

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



**Privacy Impact Assessment**  
**for the**  
**NOAA6101**  
**Office for Coastal Management (OCM)**

Reviewed by: Mark Graff Bureau Chief Privacy Officer

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

**GRAFF.MARK.HYRUM.1514447892**

Digitally signed by  
GRAFF.MARK.HYRUM.1514447892  
Date: 2023.05.22 13:01:15 -04'00'

---

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

Date

**U.S. Department of Commerce Privacy Impact Assessment**  
**NOAA/NOS/Office for Coastal Management (OCM)**

**Unique Project Identifier: NOAA6101**

**Introduction: System Description**

*Provide a brief description of the information system.*

The mission of the National Oceanic and Atmospheric Administration (NOAA) NOAA6101, Office for Coastal Management (OCM) is to catalyze and influence a broad base of leaders, citizens, and coastal practitioners to ensure healthy coastal ecosystems, resilient coastal communities, and vibrant and sustainable coastal economies. The coast and its residents are at the epicenter of the impacts of changes in weather, climate, demographics, and economies. OCM manages coastal resources and uses through strengthening governance and investments in the development and implementation of comprehensive policies, rules, and plans. OCM administers the Coastal Zone Management Act, the Coral Reef Conservation Act, the Deep Seabed Hard Mineral Resources Act of 1980, and the Ocean Thermal Energy Conversion Act of 1980.

New additions since the last PIA:

- None

New removals since the last PIA:

- None

Address the following elements:

*(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) operational, programmatic and internal administrative needs are met. The system is an integrated collection of subsystems designed to provide general office automation, infrastructure, and connectivity services to 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 (Central US)  
Microsoft Azure (East US)

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

NOAA6101 has interconnections with the following FISMA systems:

NOAA0100 – NOAA Cyber Security Center (H) NOAA OCIO (NCSC/ESS/NCIRT) (Managed by NOAA6101) PII is shared (NCIRT tickets, vulnerability data).

NOAA0550 – NOAA Enterprise Network NOAA N-Wave (NOAA Enterprise Network) (Managed by NOAA6101) PII is shared (sensitive information transmitted through the network).

NOAA0700 – NOAA High Availability Enterprise Services (HAES) (EDS/ICAM/NSD) (Managed by NOAA6101) PII is shared (employee addresses and contact information).

NOAA0900 – NOAA Consolidated Cloud Applications (H) Cloud SaaS Applications (ENS/G-Suite/MaaS360/ESRI etc.) (Managed by NOAA6101) PII is shared (NOAA has allowed employees to send and store PII using g-suite products).

NOAA6001 – NOS Enterprise Information System and cloud services (Azure) (Managed by NOAA6001)

Adobe Connect – audio/video recordings are hosted in Adobe Connect Managed Services. PII is shared (audio and video). (Adobe Connect Managed Services # 1331L521A13ES0041)

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

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

All NOAA6101 users must be furnished with GFE and valid accounts before access is granted. The information is retrieved through applications. Remote access is provided via NOAA's N-WAVE VPN solution. Internal web sites and internal information is only accessible by NOAA6101 employees. General public will only have access to the public web sites. Public data is hosted on publicly accessible web sites which are all hosted with SSL/TLS certificates for enhanced security.

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

All sensitive information identified in section f is transmitted through secure e-mail (Kiteworks), facsimile, or data is manually entered into online web applications such as Travel Manager, CBS, etc. Google mail and G-Suite is used by NOAA6101 for email and data sharing as NOAA preferred provider. Internal data security is provided by defense in depth with layered security for internal data. (Physical access, Firewalls, Active Directory, Access Controls, etc.). Public data is hosted on publicly accessible web sites which are all hosted with SSL/TLS certificates for enhanced security. NOAA6101's Communications Office manages its social media sites.

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

Social Security Numbers (SSNs) are collected for new NOAA/NOS/OCM employees, and when renewing Common Access Card or Personal Identification Verification (CAC/PIV) cards for staff members. These are transmitted to the NOAA Security Office via a secure file sharing platform that facilitates access to enterprise content sources (i.e., [Kiteworks](#)). OCM does not maintain SSNs 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 in the OCM Privacy Impact Assessment 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

Adobe Connect recorded webinars are stored on Adobe's site. Attendee information is anonymized when saved for republishing. Adobe Connect is using TLS/SSL.

Please reference question 2 in the questionnaire section of this document for NOAA guidance on recording Google Meet sessions. Google Meet is using TLS/SSL.

*(g) Any information sharing*

PII is manually entered into the system by the administrator or through a bulk upload from a

spreadsheet(s).

Social Security Numbers (SSNs) are collected for new NOAA/NOS/OCM employees, and when renewing Common Access Card or Personal Identification Verification (CAC/PIV) cards for staff members. These are transmitted to the NOAA Security Office via a secure file sharing platform that facilitates access to enterprise content sources (i.e., Kiteworks). OCM does not maintain SSNs 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 in the OCM Privacy Impact Assessment for more details), but is stored only temporarily on the system.

POC information is entered into various applications/web sites as detailed 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

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).

Just like DOC, NOAA and NOS internal/public-facing websites, OCM internal/public-facing websites also have photographs of OCM staff involved in research and/or educational programs/activities, voluntarily submitted with implied consent to serve a purpose, reviewed, verified and managed through OCM website content managers prior to publishing them on the websites.

Business Identifiable Information (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 # or Unique Entity Identifier
- 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 # or Unique Entity Identifier
- 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 voluntary and can be removed by request at any time.)

