Viewer (DAV) – Users only enter email address for delivery of data link. They have the option to sign up for NOAA OCM mailing lists when they request data. Mailing list emails have the option to unsubscribe on each email Digital Coast – Subject matter experts who provide contact information on the OCM website can review, update, or delete their PII upon request at any time. Estuaries Education – Volunteer coordinators who provide contact information on the OCM website can review, update, or delete their PII upon request at any time. Green Infrastructure Database - Per rights in the Privacy Act, users who have information listed in the scholarly articles hosted in the Green Infrastructure Database may submit a Privacy Act request to Dept of Commerce FOIA/Privacy Act Staff. This information is linked in the OCM Privacy Policy. They can also request their info be removed or modified using the Contact Us link at the bottom of every page. National Estuarine Research Reserves (NERRS) – Subject matter experts who provide contact information on the OCM website can review, update, or delete their PII upon request at any time. NERRs Performance Measures Database – Users can review and edit their account information and performance measures at any time. Ocean Law Search – Per rights in the Privacy Act, users who have information listed in the legal documents hosted in Ocean Law Search may submit a

		Privacy Act request to Dept of Commerce FOIA/Privacy Act Staff. This link is in the OCM Privacy Policy. OCM Intranet (Inet) – Staff members can update PII during performance reviews or via secure Intranet. OCM Staff Info – Staff members can update PII during performance reviews or via secure Intranet. PRiMO – Subject matter experts who provide contact information on the OCM website can review, update, or delete their PII upon request at any time. State Coastal Zone Management (CZM) Performance Measures Database - Users can review and edit their account information and performance measures at any time. Still images and video - The individuals can contact OCM using the Contact Us link on every page to have their images removed from video on web sites, online newsletters. Task Order Management Information System (TOMIS) – This is a restricted access site. Users can review and update their contact information at any time in the user profile. If a user's information is tied to task order documents, that information cannot be removed for contract compliance purposes. Training Manager System – This is a restricted access site. NOAA staff login with their ICAM login, they can update their ICAM contact information in that system. Participants who took part in a training course, can request that their information be modified or removed from the participant list by request using the Contact Us link on every page. Virtual Conferencing and Webinars (Adobe Connect) – Participants in Adobe Connect webinars have their names anonymized before the webinar is available for later viewing. If participant video module was used during the meeting, that module is removed prior to publishing for later viewing.

	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 forms of electronic PII/BII is monitored, tracked and recorded with role based access controls in place on the system.
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): August 23, 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).

Secured database

- OCM secures PII data into a SQL (2016) Server database on a secured server. Databases are only accessible based on least privilege and job requirements. Access is limited to SQL Administrators and IT Staff that are authorized for administrative system access. The servers hosting the aforementioned databases exist in an access controlled internally hosted data center where physical access is monitored and granted exclusively based on position responsibilities. Non-privileged users are restricted to access via SQL Server accounts only. Information placed in the database is only accessed on a need-to-know basis by internal staff who are identified as needing access to this information.

Secured file/folder network directory

- OCM enforces assigned authorizations for controlling access to the system through the

use of logical access control policies. Access controls lists are configured to enforce access authorization and assign user and group privileges. These access control policies are employed to control the access between users and objects (files, directories, servers, printers, etc.). Access enforcement mechanisms are in place at the network, system and application levels. Sensitive information is protected in transit and that no sensitive information is maintained on the system.

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.

- Certain instances of PII in NOAA6101 are searchable by name.

____ 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)*: Existing Privacy Act system of records notices (SORNs) for NOAA cover the personnel information in this system: • COMMERCE/DEPARTMENT-2, Accounts Receivable • DEPARTMENT-5, Freedom of Information and Privacy Request Records • DEPARTMENT-6, Visitor Logs and Permits for Facilities under Department Control • DEPARTMENT-7, Employee Accident Reports • DEPARTMENT-12, OIG Investigative Records • DEPARTMENT-13, Investigative and Security Records • DEPARTMET 14, Litigation, Claims, and Administrative Proceeding Records • DEPARTMENT-18 - Employees Personnel Files Not Covered by Notices of Other Agencies • DEPARTMENT-25, Access Control and Identity Management System

	• GSA/GOVT-7, Personal Identity Verification Identity Management System. • NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission • NOAA-12, Marine Mammals, Endangered and Threatened Species/Permits and Authorizations • NOAA-13, Personnel, Payroll, Travel, and Attendance Records of the Regional Fishery Management Councils • NOAA-21, Financial Services Division • OPM/GOVT-1, General Personnel Records
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: The retention period of these records is guided by the General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) (see https://www.archives.gov/records-mgmt/grs.html) to provide disposition authorization for records common to several or all agencies of the federal government. In accordance with NARA GRS Title 2.1 – 2.7, 3.1, 3.2, 4.1 and 4.3 electronic versions of records scheduled for disposal may be deleted at the expiration of the retention period authorized by the GRS of for the equivalent paper copies or when no longer needed, whichever is later. In accordance with NARA GRS Title 3.1, 3.2, 4.1 and 4.3, the data is presently being retained indefinitely. NOAA Records Schedules 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. 1610-01 - Coastal Zone Management Program Documents 1610-02 - Program Change Files 1610-03 - Coastal Non-point Pollution Control Program 1610-04 - Federal Consistency 1610-05 - Program Administrative Guidance

