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

Privacy Impact Assessment
for the
NOAA6602
Office Of National Marine Sanctuaries (ONMS)

Reviewed by: Robin Burress FOR 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

BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2023.07.07 07:53:18 -04'00' 07/07/23

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/NOS/ONMS

Unique Project Identifier: NOAA6602

Introduction: System Description

Provide a brief description of the information system.

The Office of National Marine Sanctuaries (ONMS), part of the National Oceanic and Atmospheric Administration (NOAA), serves as the trustee for a network of underwater parks that encompass more than 600,000 square miles of marine and Great Lakes waters from Washington State to the Florida Keys, and from Lake Huron to American Samoa. The National Marine Sanctuary System (NMSS) includes 15 national marine sanctuaries and Papahānaumokuākea and Rose Atoll marine national monuments.

Since 1972, the ONMS has worked cooperatively with the public and federal, state and local officials to promote conservation while allowing compatible commercial and recreational activities. Increasing public awareness of our marine heritage, scientific research, monitoring, exploration, educational programs and outreach are just a few of the ways the ONMS fulfills its mission to the American people.

ONMS has not added or removed any applications that would cause a change in privacy risks.

Address the following elements:

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

NOAA6602 is an information technology (IT) general support system (GSS) that services all fifteen Office of National Marine Sanctuaries sites nationwide. NOAA6602 is a GSS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system temporarily stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

(b) System location

Channel Islands NMS University of California Santa Barbara	Santa Barbara	CA
Cordell Bank	Point Reyes	CA
Florida Keys NM	Key West	FL
Florida Keys NMS	Key Largo	FL
Flower Garden Banks	Galveston	TX
GovDelivery	Saint Paul	MN
Gray's Reef NMS	Savannah	GA

Greater Farallones	San Francisco	CA
Hawaiian Islands Humpback Whale NMS	Honolulu	HI
HIHWNMS Maui Office	Kihei	HI
Monitor NMS	Newport News,	VA
Monterey Bay	Monterey	CA
National Marine Sanctuaries HQ	Silver Spring	MD
National Marine Sanctuary of American Samoa	Pago Pago	
NOS Azure Central US		IA
NOS Azure East US2		VA
Olympic Coast NMS	Port Angeles	WA
Papahānaumokuākea Marine National Monument	Honolulu	HI
Papahānaumokuākea Marine National Monument - Hilo	Hilo	HI
Santa Cruz NMS	Santa Cruz	CA
Stellwagen Bank	Scituate	MA
Thunder Bay NMS	Alpena	MI
West Coast Region NMS	Monterey	CA

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

NOAA6602 uses the network services of NOAA6001.
NOAA6602 uses the Security Services of NOAA0100.
NOAA6602 uses the Network Services of NOAA0550.
NOAA6602 Uses the directory services of NOAA0700.
NOAA6602 Uses the Google Suite of NOAA0900
NOAA6602 use the Microsoft-Azure Commercial Cloud Package ID F1209051525

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

OSPREY
An applicant for a research permit downloads the permit application from the ONMS website. Once completed the application is sent by the US postal Service or delivered in person to an ONMS facility. Permit Coordinators at each site enter the completed permit into the OSPREY applications secure web interface. Permit coordinators at each assign a unique number to each permit provide by the OSPREY application. Permit Coordinators at each ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted. The ONMS permit application is assigned to Government agencies, Universities and companies that wish to conduct research within the sanctuaries.

UAV
Uncrewed Autonomous Vehicles are uncrewed vehicles that are used to collect scientific data. This includes Aeronautical Systems as well as, uncrewed surface vehicles and uncrewed submersible vehicles. These uncrewed vehicles are used to capture photogrammetry (e.g. living marine resources and sanctuary mapping) and meteorological data. UAV requirements and

procedures are documented in the ONMS Privacy Policy, UAV Policy which includes the ONMS Data Security Plan. All three types of vehicles have the potential to collect PII. ONMS will treat all UAV similarly to prevent inadvertent PII collection. The policies and procedures are updated annually or when changes occur.

Tier 2 Web
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. The home website for NOAA6602 is http://sanctuaries.noaa.gov and the privacy policy for ONMS is https://sanctuaries.noaa.gov/about/privacy.html.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https://policy.cio.gov/web-policy/analytics), which states:

- All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And
- Agency use of web measurement and customization technologies must comply with 0MB Memorandum M-10-22, Guidance for 0nline Use of Web Measurement and Customization Technologies".
- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

Acquisition

ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

HR Data
ONMS, during the hiring process or in assisting employees with travel preparation, uses information stored in the DOC eOPF, EPP, and Etravel systems. ONMS also uses the NOAA staff directory for employee information. ONMS does not use paper copies for HR data. ONMS follows the DOC and NOAA Policy guidance for HR. Additional requirements or procedures are documented in the ONMS Privacy Policy and Procedure. The Privacy Policy and Procedure is updated annually or when changes to the system occur.

ONMS Public Websites
ONMS websites are the only publicly accessible location for ONMS information. Data on ONMS websites may include audio and video designated for the general public. Information on the ONMS sanctuary websites may be viewed, over the HTTPS protocol, by the general public.

Sanctuary Advisory Council (SAC) Application
ONMS is developing a Web Application to receive applications for positions on the ONMS

Sanctuary Advisory Council. Sanctuary advisory council members consist of members of the public and representatives from local, state, and federal agencies. Members of the general public (those not appointed by a local, state, or federal agency to serve in a government seat) are the only applicants required to complete the application. This application is still in development with the potential for completion within the year.