- Coastal and Marine Management Program (CAMMP): Application that allows for collaborative project planning with partners (state CZM and NERRS). Data collected includes names, title, email, and budget. This is an internal site and information is not shared publicly.
- 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. This is an internal site and information is not shared publicly.
- 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 via the OCM website.
- 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.
- Digital Coast Academy Campus: Digital Coast Academy Campus is the name for a Moodle based Learning Management System (LMS) where online users participate in blended (self-paced and in person) trainings. Data collected from students includes: name, email, address\*, phone\*, institution/department\*, and profile picture\* (\*voluntary).
- 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. This is an internal site and information is not shared publicly.

- 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. This is an internal site and information is not shared publicly.
- OCM Staff Info - Contact information for OCM staff. Information published includes name, email and phone number.
- Pacific Risk Management 'Ohana (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): Application that collects and maintains POC information (name, email, phone, company name) for use in administering various contractor tasks and deliverables. This is an internal site and information is not shared publicly.
- 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). This is an internal site and information is not shared publicly.
- Virtual Conferencing and Webinars - Adobe Connect and Google Meet are being used for virtual meetings and webinars.
  - Adobe Connect: Recorded webinars are stored on Adobe's site. Attendee information is anonymized when saved for republishing.
  - Google Meet: Please reference question 3.1 in the questionnaire section of this document for NOAA guidance on recording Google Meet sessions.
- 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.
- Uncrewed Systems (UxS): As outlined in the System of Records Notice (SORN) Commerce/DEPT-29 (Unmanned Aircraft Systems, February 2018), the use of UxS for OCM purposes has the potential for inadvertent collection of PII, such as images of individuals along the coastlines that are within the area of study by the UxS vehicle. However, no retrieval of information using any unique identifier within UxS collected datasets will be conducted, and any PII inadvertently collected will be deleted within 30 days. NOAA6101 does not contain any application capable of facial recognition within any captured images. OCM is working with vendors to use

UxS (drones) for gathering Light Detection and Ranging (lidar) or aerial photos in order to assist with the accuracy of the mapping of beach, marsh, wetlands, and water study areas. It is anticipated that the UxS collected imagery will be at a resolution to meet organizational needs but it would not have the ability (resolution or clarity) to uniquely identify any individuals. If the drone goes down during flight, the retrieval of the unit would be at the discretion of the operator, based on safety and technical factors. Inadvertently obtained PII captured during the flight could potentially be retrieved by others from the damaged drone, if technically possible. OCM will comply with all policies and procedures posted on the [NOAA Office of Marine and Aviation Operations site as it relates to Uncrewed Systems](#) and as posted to the [NOAA Uncrewed Systems Research to Operations site](#). Relevant policy documents include but are not limited to:

- [NOAA Unmanned Aircraft System Handbook, v1.0, June 2017](#)
- [NOAA Aircraft Operations Center UAS Policy 220-1-5 \(Version 7\)](#)
- [NOAA Uncrewed Systems Research Transition Office Privacy Policy \(NOAA OCIO\)](#)

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

OCM has the authority to collect, maintain, use, and disseminate the information under the authority of:

\* Note: Reference table at the end of this PIA for details.

*(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.

**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 (SSNs) are collected for new NOAA/NOS/OCM employees, and when renewing Common Access Card or Personal Identification Verification (CAC/PIV) cards for staff members.					

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. Marital Status	

f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship	X	n. Religion			
<p>u. Other general personal data (specify):</p> <p>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.</p> <p>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.</p> <p>Various web pages/sites throughout the system collect POC data for information sharing purposes. These are listed below in Section 5.1.</p> <p>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.</p>					

<b>Work-Related Data (WRD)</b>					
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		k. Procurement/contracting records	X
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		
<p>l. Other work-related data (specify):</p> <p>Work related data is collected and shared with employees for internal office communication purposes. Additionally, grant information or acquisitions information 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.</p>					

<b>Distinguishing Features/Biometrics (DFB)</b>					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording	X	h. Eye Color		m. DNA Sample or Profile	
d. Video Recording	X	i. Height		n. Retina/Iris Scans	
e. Photographs	X	j. Weight		o. Dental Profile	
<p>p. Other distinguishing features/biometrics (specify):</p> <p>The Uncrewed System (UxS) collected lidar or imagery will be at a resolution to meet organizational needs but it would not have the ability (resolution or clarity) to uniquely identify any individuals. Any PII collected is incidental, unintentional, and is not retained.</p>					

<b>System Administration/Audit Data (SAAD)</b>					
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	X
g. Other system administration/audit data (specify):					

<b>Other Information (specify)</b>
<p>Server logs collect IP addresses, date and time of access for IT Administration purposes.</p> <p>Building Entry Readers: Information is captured for physical access to OCM buildings.</p> <p>Contents of files are scanned using a Data Loss Prevention scanner in the TOMIS application. This scanner checks uploaded files to ensure no sensitive PII or BII is uploaded in files to the TOMIS system.</p>

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

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

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

<b>Non-government Sources</b>					
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.

<p>PII/BII 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. Staff also update PII in the system semi-annually upon request, and can make changes at any time necessary. Staff and partners QA/QC their own PII/BII entries and can either make their own updates or send update requests to a small team assigned this task.</p>
---

## 2.4 Is the information covered by the Paperwork Reduction Act?

X	<p>Yes, the information is covered by the Paperwork Reduction Act.</p> <p>Provide the OMB control number and the agency number for the collection.</p>
---	--

