Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
For
NOAA 6101
Office for Coastal Management

Reviewed by: _____Mark Graff_____, Bureau Chief Privacy Officer

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

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

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
Date: 2019.08.15 17:41:32 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA 6101
Office for Coastal Management

Unique Project Identifier: NOAA 6101

Introduction: System Description

The mission of the National Oceanic and Atmospheric Administration (NOAA)'s 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.

NOAA6101 is a general support system used to ensure that the OCM's scientific and internal administrative / operational needs are met. The system is an integrated collection of subsystems designed to provide general office automation, infrastructure, and connectivity services to NOAA OCM staff located in Charleston, SC, Silver Spring, MD, Honolulu, HI, Stennis Space Center, MS, additional OCM field offices, and other remote locations. The system enables OCM to achieve its mission, which is to support the environmental, social, and economic well-being of the coast by linking people, information, and technology. OCM assists the nation's coastal resource management community by providing access to information, technology, and training, and by producing new tools and approaches that often can be applied nationwide.

The OCM Strategic Plan addresses three strategic outcomes for the coastal management community: healthy coastal ecosystems, resilient coastal communities, and vibrant and sustainable coastal economies.

OCM has both Personally Identifiable Information (PII) and Business Identifiable Information (BII) within its system boundary. This Privacy Impact Assessment (PIA) details the types of PII/BII found within the system boundary for NOAA 6101, and how that information is protected.

Two of the component subsystems are the internal networked file servers and web application servers. The file servers are restricted to OCM staff members and typically used for administrative and operational functions and/or storage such as:

- Administrative functions (replacing a manual process),
- Employee/Contractor information needed for personnel, security, performance evaluation, merit rewards, training, travel, etc.,
- Review of applicant information (e.g., information submitted in response to requests for proposals and/or in response to a solicitation),

- To track information, requests, tasks, actions, or processes related to the OCM / NOAA mission.

The OCM web servers host and serve web-based applications and sites. OCM's web servers primarily serve publicly accessible information, which is intended for OCM and other subsets of OCM, NOAA, other federal agencies, customers, partners, and/or the general public. There are a few applications and sites that are intentionally restricted (authentication required) to NOAA employees and contractors operating from within the NOAA network. These internal applications track information related to OCM's operations / administration (e.g., safety/emergency contacts).

A subset of web applications/sites served by OCM web servers is detailed in section 5.1 below.

Information sharing:

As stated in Sections 5.1 and 6.1, information is periodically shared within the bureau on a case-by-case basis. Additionally, non-sensitive POC information for certain subject matter experts is made available via the OCM web presence.

For verification of foreign visitor identity, information may be shared with NOAA Security and DHS FLETC.

5 U.S.C. § 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

15 U.S.C. § 1512 is an Organic Law which confers general powers and duties authority to executive agencies, vesting jurisdiction and control of departments, bureaus, offices and branches.

The Federal Information Processing Standard (FIPS) 199 security impact category for the system is 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):					

_x This is an existing information system in which changes do not create new privacy risks.

OCM made this choice in part because one FISMA system was absorbed into another during the Coastal Services Center (CSC) (NOAA6101) and Office for Ocean and Coastal Resource Management (OCRM) (NOAA6601) office integration, so there was no new system created. Additionally, OCM does not believe the types of information/data that were added to NOAA6101 were different from any of the already present information and data and imparted no new risks to 6101.

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	e. File/Case ID		i. Credit Card	
b. Taxpayer ID	x	f. Driver's License		j. Financial Account	
c. Employer ID	x	g. Passport	x	k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: Social Security numbers are collected for new NOAA/NOS/OCM employees. *These are transmitted to the NOAA Security Office via secure electronic transmission and then destroyed.* OCM does not maintain them on the IT system or as hard copy files. Passport numbers are handled in the same way as SSNs. These procedures are detailed in the OCM Standard Operating Procedure-Personnel Security. This SOP will be included/referenced in the NOAA 6101 System Security Plan. Taxpayer or employer ID information is collected infrequently (see section 5.1 for more details), but is stored only temporarily on the system.					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	x	o. Medical Information	
d. Gender		j. Telephone Number	x	p. Military Service	
e. Age		k. Email Address	x	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): Employee information is collected for emergency/disaster/CoOP-related contact needs. General inquiries related to information sharing consist of collecting name and email address in order to respond to the information requests. Certain subject matter experts agree explicitly to share contact information (name, phone, email) on OCM's public web site.					