GovDelivery
GovDelivery is a service managed by NOS. When viewing an ONMS website there is a statement "To receive information about this and other subjects click here". The visitor is required to enter their email twice before being taken to the ONMS instance of GovDelivery. The visitor may check boxes for newsletters they wish to receive. The only information retained by GovDelivery is an email address, the associated preferences and how many participants each topic has. Every newsletter sent includes an Opt Out link. The user may also visit the GovDelivery website and opt out there as well. ONMS employees who wish to send newsletters from GovDelivery or Monitor GovDelivery must first read and approve the NOS Rules of Behavior and submit a formal request to me as the ONMS ISSO. The ONMS ISSO reviews the GovDelivery user list quarterly.

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

Scientific data that is collected is published on NOAA6602 websites and in scientific journals. Nonpublic data is viewed on Government Furnished equipment while connected to the NOAA network or over the NOAA VPN. Nonpublic data requires user authentication. Public data may be viewed over the internet via the HTTPS: protocol. Public data does not require authentication.

OSPREY
Permit applications, with the applicant being an institution or organization, are given a unique identifier and are then retrieved using this identifier. Permit data can only be accessed by ONMS permit coordinators, while connected to the NOS internal network. ONMS permit coordinators access the OSPREY application via a Web Browser over the HTTPS.

UAV
Data on the UAV is captured by the UAV on encrypted internal media. The data is retrieved by the ONMS UAV operator when the data is directly connected to the UAV scientific computer. The UAV computer is not connected to any computer network. Data is first reviewed by the operator of the UAV to remove any inadvertent PII prior to transferring Non PII data to the ONMS network. UAV requirements and procedures are documented in the ONMS Privacy Policy and the UAV Policy. The UAV is also only operated in remote locations to avoid the potential to capture PII. The UAV is operated by Line Of Sight and or Ship based Radar is used to verify that there are no other vessels in the vicinity.

HR
ONMS, during the hiring process or to assist employees with travel preparation, uses information stored in the DOC eOPF, EPP and Etravel systems. ONMS also uses the NOAA staff directory for employee information. ONMS does not use paper copies for HR data. All access to this data is over the internal NOAA and DOC networks.

Acquisition data
Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Access to the data is restricted to the purchasing manager and the IT manager and can only be accessed over the internal NOS network or internally.

ONMS Public Websites
ONMS websites are the only publicly accessible location for ONMS information. Information on the ONMS sanctuary websites may be viewed, over the HTTPS protocol, by the general public. Only specific ONMS employees with access approved by the application owner, IT manager and ISSO may modify change or update the data over the internal NOAA network via HTTPS protocol. All images are for public release and may be downloaded by the general public over the HTTPS protocol.

GovDelivery
ONMS uses the NOAA6001 instance of Gov Delivery. This is an online communications tool that delivers public information of interest to customers of ONMS by email. Customers submit their email addresses to ONMS, which staff enter into GovDelivery for mail-outs. Only the email address is kept within the Gov Delivery system. Staff use this application to generate and send out newsletters and other materials. The only information stored in the Gov Deliver system is the email address.

Sanctuary Advisory Council (SAC) Application
ONMS is developing a Web Application in Microsoft Azure cloud to receive applications for positions on the ONMS Sanctuary Advisory Council. SAC applications are given a unique identifier and are then retrieved using this identifier. SAC data can only be accessed by ONMS SAC Coordinators and the ONMS General Council, while connected to the NOS internal network. ONMS SAC coordinators access the SAC application via a Web Browser over HTTPS. This application is still in development with the potential for completion within the year.

ONMS Flower Garden Banks Security System
ONMS FGB has a security system, which includes video security cameras. The video footage can only be viewed on an isolated network by authorized individuals and is only shared with law enforcement.

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

OSPREY
All communication, by the permit coordinators, to and from the OSPREY application is via HTTPS protocol.

UAV
The UAV data is hand carried from UAV to Scientific workstation.

HR
HR data is stored on the DOC eOPF, EPP and Etravel systems. Administrators access the data over the NOAA secure portal. Data is transmitted to and from the system over HTTPS.

Acquisition data
Acquisition data is stored on an access control list (ACL) controlled network share and access over the secured NOS network. Data transmission occurs on the NOS secure network.

ONMS Public Websites
ONMS websites are the only publicly accessible location for ONMS information. Information on the ONMS sanctuary websites may be viewed, over the HTTPS protocol, by the general public. Only specific ONMS employees may upload data to the ONMS websites. The public may view the public websites but cannot upload or alter the information on these sites.

GovDelivery
This is an online communications tool that delivers public information of interest by email to customers of ONMS. Customers submit their email addresses to ONMS, which staff enter into GovDelivery for mail-outs. Only the email address is stored within the Gov Delivery system. Staff use this application to generate and send out newsletters and other materials.

SAC
All communication, by the SAC coordinators, to and from the SAC application is via HTTPS protocol.

(g) Any information sharing

OSPREY
NOAA6602 only shares scientific data. Permit data is used internally. Any permit data shared does not include PII. Shared Permit data may include, location in the sanctuary where the permit will be used. Activity to be conducted with in the sanctuary. NON-PII data may be shared with Local, state and other federal agencies. Non-Shared data may include Name, Address, Email Address and phone number if applicable business Name, Address, Email Address and phone number.

SAC
NOAA6602 only shares scientific data. SAC data is used internally. SAC data collected includes Name, Address, Email Address and phone number if applicable business Name, Address, Email Address and phone number.

UAV data is processed then shared internally only.

Acquisition data is not shared. Acquisition data may include Business Name, Address, Email Address, phone number, the Item for purchase and the item cost.

GovDelivery data is not shared. The only data collected is an email address and user preference.

Security System. ONMS Flower Garden Banks office has a security system, which includes video security cameras. The video footage can only be viewed on an isolated network and is only shared with law enforcement. Signage is posted.