	OMB Control # 0648-0030 (expires 07/31/23) OMB Control # 0648-0119 (expires 08/31/22) OMB Control # 0648-0121 (expires 12/31/24) OMB Control # 0648-0145 (expires 10/31/24) OMB Control # 0648-0411 (expires 02/28/23) OMB Control # 0648-0448 (expires 08/31/24) OMB Control # 0648-0459 (expires 03/31/22) OMB Control # 0648-0661 (expires 05/31/23) OMB Control # 0648-0796 (expires 07/31/24)
	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):			
	<p>Audio/video recordings: Virtual Conferencing and Webinars - Adobe Connect is being used for virtual meetings and webinars. Attendee information and recorded webinars are stored on Adobe site, and when appropriate (i.e. trainings and webinars) published for later viewing. Google Meet recordings have been recently approved within NOAA, in compliance with the <a href="#">NOAA Privacy Office defined Standard Operating Process</a>. Note that Google Meet recordings are stored in NOAA0900 and not NOAA6101.</p> <p>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.</p> <p>Building Entry Readers: Information is captured for physical access to OCM buildings.</p> <p>The utilization of UxS (drones) to gather aerial photos to assist with the accuracy of mapping of beach, marsh, wetlands, and water study areas. The use of drones is not for surveillance. Although the UxS has the potential to collect PII via patterned single images taken during the drone flight, it is not the purpose of the</p>		

	device and any inadvertently captured PII will be immediately deleted, when identified during the data processing stage.
--	--

## **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)	X	For web measurement and customization technologies (multi-session)	
Other (specify):			
<p>Google Analytics is used for web measurement technologies. All traffic sent to Google Analytics is anonymized per the GSA policy (OMB M-17-06 Digital Analytics Program). Thus, no PII is collected for web measurement technologies.</p> <p>UxS: OCM will be utilizing UxS (drones) in the future to gather lidar and aerial photos to assist with the accuracy of mapping of beach, marsh, wetlands, and water study areas. It is anticipated that the UxS collected lidar or imagery will be at a resolution to meet organizational needs but it would not have the ability (resolution or clarity) to uniquely identify any individuals. Any PII collected is incidental, unintentional, and is not retained. UxS data would be maintained in a separate folder, and mission-specific data validated for incorporation into OCM mission products. The UxS data would not be disseminated as collected images, but relevant data would be incorporated into OCM products.</p>			

## **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.)

- Coastal and Marine Management Program (CAMMP): 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 via the OCM website.
- 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.
- Digital Coast Academy Campus: Collects name, email, address\*, phone\*, institution/department\*, and profile picture\* (\*voluntary). as part of account creation process and that information is used as part of course interaction. No information is published publicly, information collected is only for use within

the course and subsequent reporting. Students in these courses are a combination of federal, contract, and general public users.

- 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.
- 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): Application that collects and maintains POC information (name, email, phone, company name) for use in administering various contractor tasks and deliverables.
- 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 and Google Meet are being used for virtual meetings and webinars.
  - Adobe Connect: Recorded webinars are stored on Adobe's site. Attendee information is anonymized when saved for republishing.
  - Google Meet: Please reference question 3.1 in the questionnaire section of this document for NOAA guidance on recording Google Meet sessions.
- 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.

- UxS: OCM is planned to utilize UxS (drones) in the future to gather lidar and/or aerial photos to assist with the accuracy of the mapping of beach, marsh, wetlands, and water study areas. UxS would be maintained in a separate folder (secured through technical permission) until validated for incorporation into OCM mission products. The UxS data would not be disseminated as collected images, but relevant data would be incorporated into OCM products. Any PII collected is incidental, unintentional, and not retained. It is anticipated that the UxS collected imagery will be at a resolution to meet organizational needs, but it would not have the ability (resolution or clarity) to uniquely identify any individuals.

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.
- There is potential for insider threat to download data

#### Controls

- Users take privacy training at least annually in the required annual IT security awareness course. After successfully completing the training section of the annual IT security awareness course. Users must sign a digital rules of behavior form stating they understand their responsibilities in order to complete the course.
- Users take Controlled Unclassified Information (CUI) course annually
- Before logging on to any NOS computer or web application the user must agree with the warning banner which has language specifying that the user has the responsibility to safeguard any CUI on the computer system.
- OCM follows least access privilege policies for users and any PII is limited access to users who have a business need for the information.

- 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.

## UxS

- Any PII collected is incidental, unintentional, and is not retained. It is anticipated that the Uncrewed System (UxS) collected lidar or imagery will be at a resolution to meet organizational needs but it would not have the ability (resolution or clarity) to uniquely identify any individuals.

## **Section 6: Information Sharing and Access**

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			X**
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

\* DHS FLETC for verification of foreign visitor identity.

\*\* Only non-sensitive, point of contact information is shared, typically for subject matter experts who have agreed to share this information

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	---

- 6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

<input type="checkbox"/>	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

- 6.3 Indicate whether the IT system connects with or receives information from any other IT

systems authorized to process PII and/or BII.

X	<p>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:</p> <p>NOAA6101 has interconnections with the following FISMA systems:</p> <ul style="list-style-type: none"> <li>• NOAA0100 – NOAA Cyber Security Center (H) NOAA OCIO (NCSC/ESS/NCIRT) (Managed by NOAA61001) PII is shared (NCIRT tickets, vulnerability data).</li> <li>• NOAA0550 – NOAA Enterprise Network NOAA N-Wave (NOAA Enterprise Network) (Managed by NOAA61001) PII is shared (sensitive information transmitted through the network).</li> <li>• NOAA0700 – NOAA High Availability Enterprise Services (HAES) (EDS/ICAM/NSD) (Managed by NOAA61001) PII is shared (employee addresses and contact information).</li> <li>• NOAA0900 – NOAA Consolidated Cloud Applications (H) Cloud SaaS Applications (ENS/G-Suite/MaaS360/ESRI etc.) (Managed by NOAA61001) PII is shared (NOAA has allowed employees to send and store PII using g-suite products).</li> <li>• NOAA6001 – NOS Enterprise Information System (Managed by NOAA6001)</li> <li>• Adobe Connect – audio/video recordings are hosted in Adobe Connect Managed Services. PII is shared (audio and video). (Adobe Connect Managed Services # 1331L521A13ES0041)</li> </ul>
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	X*	Government Employees	X
Contractors	X		
Other (specify): *The public has limited access to Subject Matter Expert Points of Contact via listings on OCM web pages.			