Work-Related Data (WRD)					
a. Occupation	x	d. Telephone Number	x	g. Salary	
b. Job Title	x	e. Email Address	x	h. Work History	
c. Work Address	x	f. Business Associates			
i. Other work-related data (specify): Work related data is collected and shared with employees for internal office communication purposes. Additionally, grant or contract proposal information often contains PII/BII, such as budgets or cost proposals; this information is only accessible to those involved in grant or contract-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). See section 5.1 below for more details.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

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

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

Government Sources					
Within the Bureau	x	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations	x	Private Sector	x	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

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

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify): OCM uses CAC cards like much of the federal government, but none of that data is stored on OCM's system.			

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

Section 3: System Supported Activities

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

Activities			
Audio recordings		Building entry readers	x
Video surveillance		Electronic purchase transactions	
Other (specify):			

Building entry readers recognize CAC cards used to gain entry, but do not store any of the data embedded on the card.

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

Section 4: Purpose of the System

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

Purpose			
To determine eligibility		For administering human resources programs	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)	x
Other (specify):			

Section 5: Use of the Information

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

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[1] 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, Continuity of Operations Plan (COOP), etc. 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

[1] http://deemedexports.noaa.gov/Documents/Message_on_Electronic_Transmission_of_PII.pdf

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 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 sensitive 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:

- PRiMO: Web site 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.
- Coastal Storms Program: Web site 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: 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.

- 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.
- National Estuarine Research Reserves: Web site 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.
- Estuaries Education: Web site 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.
- Digital Coast: Publishes contact information of trainers for some trainings listed on the Digital Coast Training page. Information includes (name, email, location). Permission is acquired (via a form) from each trainer before listing their information on the site.
- Ocean Law Search: Web site related to underwater cultural heritage that makes various public laws, statutes, articles, and court case summaries via an online searchable interface. All of the information available is publicly accessible and has been assembled to focus on underwater cultural heritage. Some of the documents available contain names and addresses of legislators, attorneys, plaintiffs, or witnesses.
- CAMMP: Application that assists in building grant proposals. Data collected from applicants includes (name, title, email, applicant personnel names and salaries for grant budgeting).
- Coral DB: Application that collects internal NOAA staff proposals to the NOAA Corals matrix program.
- Data in the Classroom: Web site that publicly lists some OCM POCs (one staff member name, with phone and email). POC information is entirely voluntary and can be removed at any time upon request. There is also a "contact us" page, which collects name, zip code, phone.
- Data Access Viewer (DAV): Application that receives requests for data from the public. Email addresses are stored to provide a method of contacting the requester when the data is ready for pickup on the OCM FTP site.
- 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).
- OCM Point of Contact Management Database: Centralized contact management database used to maintain information from customers who have requested data or information, participated in conferences, requested products/materials, or attended meetings or trainings offered by OCM. This is a secure and centralized database.

Fields collected include (name, title, organization, address, city, state, zip, country, email, phone).

- National Estuarine Research Reserves (NERRs) Intranet is an authenticated application for NERRs and OCM staff to work collaboratively. Information collected includes name, organization, email, and phone number.
- NERRs and State Coastal Zone Management Performance Measures DBs 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.

Section 6: Information Sharing and Access

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

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus			
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			x (only non-sensitive, point of contact information is shared, typically for subject matter experts who have agreed to share this information)
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

* DHS FLETC for verification of foreign visitor identity.

	The PII/BII in the system will not be shared.

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

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
x	No, this IT system does not connect with or receive information from another IT system(s) authorized to

	process PII and/or BII.

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

Class of Users			
General Public		Government Employees	x
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
x	Yes, notice is provided by Privacy Act statements (five total) and/or privacy policy. The Privacy Act statements can all be found in the appendix below and also at: • https://coast.noaa.gov/contactform/ (Contact Us) • OCM Intranet (access is restricted) (OCM Intranet) • Offline form (access is restricted) (Partner Contact Information) • Performance measure tracking system (access is restricted) (CZM Performance Measures) • NERRs Intranet and performance measure tracking system (access is restricted) (NERRs Intranet and Performance Measures) The privacy policy can be found at: coast.noaa.gov/PrivacyPolicy/privacyPolicy.html___.	
x	Yes, notice is provided by other means.	Specify how: Subject matter experts often provide contact information via the OCM public web site. 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. Visitors to the OCM web presence can request information by providing minimal PII through an information request contact form. Individuals are under no obligation to provide this information, and the details of how this information is handled are readily available via the OCM Privacy Policy and a Privacy Act statement. OCM staff members (employees) are provided notice of how PII is used (i.e., emergency contact information in case of natural disasters) upon hire. Partners/grantees may provide contact information (PII) to participate in the NERRs Intranet site established for collaboration and to enter data into grantee performance measurement tracking systems.