Only data and images designated for the public are available on ONMS websites and available for download over HTTPS.

Employee data is stored in the DOC eOPF, EPP and Etravel systems. Only employees with a need and approval may access HR data. ONMS uses the NOAA6001 file services for data storage but does not store PII on the network share. A limited amount of BII may be stored on the NOAA6001 file services in access-controlled shares.

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

ONMS Public Websites
The ONMS websites are used as a public outreach tool. ONMS websites are the only publicly accessible location for ONMS information. Information on the ONMS sanctuary websites may be viewed, over the HTTPS protocol, by the general public.

GovDelivery
GovDelivery is used as a public outreach tool.

OSPREY The Office of National Marine Sanctuaries administers the National Marine Sanctuaries Act, Executive Order 13158, Marine Protected Areas, and other authorities pertaining to designation and management of national marine sanctuaries and marine national monuments.

- The Marine Mammal Protection Act, 16 U.S.C. 1361 et seq.; the Fur Seal Act, 16 U.S.C. 1151 et seq.; and the Endangered Species Act, 16 U.S.C. 1531 et seq.
- Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531–332; 15 U.S.C. 1501 *et seq.*; 28 U.S.C. 533–535; 44 U.S.C. 3101; Equal Employment Act of 1972; and all existing, applicable Department policies, and regulations.
- E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O.12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.
- 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.
- 5 U.S.C. 3109, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533
- Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Un-crewed Aircraft Systems (Feb. 15, 2015); National Marine Sanctuaries Act, 16 U.S.C. 1431 *et seq.*; Marine Debris Act, 33 U.S.C. 1951 *et seq.;* Coast and Geodetic Survey Act, 33 U.S.C. 883a *et seq.*; Coastal Zone Management Act, 16

- U.S.C. 1451 *et seq.*; Coral Reef Conservation Act, 16 U.S.C. 6401 *et seq.*; National Historic Preservation Act, 16 U.S.C. 470 *et seq.*; Ocean Pollution Act, 33 U.S.C. 2701 *et seq.*; Comprehensive Environmental Response, Compensation and Liability Act, 42 U.S.C. 9601 *et seq.*; Clean Water Act, 33
- U.S.C. 1251; 47 CFR parts 80, 87, and 95, U.S. Office of Management & Budget (OMB)Circular A–130; the Magnuson-Stevens Fishery Conservation and Management Act, 16
- U.S.C. 1801 *et seq.* (Magnuson-Stevens Act); High Seas Fishing Compliance Act of 1995, 16 U.S.C. 5501 *et seq.*; International Fisheries Regulations: Vessels of the United States Fishing in Colombian Treaty Waters: 50 CFR 300.120; the FAA Modernization and Reform Act of 2012 (Pub. L. 112–95); the American Fisheries Act, Title II, Public Law 105–277; the Atlantic Coastal Fisheries Cooperative Management Act of 1993, 16
- U.S.C. 5101–5108, as amended 1996; the Tuna Conventions Act of 1950, 16 U.S.C. 951–961; the Atlantic Tunas Convention Authorization Act, 16 U.S.C. Chapter 16A; the Northern Pacific Halibut Act of 1982, 16 U.S.C. 773 *et seq.* (Halibut Act), the Antarctic Marine Living Resources Convention Act of 1984, 16 U.S.C. 2431– 2444 and the Debt Collection Improvement Act, 31 U.S.C. 7701.
- National Marine Sanctuaries Act, Section 301(b)(2): The act "provide[s] authority for comprehensive and coordinated conservation and management of these marine areas, and activities affecting them" Conserving and managing these marine areas requires communicating about them, which requires a web presence. As many elements of conservation and management involve people, as do activities affecting them, it is important to be able to *show* people interacting with sanctuary ecosystems in various ways.
- Section 301(b)(4):

  The act tasks ONMS with "enhancing public awareness, understanding, appreciation, and wise and sustainable use of the marine environment, and the natural, historical, cultural, and archeological resources of the National Marine Sanctuary System."

  To enhance public awareness and understanding we must first of all have a web presence. Using photos of people enables us to communicate elements of understanding, appreciation, and sustainable use of the marine environment. Photos of people are also often essential to demonstrating the historical and cultural context of these places.
- Section 309(c)(1)

  "The Secretary may support, promote, and coordinate efforts to enhance public awareness, understanding, and appreciation of national marine sanctuaries and the System." Photographs of people enable us to support existing public awareness, understanding, and appreciation of the system while also promoting future public awareness, understanding, and appreciation.
- Section 301(c)(2) Activities under this subsection may include education of the general public, teachers, students, national marine sanctuary users, and the ocean and coastal resource managers."

  Video recordings, Audio recording and Photographs of people are often necessary for such education.

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

the system

ONMS is a FIPS 199 Moderate Security impact category.

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*		f. Driver's License	X	j. Financial Account	x
b. Taxpayer ID		g. Passport	X	k. Financial Transaction	x
c. Employer ID		h. Alien Registration	X	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:					

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

g. Citizenship		n. Religion			

u. Other general personal data (specify):

The **OSPREY** application collects the Applicant's name Business or Institution Mailing Address, Business or Institution Phone Number and Business or Institution email address. The potential exists for an applicant to provide personal information and is being included in this section as well as the work-related data section. The applicant must provide the following information: (1) the names, addresses, and telephone numbers of owner, captain, and applicant; (2) vessel name and home port; (3) USCG documentation number, state license, or boat registration number; (4) Length of vessel and primary propulsion type (i.e., motor or sail); (5) Number of divers aboard; and (6) Requested effective date and duration of permit.

The **UAV** does not collect any of the above data types.

GovDelivery only collects email addresses.