## **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	<p>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:</p> <ul style="list-style-type: none"> <li>● CAMMP (<a href="https://coast.noaa.gov/cammp/">https://coast.noaa.gov/cammp/</a>) (Privacy Act Statement on login page)</li> <li>● Coastal Management Fellows Contacts (<a href="https://coast.noaa.gov/fellowship/Directory/alphabetical.html">https://coast.noaa.gov/fellowship/Directory/alphabetical.html</a>) (<a href="#">Privacy Policy</a> link in footer)</li> <li>● Coastal Zone Management Program Change Public Comments Form (<a href="https://coast.noaa.gov/czmprogramchange/#/public/change-view/1230">https://coast.noaa.gov/czmprogramchange/#/public/change-view/1230</a>) (Privacy Act Statement linked on top of public comments form)</li> <li>● CZM Performance Measure tracking system (<a href="https://coast.noaa.gov/czmpm/">https://coast.noaa.gov/czmpm/</a> - access is restricted) (<a href="#">Privacy Act Statement</a> is provided on the login page.)</li> <li>● Corals DB (<a href="https://inet.coast.noaa.gov/coral/">https://inet.coast.noaa.gov/coral/</a>) (Privacy Act Statement on login page)</li> <li>● Data Access Viewer (<a href="https://coast.noaa.gov/dataviewer/">https://coast.noaa.gov/dataviewer/</a>) (Privacy Act Statement on request submission form)</li> <li>● Digital Coast Training Section Host This Course form (<a href="https://coast.noaa.gov/digitalcoast/training/ecosystem-services.html">https://coast.noaa.gov/digitalcoast/training/ecosystem-services.html</a>) (Privacy Act Statement link to contact us statement)</li> <li>● Digital Coast Academy Campus: (<a href="https://coast.noaa.gov/campus/user/profile.php">https://coast.noaa.gov/campus/user/profile.php</a>) (Privacy Act Statement link on Profile and Preferences Page) (Privacy Policy in Footer)</li> <li>● Estuary Education Volunteer Contacts (<a href="https://coast.noaa.gov/estuaries/news/volunteer.html">https://coast.noaa.gov/estuaries/news/volunteer.html</a>) (<a href="#">Privacy Act Statement</a> included on consent form)</li> <li>● Green Infrastructure Effectiveness Database (<a href="https://coast.noaa.gov/gisearch/#/search">https://coast.noaa.gov/gisearch/#/search</a>) (Privacy Policy in Footer)</li> <li>● National Estuarine Research Reserves - Reserve Profiles (<a href="https://coast.noaa.gov/nerrs/reserves/wells.html">https://coast.noaa.gov/nerrs/reserves/wells.html</a>) (Privacy Policy in Footer)</li> <li>● NERRS Performance Measure tracking system (<a href="https://coast.noaa.gov/nerrspm/">https://coast.noaa.gov/nerrspm/</a>) (<a href="#">Privacy Act Statement</a> is provided on the login page.)</li> <li>● OCM Contact Form (<a href="https://coast.noaa.gov/contactform/">https://coast.noaa.gov/contactform/</a>) (<a href="#">Privacy Act Statement</a> linked at bottom of form)</li> <li>● OCM Intranet (<a href="https://inet.coast.noaa.gov/">https://inet.coast.noaa.gov/</a> - access is restricted) (<a href="#">Privacy Act Statement</a> is on login page and linked at top of employee update form)</li> <li>● OCM Partner Contact Information Sharing Consent Form (<a href="https://docs.google.com/forms/d/e/1FAIpQLScFY_9d8lWPgG0U1cjiitiPWxiIAJl2oH2bwabFDnUfJaCpPA/viewform?fbzx=-4541248695308170028">https://docs.google.com/forms/d/e/1FAIpQLScFY_9d8lWPgG0U1cjiitiPWxiIAJl2oH2bwabFDnUfJaCpPA/viewform?fbzx=-4541248695308170028</a> - access is restricted) (Privacy Act Statement is on the form provided to partners when they consent to publishing their information on OCM website(s))</li> <li>● PRiMO leadership page (<a href="https://coast.noaa.gov/primmo/about/leadership.html">https://coast.noaa.gov/primmo/about/leadership.html</a>) (Privacy Policy in footer, POC consent form for users on page)</li> </ul>
---	---

	<ul style="list-style-type: none"> <li>• Still Images and Video on websites (Privacy Policy link in footer)</li> <li>• TOMIS V2 (<a href="https://coast.noaa.gov/tomis">https://coast.noaa.gov/tomis</a>) (Privacy Act Statement on login)</li> <li>• Training Management System (<a href="https://coast.noaa.gov/trainingmanager/">https://coast.noaa.gov/trainingmanager/</a>) (Privacy Policy in footer, POC consent form with Privacy Act Statement linked in course participants section)</li> <li>• Virtual Conferencing and Webinars (via Adobe Connect) (Privacy Act Statement link to Adobe Connect Exit link)</li> </ul> <p>The privacy policy is linked in footers of every page and can be found at:  <a href="https://coast.noaa.gov/PrivacyPolicy/privacyPolicy.html">https://coast.noaa.gov/PrivacyPolicy/privacyPolicy.html</a></p>
X	<p>Yes, notice is provided by other means. Specify how:</p> <p>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.</p> <p>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.</p> <p>OCM staff members (government employees and contractor staff) 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.</p> <p>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.</p> <p>Vendors and grantees are notified via solicitations and calls for proposals that BII will be collected as necessary to effectively evaluate proposals.</p> <p>Video surveillance: Notice is posted at all ingress/egress points that video monitoring is occurring for the purpose of safety/security monitoring.</p> <p>Photographic images: Prior to collection, individuals are notified that photographs may be taken at organizational events. Notice is either provided by posting notice in the area where photographs will be taken or verbally/in writing of occasions where photos may be taken. A PAS is provided to individuals prior to the recording of any Google Meet notifying them that the Meet will be recorded.</p>