		Vendors and grantees are notified via solicitations and calls for proposals that BII will be collected as necessary to effectively evaluate proposals.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

x	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Subject matter experts often provide contact information via the OCM public web site. Prior to making the POC information public, the subject matter experts are asked to fill out a form acknowledging that they will be providing this information on a public web site and that they agree to do so; all have the opportunity to decline to provide PII as it is an "opt in" scenario. A Privacy Act statement is also made available. Visitors to the OCM web presence can request information by providing minimal PII through an information request contact form. Individuals are under no obligation to provide this information, and the details of how this information is handled are readily available via the OCM Privacy Policy and a Privacy Act statement. Staff members provide PII upon hire as a condition of employment. A Privacy Act statement concerning usage of this information is made available to OCM staff members. They may decline to provide PII but this may affect their employment status. 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. Partners can decline to provide this information as it is an "opt in" scenario. Vendors and/or grantees provide BII when submitting proposals of various types. Proposers may decline to provide BII, by not including it in their proposals; however, that declination effectively removes them from consideration of contract or grant awards, as there are certain types of information that contain BII that are essential to a full and valid competition.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Subject matter experts who may be asked or offer to provide contact information are informed of exactly how and where on the OCM web site their contact information will be made available. A Privacy Act statement for this type of scenario is also available.

		Visitors to the OCM web presence can learn how PII is used via the OCM Privacy Policy and make the choice to opt in to the particular stated uses. A Privacy Act statement for this type of scenario is also available. Staff members provide PII upon hire as a condition of employment. They may consent to only particular uses, but this may affect their employment. A Privacy Act statement for this type of scenario is also available. Partners/grantees who provide contact information (PII) to participate in the NERRs Intranet site established for collaboration or to enter data into grantee performance measurement tracking systems opt in to providing PII for the particular stated uses. For vendors and grantees, the only usage of the BII is during proposal review and subsequent consultation with vendors or grantees. The BII is not shared or disseminated beyond this scope.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

x	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Subject matter experts who provide contact information on the OCM web site can review, update, or delete their PII upon request at any time. Web site visitors who provide PII via a request for information can request to review, update or delete the PII provided at any time. Staff members can update PII during performance reviews or via secure Intranet. Partners/grantees who provide contact information (PII) to participate in the NERRs Intranet site established for collaboration or to enter data into grantee performance measurement tracking systems can review, update, or delete their PII upon request at any time. Vendors or grantees can review/update BII at any time upon request to the NOS proposal contact.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access to PII is tracked via logging of network directory access; logging of secured database access; and logging of Intranet administrative access.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): ***3/27/2018*** ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones. An independent A&A is scheduled for completion by March 2017. All findings will be analyzed and will undergo NOS POA&M Management Process that could result in risk acceptance or creation of a POA&M.
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

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

Secured database

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

Secured file/folder network directory

- OCM enforces assigned authorizations for controlling access to the system through the use of logical access control policies. Access controls lists are configured to enforce access authorization and assign user and group privileges. These access

	control policies are employed to control the access between users and objects (files, directories, servers, printers, etc.). Access enforcement mechanisms are in place at the network, system and application levels. Plans for encryption at rest: OCM's SQL Server databases are SQL v 2012 Standard Edition. This version/edition does not allow for straightforward encryption and therefore the PII data stored in our secure database is not encrypted. We secure the database via access control and configuration management as stated above. OCM does intend to upgrade to SQL 2016 SP1 as soon as possible, and at latest, by 9/30/2017. This upgrade will provide a straightforward pathway to database encryption. In addition, we are actively engaged in moving applications and databases into Microsoft Azure which also provides automatic SQL DB encryption.