Financial Data Financial data is collected for use in the purchase of vendor products.

HR Data is stored in the DOC HR system.

SAC The applicant must provide the following information: their names, addresses, and telephone numbers. The application also collects the Applicant's name Business or Institution Mailing Address, Business or Institution Phone Number and Business or Institution email address. This application is still in early development.

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary		j. Proprietary or Business Information	X
c. Work Address	X	g. Work History	X	k. Procurement/contracting records	X
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		

l. Other work-related data (specify):

The **OSPREY** application collects Name, Address, phone number, and email address.

The **SAC** application collects both individual and business Name, Address, phone number, and email address.

The **UAV** does not collect any of the above data types.

ONMS, during the hiring process or to assist employees with travel preparation uses information stored in the DOC eOPF, EPP and Etravel systems. ONMS also uses the NOAA staff directory for employee information.

ONMS does not use paper copies for HR data.

GovDelivery only collects email addresses.

HR Data is stored in the DOC HR system.

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	X
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. Other distinguishing features/biometrics (specify):
ONMS places photographic images on their web site. ONMS web sites contain images of staff, volunteers and affiliates, guest and visitors to ONMS sites. These include photographs and videos of events and interviews that occur at our sites.

Various applications, permits and HR forms require signatures.

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify): The NOAA6602 OSPREY application uses the NOAA ICAM to authenticate the permit coordinators. Only ONMS permit coordinators have access to the OSPREY application Auditing of ONMS permit coordinator access is sent to NOAA ArcSight. ArcSight records User ID, date, and time of access to the OSPREY system.					

Other Information (specify)
SAC: The SAC application is still in development. In addition to the information outlined above, applicants may also be asked to complete a number of questions to assist in the application review process. Typically, questions would seek information on applicant familiarity with the sanctuary, expertise and professional affiliation, and understanding the purpose and function of an advisory council.

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		Email	X		
Other (specify): Gov Delivery User email addresses are submitted online from the ONMS websites. Osprey is located in the ONMS instance of the OSPREY cloud. **SAC**: Source of PII/BII may be collected by submitting a hard copy of the application in-person or in the future online through a fillable application					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify): **SAC**: PII/BII may be collected through General Counsel Oceans and Coasts background vetting process and through NOS's departmental bureau check.					

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

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

OSPREY The completion of ONMS permits is an interactive task completed by the applicant and the ONMS permit coordinator. The permit process is accomplished over multiple weeks and requires interaction between the applicant and permit coordinator. During this process, the permit coordinator contacts the applicant via Email and phone calls and verifies information provided.

Acquisitions
Acquisition data is reviewed by the contracting officer. Data is verified by the contracting officer contacts via Email and phone calls; this process is used to verify information provided by the vendor.

HR Data
ONMS, during the hiring process or to assist employees with travel preparation, uses information stored in the DOC eOPF, EPP and Etravel systems. ONMS also uses the NOAA staff directory for employee information. ONMS does not use paper copies for HR data. HR data is validated at the time of hiring by the HR representative. The HR representative compares picture ID and other information to validate the applicant's identity. For travel, the HR representative also validates the users Driver's License and Passport if necessary. HR data for travel is only used to assist the employee in making travel arrangements and is not stored.
GovDelivery
The communications team reviews user data at least annually through user audits. If the data is outdated, the email audit will return an undeliverable message and admin deletes the user from the database. The user can also reply that they would like to be removed from the system or use the unsubscribe function in the email. The administrators review users' data prior to inputting into the system and the user reviews their data at various points in the process.

UAV
The ONMS UAV is used for mapping the ONMS sanctuaries in remote locations and is not used as a source for PII.

SAC: All information collected in the application is verified through a background checking process with ONMS General Counsel.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB control Numbers: • 0648-0141, National Marine Sanctuary Permits • 0648-0432 Dr. Nancy Foster Scholarship Program • 0648-0397 Application Form for Membership on a National Marine Sanctuary Advisory • 0648-0719 National Oceanic and Atmospheric Administration's Papahanaumokuakea Marine National Monument and University of Hawaii Research Internship Program • 0648-0582 Evaluation of Public Visitors' Experience of Exhibits at Mokupapapa Discovery Center • 0648-0548 Papahanaumokuakea Marine National Monument Permit Applications and Reports for Permits • 0648-0682 Nomination Process for National Marine Sanctuaries
	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): SAC application may collect PII similar to the OSPREY application and when complete will reside on a similar platform.			

	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	
Video surveillance	X	Electronic purchase transactions	
Other (specify): **UAV Only:** Although the ONMS UAV has the potential to collect PII via video surveillance, it is not the purpose of the device and any PII captured is immediately deleted. The UAV is also only operated in remote locations to avoid the potential to capture PII. The UAV is flown with Line Of Sight and or Ship based Radar is used to verify that there are no other vessels in the vicinity. **Security System.** ONMS Flower Garden Banks office has a security system which includes video security cameras. The video footage can only be viewed on an isolated network by authorized individuals and is only shared with law enforcement. Signage is posted.			
	There are not any IT system supported activities which raise privacy risks/concerns.		

Section 4: Purpose of the System

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

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	X
Other (specify): **ONMS** Both the National Marine Sanctuaries Act and ONMS regulations prescribe procedures by which certain activities that would otherwise be prohibited may be conducted through the issuance of a permit. Any person proposing to conduct an activity prohibited by ONMS regulations must apply for and receive a permit prior to conducting that activity. There are nine types of permits, including those for research, education, and special use activities. **HR**: ONMS, during the hiring process or to assist employees with travel preparation uses information stored in the DOC eOPF, EPP and Etravel systems. ONMS also uses the NOAA staff directory for employee information. ONMS does not use paper copies for HR data. ONMS also uses HR information such as travel authorization and			

vouchers, passports and international travel forms, and information for transmitting the security badge request email.