	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.	<p>Specify how:</p> <p>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.</p> <p>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.</p> <p>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.</p> <p><u>Site specific details:</u></p> <p>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.</p> <p>Coastal Management Fellowship Projects and News – No data entry, this section lists fellows in relationship to the projects they worked on and highlights in the fellowship news. Fellows are</p>
---	---	---

		<p>required to fill out the OCM POC sharing consent form in order to list their name on the site. 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.</p> <p>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.</p> <p>Coral Database – Restricted access site. If user information is not provided, users can’t login to the site to manage projects.</p> <p>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.</p> <p>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 <a href="https://coast.noaa.gov/digitalcoast/training/risk-communication.html">https://coast.noaa.gov/digitalcoast/training/risk-communication.html</a>).</p> <p>Digital Coast Academy Campus – Registration for courses in Digital Coast Academy Campus requires contact information for account management purposes. If a course participant wishes to have their information removed from the Digital Coast Academy Campus learning management system, they can request to have their account deleted via email.</p> <p>Estuaries Education – No data entry allowed. Education Volunteer Coordinator’s contact info is provided, but some states have generic contact info (i.e.: Delaware – <a href="mailto:info@nerra.org">info@nerra.org</a>). If a volunteer coordinator wishes to remove their contact info, they can use a generic contact email address.</p>
--	--	---

		<p>Green Infrastructure Database - No data entry. All information listed in this database is from publicly available literature.</p> <p>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.</p> <p>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.</p> <p>OCM Intranet (Inet) – Staff are required to have accounts to access internal documents. If they decline to provide information, users cannot use the system.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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</p>
--	--	---

		<p>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.</p> <p>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.</p> <p>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.</p> <p>Individuals may decline to provide PII during Google Meets by turning off their web cam.</p>
	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.	<p>Specify how:</p> <p>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.</p> <p>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.</p> <p>Staff members provide PII upon initial onboarding as a condition of employment. They may consent to only</p>
---	--	--

		<p>particular uses, but this may affect their employment. A Privacy Act statement for this type of scenario is also available.</p> <p>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.</p> <p>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.</p> <p>Just like DOC, NOAA and NOS internal/public-facing websites, OCM internal/public-facing websites also have photographs of OCM staff involved in research and/or educational programs/activities, voluntarily submitted with implied consent to serve a purpose, reviewed, verified and managed through OCM website content managers prior to publishing them on the websites.</p> <p><u>Site specific details:</u></p> <p>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.</p> <p>Coastal Management Fellowship Projects and News – Fellows fill out the OCM POC sharing consent form to have their name listed with their project descriptions. Fellows contact information (as a Subject Matter Expert) is shared on OCM web site upon consent of the Fellow.</p> <p>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</p>
--	--	---

		<p>also available.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Digital Coast Academy Campus - 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 declined to register for a course, they can request course materials via email.</p> <p>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.</p> <p>Green Infrastructure Database - There is no data entry or PII created to end users. This is a database of publicly available scholarly papers.</p> <p>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</p>
--	--	---

		<p>Reserve Profiles can request that their info be removed through the Contact Us form linked in the bottom of every page.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Still images and video – Employees and partners identified in still images or videos will be asked to submit the POC consent form.</p> <p>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.</p>
--	--	---

		<p>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.</p> <p>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.</p> <p>Any PII captured during a Google Meet will be used for the purpose of that meeting only. Individuals have the opportunity to consent to this use by having their webcam on.</p>
	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.	<p>Specify how:</p> <p>Subject matter experts who provide contact information on the OCM website can review, update, or delete their PII upon request at any time.</p> <p>Web site visitors who provide PII via a request for information can request to review, update or delete their PII at any time.</p> <p>Staff members can update PII during performance reviews or via secure Intranet.</p> <p>Partners/grantees who provide contact information (PII) to participate in the NERRs Intranet site established for</p>
---	---	--

	<p>collaboration or to enter data into grantee performance measurement tracking systems can review, update, or delete their PII upon request at any time.</p> <p>Vendors or grantees can review/update BII at any time upon request to the NOS proposal contact.</p> <p>Anyone can at any time request the removal/update of a photograph or video, voluntarily submitted by them with implied consent in the past and still published on OCM internal/public-facing websites, through OCM website content managers.</p> <p><u>Site specific details:</u></p> <p>CAMMP – Users can review their account information and grant application preparation materials in their user profile.</p> <p>Coastal Management Fellowship Projects and News – Fellows can review the information on the web page and request modifications via the contact us page linked at the bottom of every page.</p> <p>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.</p> <p>Coral Database – Users can review and update their account information in their user profile at any time.</p> <p>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</p> <p>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.</p> <p>Digital Coast Academy Campus - Users can review and edit their account information in their user profile.</p> <p>Estuaries Education – Volunteer coordinators who provide contact information on the OCM website can review, update,</p>
--	---

	<p>or delete their PII upon request at any time.</p> <p>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.</p> <p>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.</p> <p>NERRs Performance Measures Database – Users can review and edit their account information and performance measures at any time.</p> <p>OCM Intranet (Inet) – Staff members can update PII during performance reviews or via secure Intranet.</p> <p>PRiMO – Subject matter experts who provide contact information on the OCM website can review, update, or delete their PII upon request at any time.</p> <p>State Coastal Zone Management (CZM) Performance Measures Database - Users can review and edit their account information and performance measures at any time.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Virtual Conferencing and Webinars (Adobe Connect) – Participants in Adobe Connect webinars are able to view the</p>
--	---