Section 9: Privacy Act

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

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

x	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: Existing Privacy Act system of records notices (SORNs) for NOAA cover the personnel information in this system: COMMERCE/DEPT-18 - Employees Personnel Files Not Covered by Notices of Other Agencies and NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission. Also, DEPT-2, Accounts Receivable; DEPT-6, Visitor Logs and Permits for Facilities under Department Control; DEPT-13, Investigative and Security Records; DEPT-25, Access Control and Identity Management System; and GSA/Govt-7, Federal Personal Identity Verification Identity Management System.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

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

x	There is an approved record control schedule. Provide the name of the record control schedule: The retention period for these records is guided by the

	General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the federal government. The underlying paper records relating to employees are covered by GRS 1, Civilian Personnel Records. In accordance with GRS 20, item 3, electronic versions of records scheduled for disposal under other records schedules may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. Guidance for these records in the NOAA Records Schedules refers disposition to GRS 20. NOAA Records Schedules Chapter 1600 – National Ocean Service (NOS) Functional Files describes records created and maintained in the National Ocean Service (NOS) on the ocean and coastal zone management services and information products that support national needs arising from increasing uses and opportunities of the oceans and estuaries. 1610-01 - Coastal Zone Management Program Documents 1610-02 - Program Change Files 1610-03 - Coastal Non-point Pollution Control Program 1610-04 - Federal Consistency 1610-05 - Program Administrative Guidance 1610-06 - The Coastal and Marine Management Program Information System
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
x	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	x	Overwriting	x
Degaussing	x	Deleting	x
Other (specify):			

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

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

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

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

x	Identifiability	Provide explanation: 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.
x	Quantity of PII	Provide explanation: Information collected is limited to a small subset of specific applications and personnel files.
x	Data Field Sensitivity	Provide explanation: Phone numbers and e-mail addresses are the primary information collected, and are used for communication purposes.
x	Context of Use	Provide explanation: The vast majority of PII collected is used for emergency contact information for staff members, or for communicating back to information requesters.
	Obligation to Protect Confidentiality	Provide explanation:
x	Access to and Location of PII	Provide explanation: Concept of least privilege; secure network and database; encrypted storage and transmission
	Other:	Provide explanation:

Section 12: Analysis

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

X	Yes, the conduct of this PIA results in required business process change. Explanation: Addition of Privacy Act Statements to several sites.
	No, the conduct of this PIA does not result in any required business process changes.

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

X	Yes, the conduct of this PIA results in required technology changes Explanation: addition of Privacy Act Statements to several sites.
	No, the conduct of this PIA does not result in any required technology changes.

Appendix – Privacy Act Statements

NOAA OCM Privacy Act Statement (Contact Us)

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: NOAA Office for Coastal Management (OCM) collects this information for the purpose of responding to "contact us" form requests and subscriptions to newsletters from NOAA OCM websites.

Routine Uses: NOAA will use this information to respond to requests submitted on the Contact Us page and for subscriptions to newsletters as selected on the contact us form. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a**)** to be shared for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice Commerce/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.

Disclosure: Furnishing this information is voluntary.

NOAA OCM Privacy Act Statement (OCM Intranet)

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: NOAA Office for Coastal Management (OCM) collects this intranet information for employee emergency and administrative contact purposes.

Routine Uses: NOAA will use this information for emergency or administrative contact purposes. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a**)** to be shared among NOAA staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice Commerce/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.

Disclosure: Furnishing this information is voluntary.

NOAA OCM Privacy Act Statement (Partner Contact Information)

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: NOAA Office for Coastal Management (OCM) collects this information for the purpose of publishing the contact information of partners who provide services or resources on NOAA OCM websites.

Routine Uses: NOAA will use this information on public websites to identify points of contact for various resources listed on the NOAA Office for Coastal Management websites. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a**)** to be shared for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice Commerce/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.

Disclosure: Furnishing this information is voluntary.

NOAA OCM Privacy Act Statement (CZM Performance Measures)

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: NOAA Office for Coastal Management (OCM) collects this intranet information for user authentication, performance measurement project tracking and administrative contact purposes.

Routine Uses: NOAA will use this information for authentication, performance measurement project tracking and administrative contact purposes. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a**)** to be shared among NOAA staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice Commerce/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.

Disclosure: Furnishing this information is voluntary.

NOAA OCM Privacy Act Statement (NERRs Intranet and Performance Measures)

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: NOAA Office for Coastal Management (OCM)collects this intranet information for user authentication, organizational directory, performance measurement tracking, and administrative contact purposes.

Routine Uses: NOAA will use this information for authentication, organizational directory, employee emergency, and administrative contact purposes. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a**)** to be shared among NOAA staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice Commerce/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.

Disclosure: Furnishing this information is voluntary.