Information sharing:
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. The use of Tier 2 multi-session II is a requirement by the Federal CIO (https://policy.cio.gov/web-Policy/analytics). Information shared is scientific data only.

Photographic images on Web sites
ONMS collects and displays photographs, audio and video files on their websites in support of the education and outreach portion of the National Marine Sanctuaries act.

- Portions of the National Marine Sanctuary provide[s] authority for comprehensive and coordinated conservation and management of these marine areas, and activities affecting them"

  Conserving and managing these marine areas requires communicating about them, which requires a web presence. As many elements of conservation and management involve people, as do activities affecting them, it is important to be able to show people interacting with sanctuary ecosystems in various ways.

- Section 301(b)(4):

  The act tasks ONMS with "enhancing public awareness, understanding, appreciation, and wise and sustainable use of the marine environment, and the natural, historical, cultural, and archeological resources of the National Marine Sanctuary System." To enhance public awareness and understanding we must first of all have a web presence. Using photos of people enables us to communicate elements of understanding, appreciation, and sustainable use of the marine environment. Photos of people are also often essential to demonstrating the historical and cultural context of these places.

- Section 309(c)(1)

- "The Secretary may support, promote, and coordinate efforts to enhance public awareness, understanding, and appreciation of national marine sanctuaries and the System. “Photographs of people enable us to support existing public awareness, understanding, and appreciation of the system while also promoting future public awareness, understanding, and appreciation.

- Section 301(c)(2)

  "Activities under this subsection may include education of the general public, teachers, students, national marine sanctuary users, and the ocean and coastal resource managers." Photographs of people are often necessary for such education.

SAC: The ONMS Sanctuary Advisory Council application will receive applications containing PII from the public. The applications are used to apply for positions on the Sanctuary Advisory Council. The application will use a frontend to accept the application but store the application in a location not accessible external to ONMS.

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).

ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

ONMS, during the hiring process or to assist employees with travel preparation, uses information stored in the DOC eOPF, EPP and Etravel systems. ONMS also uses the NOAA staff directory for employee information. ONMS does not use paper copies for HR data. This includes electronic copies of resumes stored temporarily during the hiring phase. Also stored temporarily are standard HR information such as travel authorization and vouchers, passports and international travel forms, and information for transmitting the security badge request email, which includes only an email address and possibly a phone number.

UAV

UAV are used for mapping photogrammetry living marine resources and sanctuary mapping and meteorological data. ONMS' use of the UAV is covered by the DOC SORN and the ONMS UAV Policy. The UAV would be exclusively operated in remote areas and is not authorized to operate above people or structures. The UAV is operated line of sight to prevent the inadvertent capture of PII. Ship based radar is also used to ensure the area is free of other vessels. Any privacy data that is inadvertently collected will be immediately deleted.

OSPREY

1. The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries. A brief description of some permits are as follows:

(a) General Permits

Scope of this category. This category includes all permits not specifically addressed in subsections (b) through (j) below; typically, permit applications for scientific research, education, management, and salvage (excluding activities aimed at historical resources) activities permits, which fall into this category. This category also includes requests for authorizations of another agency permits processed pursuant to 15 CFR §922.49.

(b) Baitfish Permits

Scope of this category. This category includes applications for permits to collect baitfish in certain Sanctuary Preservation Areas (SPAs) of the Florida Keys National Marine Sanctuary that are otherwise closed to fishing. There are two types of baitfish permits that may be issued depending on the gear used (castnet or hairhook).

(c) Special Use Permits

Scope of this category. This category includes all permit applications processed under section 310 of the NMSA (16 U.S.C. §1441). Activities must be noticed in the Federal Register before NOAA can issue special use permits for those activities. Presently, these activities are as follows:

- The disposal of cremated human remains by a commercial operator in any national marine sanctuary
- The operation of aircraft below the minimum altitude in restricted zones of national marine sanctuaries for commercial purposes
- The placement and subsequent recovery of objects associated with public events on non-living substrate of the seabed
- The discharge and immediate recovery of objects related to special effects of motion pictures; and

- The continued presence of submarine cables beneath or on the seabed.

- Historical Resource Permits

Scope of this category. This category includes all permit applications for activities aimed at historical, cultural, and/or maritime heritage resources of sanctuaries.

- Certification

Scope of this category. This category includes all requests for the ONMS to certify activities that are being conducted pursuant to a valid government authorization prior to a sanctuary being designated (commonly known as "grandfathered" activities).

- Voluntary Registry

Scope of this category. This category is for researchers who are conducting activities that are not otherwise prohibited. The registry allows them to register their activity, which adds to the database of research activities within a sanctuary.

- Tortugas Access Permits

Scope of this category. In 2001, NOAA established the Tortugas Ecological Reserve in the Florida Keys National Marine Sanctuary. Regulations implementing the reserve include controlling access to the reserve through the granting of "access permits" (15 CFR §922.167). Applicants give their information and receive their permit orally, via phone or VHF radio, prior to entering the reserve.

- Lionfish Permits

Scope of this category. Florida Keys National Marine Sanctuary encourages the safe removal of invasive lionfish from its waters and issues lionfish removal permits to divers for the collection of lionfish from Sanctuary Preservation Areas (SPAs). The permit allows lionfish to be removed from the SPAs, which are otherwise no-fishing, no-take zones, with hand nets or slurp guns only. Spear guns or pole spears may not be used. This permit does not allow lionfish removal from the Ecological Reserves or the four Special-use Research only Areas.