		<p>videotaped material before it goes live.</p> <p>Individuals participating in Google Meets can request that their image be removed at any time.</p>
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	<p>Specify why not:</p> <p>Video surveillance: This imagery is archived as a record of events occurring in the surveilled area. Individuals do not have the opportunity to review/update this imagery.</p>

## **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	<p>Access to the PII/BII is being monitored, tracked, or recorded.</p> <p><b>Explanation:</b> All forms of electronic PII/BII are monitored, tracked and recorded with role based access controls in place on the system.</p>
X	<p>The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.</p> <p>Provide date of most recent Assessment and Authorization (A&amp;A): 1/5/2023 _____</p> <p><input type="checkbox"/> This is a new system. The A&amp;A date will be provided when the A&amp;A package is approved.</p>
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 in SQL Server databases on secured servers on premises and in Microsoft Azure Cloud Environment. Databases are only accessible based on least privilege and role-based access control. There are physical and network (firewall and internal only connections) security in place for both on premises and Azure data centers to ensure authorized access to the SQL Servers. Information placed in the database is only accessed on a need-to-know basis by OCM administrator staff who are identified as needing access to this information. The data in the SQL Servers is encrypted at rest via transparent data encryption and in transit for any transactions using HTTPS. SQL Server databases are scanned for vulnerabilities weekly and vulnerabilities are addressed per the OCM security policy schedules.

#### 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.

### **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.”

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/DEPT-2](#), Accounts Receivable
- [COMMERCE/DEPT-5](#), FOIA Records
- [COMMERCE/DEPT-6](#), Visitor Logs and Permits for Facilities under Department

	<p>Control</p> <ul style="list-style-type: none"> <li>• <a href="#">COMMERCE/DEPT-7</a>, Employee Accident Reports</li> <li>• <a href="#">OPM/GOVT-2</a>, Employee Performance File System Records</li> <li>• <a href="#">COMMERCE/DEPT-13</a>, Investigative and Security Records</li> <li>• <a href="#">COMMERCE/DEPT-27</a>, Investigation and Threat Management Records</li> <li>• <a href="#">COMMERCE/DEPT-18</a> - Employees Personnel Files Not Covered by Notices of Other Agencies</li> <li>• <a href="#">COMMERCE/DEPT-25</a>, Access Control and Identity Management System</li> <li>• <a href="#">COMMERCE/DEPT-29</a>, Unmanned Aircraft Systems</li> <li>• <a href="#">GSA/GOVT-9</a>, System for Award Management (SAM)</li> <li>• <a href="#">NOAA-11</a>, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.</li> <li>• <a href="#">COMMERCE/DEPT-20</a>, Biographical Files and Social Networks</li> <li>• <a href="#">OPM/GOVT-1</a>, General Personnel Records</li> <li>• <a href="#">COMMERCE/DEPT-31</a>, Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations.</li> <li>• <a href="#">OPM/GOVT-10</a>, Employee Medical File System Records.</li> </ul> <p>*NOTE: Reference table at the end of this PIA for additional details.</p>
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	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	<p>There is an approved record control schedule. Provide the name of the record control schedule:</p> <p>General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for</p>
---	--

	<p>records common to several or all agencies of the federal government. The underlying paper records relating to employees are covered by GRS 1, Civilian Personnel Records. In accordance with GRS 20, item 3, electronic versions of records scheduled for disposal under other records schedules may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. Guidance for these records in the NOAA Records Schedules refers disposition to GRS 20.</p> <p>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.</p> <p>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</p> <p>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.</p> <p>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.</p>
	<p>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:</p>
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 level. *(Check all that apply.)*

X	Identifiability	<p>Provide explanation:</p> <p>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.</p> <p>Just like DOC, NOAA and NOS internal/public-facing websites, OCM internal/public-facing websites also have photographs of OCM staff involved in research and/or educational programs/activities, voluntarily submitted with implied consent to serve a purpose, reviewed, verified and managed through OCM website content managers prior to publishing them on the websites.</p> <p>CAMMP – Restricted access site. System user name, First Name, Last Name, Email, Address, Phone Number, Organization Name, EIN/TIN/DUNS number</p> <p>Coastal Management Fellowship Contacts – First Name, Last Name, Email, Organization</p> <p>Coastal Zone Management Act Program Changes – System Username, First Name, Last Name, Affiliation, Email, City, State, Zip</p> <p>Coral Database – ICAM Username, First Name, Last Name, Email, Organization</p> <p>Data Access Viewer (DAV) – Email, Organization</p> <p>Digital Coast – Training Partners Case Studies - Subject Matter Experts - Picture, First Name, Last Name, Email,</p>
---	-----------------	--

		<p>Organization - Training Webinars - Videos - Presenters Name(s), Organization</p> <p>Digital Coast Academy Campus – Restricted access site. User Profile: First/Last Name, Email, Location, Phone, Institution/Department, Profile Picture</p> <p>Estuaries Education – Volunteer Coordinator Names and Email</p> <p>Green Infrastructure Database - Links to scholarly articles Author(s) First Name, Last Name in citation.</p> <p>National Estuarine Research Reserves (NERRS) – Names of authors, editors, contributors.</p> <p>NERRs Performance Measures Database – Restricted access site. Username, First Name, Last Name, Email</p> <p>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)</p> <p>PRiMO – Leadership First Name, Last Name, Title, Organization, Picture, Conference Programs with presenter names and abstracts.</p> <p>State Coastal Zone Management (CZM) Performance Measures Database - Restricted access site. Username, First Name, Last Name, Email</p> <p>TOMIS – First Name, Last name, Organization, Email, Phone Number</p> <p>Training Manager System – Training Host (Name, Email, Phone, Organization), Facility Contact (Name, Address, Email), Training Participants (Name, Email, Zipcode)</p> <p>Virtual Conferencing and Webinars (Adobe Connect) – First Name, Last Name, Email, State, Zip, County, Organization</p>
X	Quantity of PII	Provide explanation:

		<p>Information collected is limited to a small subset of specific applications and personnel files.</p> <p>CAMMP – 137 System User (38 NOAA users, 99 External Users)</p> <p>Coastal Management Fellowship Projects and News – 129 Fellows listed in project descriptions and Fellows news highlights.</p> <p>Coastal Zone Management Act Program Changes – 71 total users (25 NOAA staff, 46 State CZM staff) with access to the admin section. 23 people have submitted public comments.</p> <p>Coral Database – 485 NOAA staff system user accounts and project members.</p> <p>Data Access Viewer (DAV) – 536,808 download requests according to DAV Data report. Not all are unique email addresses.</p> <p>Digital Coast – 341 Subject matter experts and training presenters.</p> <p>Digital Coast Academy Campus – 636 user accounts (77 NOAA users, 559 non-NOAA users) – 219 active accounts, 417 inactive accounts</p> <p>Estuaries Education – 30 Coordinators contact information listed.</p> <p>Green Infrastructure Database - 237 scholarly article citations with multiple authors each.</p> <p>National Estuarine Research Reserves (NERRS) – 30 NERRS reserves site profile documents with varying number of authors, editors, and contributors' names.</p> <p>NERRs Performance Measures Database – 71 NOAA users, 188 Partner user accounts</p> <p>OCM Intranet (Inet) – 284 Employee Records</p> <p>PRiMO – 32 Leadership names and photos, 17 Conference Programs with varying number of presenters' information.</p> <p>State Coastal Zone Management (CZM) Performance Measures Database - 87 NOAA Employee users, 129 External Partner Users</p> <p>TOMIS – 205 active and 775 inactive accounts with user contact information.</p>
--	--	---

		<p>Training Manager System – 1306 planned and completed courses, of which 755 were completed with participant lists. An average of 28 participants per class in a random sampling.</p> <p>Virtual Conferencing and Webinars (Adobe Connect) – There are approximately 10,637 unique attendees registered for approximately 2,443 meetings and virtual classes. Many attendees have registered for multiple meetings.</p>
X	Data Field Sensitivity	<p>Provide explanation:</p> <p>Phone numbers and e-mail addresses are the primary information collected, and are used for communication purposes.</p>
X	Context of Use	<p>Provide explanation:</p> <p>The vast majority of PII collected is used for emergency contact information for staff members, or for communicating back to information requesters.</p> <p>Just like DOC, NOAA and NOS internal/public-facing websites, OCM internal/public-facing websites also have photographs of OCM staff involved in research and/or educational programs/activities, voluntarily submitted with implied consent to serve a purpose, reviewed, verified and managed through OCM website content managers prior to publishing them on the websites.</p> <p>CAMMP – Users accounts are created by project administrators as necessary. Grant applications prepared by potential grantees voluntarily.</p> <p>Coastal Management Fellowship Projects and News – Fellows added to the projects list when they are awarded a fellowship and the project is approved.</p> <p>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.</p>

		<p>Coral Database – Projects and Deliverables tracking with users associated with each project and deliverable.</p> <p>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.</p> <p>Digital Coast – Subject matter experts and training presenters’ names, email and organization are listed on cast study pages and webinar description pages.</p> <p>Digital Coast Academy Campus - Users accounts are created by system administrators as necessary for access to active courses. Accounts are disabled monthly after final courses have closed.</p> <p>Estuaries Education – Contact information is listed for each state’s NERRS volunteer coordinators on the estuary resources page.</p> <p>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.</p> <p>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.</p> <p>NERRs Performance Measures Database – User accounts are used for managing project performance measures and partnership linkages in projects.</p> <p>OCM Intranet (Inet) – Employee contact information used for daily inter-office business and emergency contact.</p> <p>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.</p> <p>State Coastal Zone Management (CZM) Performance Measures Database - User accounts are used for managing project performance measures and</p>
--	--	---

		<p>partnership linkages in projects.</p> <p>TOMIS – User accounts are used for role-based authentication of appropriate access for federal and contract users to manage task orders.</p> <p>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.</p> <p>Virtual Conferencing and Webinars (Adobe Connect) – Webinars are hosted and recorded in Adobe Connect. Webinar attendees are required to register to enter the training.</p>
X	Obligation to Protect Confidentiality	Provide explanation: BII is collected via Grants Online but the information is considered confidential.
X	Access to and Location of PII	<p>Provide explanation:</p> <p>Concept of least privilege; secure network and database; encrypted storage and transmission</p> <p>Just like DOC, NOAA and NOS internal/public-facing websites, OCM internal/public-facing websites also have photographs of OCM staff involved in research and/or educational programs/activities, voluntarily submitted with implied consent to serve a purpose, reviewed, verified and managed through OCM website content managers prior to publishing them on the websites.</p> <p>CAMMP – Restricted access website, SQL server database,</p> <p>Coastal Management Fellowship Projects and News – Public website</p> <p>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</p>