	1610-06 - The Coastal and Marine Management Program Information System NOAA Records Schedules Chapter 2300 applies to OCM's internal records related to IT and software development. OCM typically does not remove these records, but preserves them in perpetuity. NOAA Records Schedules Chapter 2400-Information System Security Records, provides guidance on records created and maintained by OCM and is related to protecting the security of IT systems and data, and responding to computer security incidents.
	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	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels.
(Check all that apply.)

X	Identifiability	Provide explanation: OCM only collects non-sensitive PII such as phone

		numbers and e-mail addresses. No SSNs or other sensitive PII/BIA information is electronically stored. CAMMP – Restricted access site. System user name, First Name, Last Name, Email, Address, Phone Number, Organization Name, EIN/TIN/DUNS number Coastal Management Fellowship Contacts – First Name, Last Name, Email, Organization Coastal Zone Management Act Program Changes – System Username, First Name, Last Name, Affiliation, Email, City, State, Zip Coral Database – ICAM Username, First Name, Last Name, Email, Organization Data Access Viewer (DAV) – Email, Organization Digital Coast – Training Partners Case Studies - Subject Matter Experts - Picture, First Name, Last Name, Email, Organization - Training Webinars - Videos - Presenters Name(s), Organization Estuaries Education – Volunteer Coordinator Names and Email Green Infrastructure Database - Links to scholarly articles Author(s) First Name, Last Name in citation. National Estuarine Research Reserves (NERRS) – Names of authors, editors, contributors. NERRs Performance Measures Database – Restricted access site. Username, First Name, Last Name, Email Ocean Law Search – Names and professional titles listed in legal briefs OCM Intranet (Inet) – Restricted access site. User names, First Name, Last Name, Email, Job Title, Phone Number, Business Address, Organization, Birth Month and Day, Manager Names. (Not visible to staff beyond management is Emergency Contact Information and Home Address) OCM Staff Info – Staff contact list - First Name, Last Name, Email, Phone Number, Upper Management

		Roles and Profiles with Pictures. PRiMO – Leadership First Name, Last Name, Title, Organization, Picture, Conference Programs with presenter names and abstracts. State Coastal Zone Management (CZM) Performance Measures Database - Restricted access site. Username, First Name, Last Name, Email TOMIS – First Name, Last name, Organization, Email, Phone Number Training Manager System – Training Host (Name, Email, Phone, Organization), Facility Contact (Name, Address, Email), Training Participants (Name, Email, Zipcode) Virtual Conferencing and Webinars (Adobe Connect) – First Name, Last Name, Email, State, Zip, County, Organization
X	Quantity of PII	Provide explanation: Information collected is limited to a small subset of specific applications and personnel files. CAMMP – 265 System User (68 NOAA users, 197 External Users) Coastal Management Fellowship Contacts – 129 Fellows listed in directory Coastal Zone Management Act Program Changes – 56 total users (19 NOAA staff, 37 State CZM staff) with access to the admin section. No public comments on public site, yet. Coral Database – 456 NOAA staff system user accounts and project members. Data Access Viewer (DAV) – 262,629 download requests according to DAV Data report. Not all are unique email addresses. Digital Coast – 165 Subject matter experts and training presenters. Estuaries Education – 28 Coordinators contact information listed.

		Green Infrastructure Database - 237 scholarly article citations with multiple authors each. National Estuarine Research Reserves (NERRS) – 30 NERRS reserves site profile documents with varying number of authors, editors, and contributors names. NERRs Performance Measures Database – 66 NOAA users, 219 Partner user accounts Ocean Law Search – Several hundred documents, including: Court Documents, International Law, Law Articles, Legislative History Documents, Press Releases, Case Summaries, Summary of Law and Legislative History. Each with a varying number of persons mentioned. OCM Intranet (Inet) – 304 Employee Records OCM Staff Info – 304 Employee Records PRiMO – 32 Leadership names and photos, 17 Conference Programs with varying number of presenters information. State Coastal Zone Management (CZM) Performance Measures Database - 87 NOAA Employee users, 129 External Partner Users TOMIS – 800 active and inactive accounts with user contact information. Training Manager System – 1060 planned courses, of which 630 were completed with participant lists. An average of 24 paricipants per class in a random sampling. Virtual Conferencing and Webinars (Adobe Connect) – There are approximately 3,000 unique attendees registered for approximately 600 meetings. Many attendees have registered for multiple meetings.
X	Data Field Sensitivity	Provide explanation: Phone numbers and e-mail addresses are the primary information collected, and are used for communication purposes.
X	Context of Use	Provide explanation: The vast majority of PII collected is used for emergency contact information for staff members, or for communicating back to information requesters.