2. When designating each sanctuary, NOAA consulted with the relevant states and Federal agencies regarding their permitting requirements and procedures. Where appropriate, agreements were put in place to use a coordinated permit process. Post-designation, the ONMS continuously works with other state and Federal agencies to identify and eliminate duplication of permit requirements or conditions and, when appropriate, coordinate reviews of applications. In addition, the ONMS routinely accepts information developed for other purposes (e.g., a report on an activity developed for another agency) as part of an ONMS permit application or to meet requirements of an ONMS permit condition.

When designating each sanctuary ONMS reviews public comment on the Federal Register. ONMS does not directly solicit public comment.

ONMS Public Websites

ONMS uses photographs, Audio recordings, and Video Recordings on our websites to:

- Illustrate main points and support textual information;

- Provide visual interest; and
- Show examples of sanctuary wildlife, locations, and forms of compatible use and engagement with the resources.

We use a variety of images of people on our websites. Some are from sanctuary events (like wildlife watching tours or SAC meetings); others are photos the ONMS production team takes; others are submitted via the photo contest.

Images of people support all of those uses. They support textual information about recreation, science and citizen science, volunteering, and other programs. They provide visual interest to the reader. And they are essential for showing forms of compatible use, engagement with sanctuary resources (wildlife watching, science, recreation, volunteer activities, commercial activities such as fishing, etc.), and sanctuary programming.

ONMS only publishes photographic images of individuals and children that they have signed releases for. ONMS publishes images of large crowds where individuals do not expect to have a right to privacy. At large crowd events signage is posted alerting individuals that photography is in use and they can inform ONMS if they do not wish to be photographed or have their image posted on the ONMS website.

ONMS web sites contain images of staff, volunteers and affiliates, guest and visitors to ONMS sites. These include photographs and videos of events and interviews that occur at our sites.

GovDelivery:
ONMS uses GovDelivery to provide information to constituents on information about ONMS. Constituents may sign up for various ONMS newsletters. ONMS only collects email addresses and the newsletter the constituent wishes to receive. ONMS does not associate any other information with this PII collection.

SAC:
The SAC application will be used to select applicants to the Sanctuary advisory Council. The information will only be shared internally with the ONMS General Council and externally with law enforcement. All applications will be stored on an encrypted database only accessible internally. No data will reside externally to ONMS. Information is collected from members of the public who voluntarily apply for Council seats.

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.).

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.

Old data is purged from the systems per retention schedule.

There is a potential for insider threat. However, users take privacy training at least annually in the required annual security awareness course.

Users sign rules of behavior to ensure they understand their responsibilities.

ONMS data is encrypted at rest and in transit.

All users are only given the access necessary to complete their job.

UAV

The data captured by the UAV is encrypted through the system. In order to fully exploit the data, it must be converted from the proprietary software and saved into commonly accessible formats. If the UAV was lost, data can only be decrypted by the Proprietary base unit when the UAV is connected to it. The UAV has the potential to collect PII if it inadvertently operated over an individual. The UAV is operated by line of sight and or by using ship-based radar to insure no other vessels are in the vicinity. All three types of UAV have the potential to collect inadvertent PII.

ONMS Public Websites Audio, Video and Photographic images on Web sites

ONMS uses Audio, Video and photographs on our websites to:

- Illustrate main points and support textual information;
- Provide visual interest; and
- Show examples of sanctuary wildlife, locations, and forms of compatible use and engagement with the resources.

Images of people support all of those uses. They support textual information about recreation, science and citizen science, volunteering, and other programs. They provide visual interest to the reader. And they are essential for showing forms of compatible use, engagement with sanctuary resources (wildlife watching, science, recreation, volunteer activities, commercial activities such as fishing, etc.), and sanctuary programming.

We use a variety of images of people on our websites. Some are from sanctuary events (like wildlife watching tours or SAC meetings); others are photos the ONMS production team takes; others are submitted via the photo contest.

The National Marine Sanctuaries Act, Section 301(b)(4), tasks ONMS with "enhancing public awareness, understanding, appreciation, and wise and sustainable use of the marine environment, and the natural, historical, cultural, and archeological resources of the National Marine Sanctuary System." Using photos of people enables us to communicate elements of understanding, appreciation, and sustainable use of the marine environment. Photos of people are also often essential to demonstrating the historical and cultural context of these places.

ONMS web sites contain images of staff, volunteers and affiliates, guest and visitors to ONMS sites. These include photographs and videos of events and interviews that occur at our sites.

ONMS only publishes photographic images of individuals and children that they have signed releases for. ONMS publishes images of large crowds where individuals do not expect to have a right to privacy. At large crowd events signage is posted alerting individuals that photography is in use and they can inform ONMS if they do not wish to be photographed or have their image posted on the ONMS website.

GovDelivery:
GovDelivery collects email addresses and the data the addresses wish to receive. There is a minimal PII risk if the email address was leaked.

NOAA6602 uses Microsoft - Azure Commercial Cloud Package ID F1209051525
All traffic to and from Azure is encrypted. Data is stored in encrypted database within Azure.

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):			

* Includes instances of security or privacy breach.

	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?