		<p>to being published.</p> <p>Coral Database – NOAA Restricted Access SharePoint site using ICAM login for managing users and authentication. Data is in SQL Server.</p> <p>Data Access Viewer (DAV) – Data request records are stored in secured SQL Server.</p> <p>Digital Coast – Public access web pages.</p> <p>Digital Coast Academy Campus – Restricted access website, MySQL database</p> <p>Estuaries Education – Public access web page.</p> <p>Green Infrastructure Database - Public access search interface, data is stored in a secured SQL Server database.</p> <p>National Estuarine Research Reserves (NERRS) – Site profiles are pdf documents hosted on a public access website.</p> <p>NERRs Performance Measures Database – Restricted access website, data is stored in Secured SQL Server database.</p> <p>OCM Intranet (Inet) – Restricted access site. SharePoint intranet site, using ICAM authentication. Data stored in secured SQL Server database.</p> <p>PRiMO – Public access website, with PDF conference programs</p> <p>State Coastal Zone Management (CZM) Performance Measures Database -Restricted access website. Data stored in secured SQL Server database.</p> <p>TOMIS – Restricted access website. Data stored in secured SQL Server.</p> <p>Training Manager System – Restricted access website. Data stored in secured SQL Server database.</p> <p>Virtual Conferencing and Webinars (Adobe Connect) – Trainings are recorded in Adobe Connect. An admin is required to login to access registration information.</p>
--	--	---

	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 the principle of least privilege, separation of duties, and role-based access control in combination with rule-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.

	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.

	Programmatic Authorities (Introduction h.)	Type of Information Collected (Introduction h.)	Applicable SORNs (Section 9.2)
1.	5 U.S.C. 301 15 U.S.C. 1512	Contact Information for Customers and Stakeholders	NOAA-11
2.	5 U.S.C. 301 44 U.S.C. 3101 Executive Orders 12107, 12656, 13164, 12196, 12564 41 U.S.C. 433(d) 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 5379, 8347 Executive Orders 9397, as amended by 13478, 9830, and 12107 5 U.S.C. 33, 63 5 U.S.C. 1104, 3321, 4305, and 5405 Budget and Accounting Act of 1921 Accounting and Auditing Act of 1950 Federal Claim Collection Act of 1966 Federal Preparedness Circular (FPC) 65, July 26, 1999 5 U.S.C. 5701 Chapter 57 Coronavirus Aid, Relief, and Economic Security (CARES) Act, Public Law 116-136, Div. B., Title VIII, sec. 18115, 134 Stat. 574 Medical Examinations for Fitness for Duty Requirements, including 5 CFR part 339 Workforce safety federal requirements, including the Occupational Safety and Health Act of 1970, Executive Order 12196, 5 U.S.C. 7902 Other federal laws, regulations, Executive orders, or guidance related to the specific public health emergency or similar health and safety incident, including guidance issued by the Office of Management and Budget, the Centers for Disease Control and Prevention, or other appropriate agency or entity, as applicable	Employee Personnel & Work-Related Information	COMMERCE/DEPT-7 COMMERCE/DEPT-18 OPM/GOVT-1 OPM/GOVT-10 OPM/GOVT-2 COMMERCE/DEPT-9 COMMERCE/DEPT-31
3.	Executive Orders 10450, 11478 5 U.S.C. 7531-332 28 U.S.C. 533-535 Equal Employment Act of 1972 Electronic Signatures in Global and National Commerce Act, Public Law 106-229 5 U.S.C. 301 Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors	Security Investigation Information Badging & CAC issuance Passport Numbers Building surveillance/entry	COMMERCE/DEPT-13 COMMERCE/DEPT-18 COMMERCE/DEPT-25
4.	5 U.S.C. 301 44 U.S.C. 3101 28 U.S.C. 533-535 44 U.S.C. 3101 5 U.S.C. 301 Executive Orders 13526, 12968, 13356, and 13587 Public Law 108-458, Intelligence Reform and Terrorism Prevention Act of 2004 Intelligence Authorization Act for FY 2010, Public Law 111-259 31 U.S.C. 951-953 8 U.S.C. 1324a 15 CFR Parts 730-774, Export Administration Regulations	Visitor / Foreign National Access Information	COMMERCE/DEPT-6 COMMERCE/DEPT-27

	NAO 207-12, Technology Controls & Foreign National Access DAO 207-12, Foreign National Visitor and Guest Access Program		
5.	Freedom of Information Act, 5 U.S.C. 552 Privacy Act of 1974 as amended, 5 U.S.C. 552a 5 U.S.C. 301 44 U.S.C. 3101	FOIA Privacy Act Information	COMMERCE/DEPT-5
6.	Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (Feb. 15, 2015), Coast and Geodetic Survey Act, 33 U.S.C. 883a et seq., Coastal Zone Management Act, 16 U.S.C. 1451 et seq., Comprehensive Environmental Response, Compensation and Liability Act, 42 U.S.C. 9601 et seq., Coral Reef Conservation Act, 16 U.S.C. 6401 et seq., The Deep Seabed Hard Mineral Resources Act of 1980, The Ocean Thermal Energy Conversion Act of 1980	Unmanned Aircraft Surveillance	COMMERCE/DEPT-29
7.	5 U.S.C. 301 Presidential Memorandum to the Heads of Executive Departments and Agencies on Transparency and Open Government, January 21, 2009 OMB Open Government Directive, M-10-06, December 8, 2009 OMB Guidance for Agency Use of Third-Party Web sites and Applications, M-10-23, June 25, 2010	Biographical Files and Social Network Information	COMMERCE/DEPT-20
8.	28 U.S.C. 3101-3105, Debt Collection Act of 1982 (Pub. L. 97-365) 26 U.S.C. 6402(d) 31 U.S.C. 3711 FAR Subparts 4.11, 52.204 2 CFR Subtitle A 40 U.S.C. 121(c) FAR Subparts 9.4 and 28.2 Executive Orders 12549, 12689	Contract / Grant Info	COMMERCE/DEPT-2 GSA/GOVT-9