		CAMMP – Users accounts are created by project administrator as necessary. Grant applications prepared by potential grantees voluntarily. Coastal Management Fellowship Contacts –Fellows added to directory when they are awarded fellowship. Coastal Zone Management Act Program Changes – State CZM User accounts are used for submitting proposed State CZM rules. NOAA accounts are used for verifying the proposals are ready to be published and for verifying public comments are real submissions. Public citizens submit public comments voluntarily, contact information is for verification of authentic users. Coral Database – Projects and Deliverables tracking with users associated with each project and deliverable. Data Access Viewer (DAV) – Email addresses are used to send a link to data requestors after the requested data has been processed. Email addresses are never published publicly, but are maintained in the database. Digital Coast – Subject matter experts and training presenters' names, email and organization are listed on cast study pages and webinar description pages. Estuaries Education – Contact information is listed for each state's NERRS volunteer coordinators on the estuary resources page. Green Infrastructure Database - The database provides a search engine of scholarly articles on Green Infrastructure. Each record has citations for the link to the article, which include authors' names. National Estuarine Research Reserves (NERRS) – NERRS Reserves each contain a site profile document which was published by each reserve. The documents contain a varying number of authors, editors, and contributors' names and organizations. NERRs Performance Measures Database – User accounts are used for managing project performance measures and partnership linkages in projects.

		Ocean Law Search – Legal documents used for research on Ocean Law. The documents contain listings of Lawyers, Judges, and parties involved in the cases or creation of the laws. OCM Intranet (Inet) – Employee contact information used for daily inter-office business and emergency contact. OCM Staff Info – Public access contact list PRiMO – PRiMO leadership is listed with photos as a contact list. All of PRiMO's past conference programs are available as pdf documents with session presenters listed with their abstracts. State Coastal Zone Management (CZM) Performance Measures Database - User accounts are used for managing project performance measures and partnership linkages in projects. TOMIS – User accounts are used for role based authentication of appropriate access for federal and contract users to manage task orders. Training Manager System – Training manager is a restricted access website that uses ICAM for authentication. The site is used for managing training courses provided by OCM. Each course has a Host, Trainer and registered participants with basic contact information and training evaluations and comments. All information is used for administrative and planning purposes. Virtual Conferencing and Webinars (Adobe Connect) – Webinars are hosted and recorded in Adobe Connect. Webinar attendees are required to register to enter the training.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Concept of least privilege; secure network and database; encrypted storage and transmission

		CAMMP – Restricted access website, SQL server database, Coastal Management Fellowship Contacts – Public website Coastal Zone Management Act Program Changes – Public website, with an administrative page that is used by OCM CZM staff to validate and publish public comments. Comments are stored in SQL server and displayed on restricted access site for verification prior to being published. Coral Database – NOAA Restricted Access sharepoint site using ICAM login for managing users and authentication. Data is in SQL Server. Data Access Viewer (DAV) – Data request records are stored in secured SQL Server. Digital Coast – Public access web pages. Estuaries Education – Public access web page. Green Infrastructure Database - Public access search interface, data is stored in secured SQL Server database. National Estuarine Research Reserves (NERRS) – Site profiles are pdf documents hosted on a public access website. NERRs Performance Measures Database – Restricted access website, data is stored in Secured SQL Server database. Ocean Law Search – Public access search site, which indexes PDFs and citation information stored in a secured SQL Server database. OCM Intranet (Inet) – Restricted access site. Sharepoint intranet site, using ICAM authentication. Data stored in secured SQL Server database. OCM Staff Info – Contact list is provided from a secured SQL Server database. PRiMO – Public access website, with PDF conference

		programs State Coastal Zone Management (CZM) Performance Measures Database -Restricted access website. Data stored in secured SQL Server database. TOMIS – Restricted access website. Data stored in secured SQL Server. Training Manager System – Restricted access website. Data stored in secured SQL Server database. Virtual Conferencing and Webinars (Adobe Connect) – Trainings are recorded in Adobe Connect. An admin is required to login to access registration information.
	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.)

Minimal PII is collected. NOAA6101 collects only enough information to be able to provide users with the information they need to do business with us. Users provide their information voluntarily in order to be able to receive the information they request.

Potential threats that exist for information collected include data exfiltration and improper handling, retention, sanitization and/or disposal of data.

OCM follows and implements principle of least privilege and separation of duties (RBAC) in combination with role-based access control. Only authorized individuals with a need to know will have access to data.

All OCM components are configured following secure baselines and are continuously monitored through weekly/monthly vulnerability scans and log reviews. All OCM staff complete the mandatory IT security awareness training every year.

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

X	Yes, the conduct of this PIA results in required business process changes.
	Explanation: Adding Privacy Act Statements for TOMIS, CZM Program Change, and CAMMP (see Section 7 for more details).
	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.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: Included new Data Loss Prevention (DLP) technology in TOMIS.
	No, the conduct of this PIA does not result in any required technology changes.