X	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	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	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: NOAA6602 Uses the NOAA0100 for the reporting of security incidents. *When a security incident occurs, we may need to submit Privacy information in the NOAA NIRRA system over HTTPS:* NOAA6602 uses the NOAA0550 NWAVE. *NWAVE is the service provider for ONMS and is used for network connectivity. NWAVE encrypts all network traffic. Network communications is provided over VPN or behind a Trusted Internet Connection.* NOAA6602 uses the NOAA0700 High Availability Enterprise Services for ICAM authentication. *ONMS requests that users do not transmit PII via email. ICAM communication uses SSL certificates. NOAA provides Kiteworks for the transmission of secure email.* NOAA6602 Uses NOAA6001 for Management of Network devices and for Network Services. NOAA 6001 also manages the firewalls protecting ONMS communications. *ONMS requests that users do not store PII on network drives provided by NOAA6001. NOAA6001 manages all network devices including firewalls that prevent data leakage.* NOAA6602 uses Microsoft - Azure Commercial Cloud Package ID F1209051525 *All traffic to and from Azure is encrypted. Data is stored in encrypted database within Azure.*
	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 only privacy information shared with the general public are photographic images and audio video available on ONMS web Sites for as described in ONMS Public websites. **OSPREY** The PII is only accessed by ONMS employees. **SAC** PII is only accessed by ONMS employees and the ONMS General Council			

Section 7: Notice and Consent

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

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://sanctuaries.noaa.gov/about/privacy.html .	
X	Yes, notice is provided by other means.	Specify how: **COOP:** Individuals are instructed verbally by their supervisor of the need for their contact information. The information is provided in hard copy form only to the users performing roles in the COOP function (ACIO, deputy ACIO, ISSO and CTO). Any employee data for the COOP is gathered from the employee on a voluntary basis when they agree to take the position. **HR**: Applicants and employees: Each individual federal form provides notice that their PII will be collected, and also includes Privacy Act Statements. **Acquisition:** Notice is contained in the applicable Request for Quote or Notice of Federal Funding Opportunity. **Audio, Video and Photographs on Web Pages** Photographic, Audio Recordings and Video recordings releases containing a Privacy Act Statement are obtained for all images of individuals except group photographs taken at public site events. Parental consent release forms are obtained for any image of children under the age of 18. **GovDelivery**: Gov. Delivery is a voluntary submission. ONMS does not solicit the information. If a Constituent wishes to participate, they may subscribe to ONMS newsletters by providing and email address. On the subscription page, the constituent has the option to delete their account if the subscription is by accident. The privacy policy for GovDelivery is contained on the ONMS privacy policy page. **SAC** A link is not available because the application is still in development. The privacy disclaimer will be similar to the OSPREY disclaimer. **Security System.** ONMS Flower Garden Banks office has a security system which includes video security cameras. The video footage can only be viewed on an isolated network by authorized individuals and is only shared with law enforcement. Signage is posted. **OSPREY** Only approved ONMS employees may access the OSPREY database. The ONMS, NOS and NOAA privacy policies are linked to the sign in page. https://osprey.nos.noaa/privacy.html This link is internal to the OSPREY application and only accessible if the user has permission. See attached screen shots. https://www.noaa.gov/protecting-your-privacy

X	No, notice is not provided.	Specify why not: Notice is not provided and releases are not obtained from individuals who are in a public venue, such as a beach or group event. ONMS does not use the UAV to capture images of individuals. All UAV are operated in remote locations. ONMS uses ship-based radar and or line of site operations to prevent the capture of images of individuals. In the rare event that an image of an individual was captured, it would be deleted.

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: **HR** Federal employees may decline in writing to provide PII to their supervisors, but this may affect their employment. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR). Information is provided on a voluntary basis through individuals who provide their business cards. If they do not want to be placed in the database, they do not provide business cards. **Photographs, Audio recordings and Video recordings on Web Pages** The individual can decline to provide audio, video or their image by not signing the release form. If an image has previously been uploaded to the web site, the individual can request to have the image removed from the web site. **GovDelivery**: Gov. Delivery is a voluntary submission. ONMS does not solicit the information. If a Constituent wishes to participate, they may subscribe by providing an email address to subscribe to ONMS newsletters. On the subscription page the constituent has the option to delete their account if the subscription is by accident. All ONMS web pages including the subscription page contain a link to the ONMS privacy policy. In addition, an email is sent to the email address provided confirming the subscription and provides a link to unsubscribe. **OSPREY** Permits to conduct activities in an ONMS sanctuary are received in person or via US mail. If an applicant does not wish to provide PII, they do not submit a permit application.

		Security System. ONMS Flower Garden Banks office has a security system which includes video security cameras. Individuals have the opportunity to decline to provide PII by not entering the area being surveilled. Appropriate signage is posted. **SAC** Applicants can choose not to apply and not submit an application. Information will be displayed alerting the applicant that we are collecting PII and why we need it, by submitting the application they agree to that collection. The application is still in development and will be similar to OSPREY.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: **UAV** ONMS does not use the UAV to capture images of individuals. All UAV are operated in remote locations. ONMS uses ship-based radar and or line of site operations to prevent the capture of images of individuals. In the rare event that an image of an individual was captured, it would be deleted.

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: **HR:** Applicants for positions who have applied through the USA Jobs system are able to consent to the use of their information in the system. Applicants for positions through contractor companies consent to the use of their information through their companies. For ongoing employee business, such as travel, the user consents to the use of their information by submitting travel requests to their admins. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR). **Photographs, Audio Recordings and Video Recordings on Web Pages** The proposed use of the photographic image, Audio Recordings and video recordings is described in the ONMS release form. Individuals may decline to consent to a particular use of their image by not signing the image release form. **GovDelivery:** GovDelivery is a voluntary submission with only one use for

		the information. ONMS does not solicit the information. If a Constituent wishes to participate the constituents may choose to subscribe by providing and email address to subscribe to ONMS newsletters. The link to the ONMS privacy policy is provided on all ONMS web pages and provides information on the use of PII. Users can unsubscribe on the subscription page or by the link on all emails sent to the constituent if they do not consent to the use of the information. **OSPREY** Permits to conduct activities in an ONMS sanctuary are received in person or via US mail. The use of the PII collected is explained in the permit application. If the applicant does not consent to the use of the PII they do not have to submit the application. **SAC** Applicants can choose not to apply and not submit an application. Information will be displayed alerting the applicant that we are collecting PII and why we need it, by submitting the Application they agree to use of their Pll for that collection. The application is still in development and will be similar to OSPREY.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: **Security System.** ONMS Flower Garden Banks office has a security system which includes video security cameras. The video footage can only be viewed on an isolated network by authorized individuals and is only shared with law enforcement. Signage is posted an individual may chose not to enter the facility and be recorded. All recorded footage is used for security purposes.

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: **HR** Applicants apply for positions through USA Jobs which allows the applicant to review and update information until the position closes. Contract employees initiate the change through their contracting company in person. Once an employee is hired, all changes and updates are made directly to the employee's HR representative. **Acquisition** The business works closely with the purchasing manager and any updates are made directly to the purchasing manager, in writing. **Photographs, Audio Recordings and Video Recordings on Web Pages** An individual may request to have their audio, video or photographic image removed from an ONMS website at any

		time by contacting ONMS. **GovDelivery**: All emails sent to ONMS constituents contain a link for individuals to modify or cancel their subscription. The confirmation email from GovDelivery also contains instructions of how to manage or delete subscriptions. **OSPREY** Permits to conduct activities in an ONMS sanctuary are reviewed multiple times by the applicant and the ONMS permit coordinator. The permit process can take many months to complete where the applicant can review and correct any information even after the approval of the permit. **SAC** Applications for Sanctuary Advisory Council Members are reviewed multiple times by ONMS employees and the ONMS General Council. Applicants will have multiple opportunities to update information during the review process.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: **UAV** ONMS does not use the UAV to capture images of individuals. All UAV are operated in remote locations. ONMS uses ship-based radar and line of site operations to prevent the capture of images of individuals. In the rare event that an image of an individual was captured, it would be deleted. **Security System.** ONMS Flower Garden Banks office has a security system which includes video security cameras. The video footage can only be viewed on an isolated network by authorized individuals and is only shared with law enforcement. Signage is posted an individual may chose not to enter the facility and be recorded. All recorded footage is used for security purposes.

Section 8: Administrative and Technological Controls

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

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. **Explanation:** Acquisition data is monitored and tracked temporarily until a procurement is concluded. It is kept on shared drives, access to which is restricted by access control lists (ACLs). Laptop tops are configured with full disk encryption. If PII is kept on a laptop, the data is encrypted. NOAA6602 restricts access to shared folders by ACL. PII is not centralized in a database, and it cannot

	be easily monitored for access. However, as stated above, the access to the shared folders is restricted by ACL. Employee evaluations and potential employee resumes are monitored and tracked temporarily, until transfer to the NOAA OHCS. They are kept on shared drives, access to which is restricted by ACL. NOAA policy requires users not to keep data on their local drives. Policy indicates that they should use restricted folders on the shared drive. Policy also requires users to remove all PII from their file share when no longer needed. The OSPREY application is located in an encrypted database stored in the ONMS instance of AZURE. Access to the OSPREY Application and Database is controlled by ICAM. SAC: The SAC application is still in development but will reside in an encrypted secure database similar to OSPREY. **Security System.** ONMS Flower Garden Banks office has a security system which includes video security cameras. The video footage can only be viewed on an isolated network by authorized individuals and is only shared with law enforcement. **Photographs, Audio Recordings and Video Recordings on Web Pages** All photographic, audio and video recordings are maintained on ONMS websites in the Azure cloud. All access to the ONMS websites require multifactor authentication from an internal ONMS IP address.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): January 10, 2023 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

OSPREY
The ONM Permit application (OSPREY) is hosted on a database. All communication with the application is using encryption for data in transit. Only approved Permit coordinators are allowed access to the OSPREY system. User access to the OSPREY database is controlled by NOAA enterprise directory. All access audit trails are uploaded to the NOAA enterprise audit logging solution, Audit solution.

UAV

The UAV system stores data on an encrypted SD card. All data is overwritten or the SD card is destroyed once the data is removed from the SD card. UAV procedures are documented in the data protection section of the ONMS UAV policy.

HR
ONMS, during the hiring process or in assisting employees with travel preparation, uses information stored in the DOC eOPF, EPP, and Etravel systems. ONMS also uses the NOAA staff directory for employee information. ONMS does not use paper copies for HR data.
ONMS follows the DOC and NOAA Policy guidance for HR.

Acquisition
Digital Acquisition data is stored on an ACL controlled networks file share accessible only by contract specialists. Paper copies of acquisition materials are stored in an access-controlled file cabinet.

SAC
The SAC application is still in development. It will reside on an encrypted database and use HTTPS for communications. The security measures will be similar to the OSPREY application.

All PII stored within Azure are stored in an Encrypted SQL database.
All PII and BII are encrypted at rest.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g,, name or Social Security number)?

X Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*
As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Authorizations Applicants COMMERCE/DEPT-13, Investigative and Security Records COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies COMMERCE/DEPT-29, Unmanned Aircraft Systems

	OPM/GOVT-5, Recruiting, Examining, and Placement Records NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission COMMERCE/DEPT-31, Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations COMMERCE/DEPT-25, Access Control and Identity Management Systems
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

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

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Schedules Chapter 1609 Marine Sanctuaries Chapter 2200 Records of the Chief Information Officer Chapter 2300 General Information Technology Management Record Chapter 2400 Information System Security Records **UAV** All data is overwritten or the SD card is destroyed once the data is removed from the SD card. Any PII collection is incidental, unintentional, and not retained. See DEPT-29, Section 9.1 UAV procedures are documented in the data protection section of the ONMS UAV policy.
	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		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	Provide explanation: Individuals may be identified by the provision of their contact information. A limited number of individuals may be identified by name on ONMS websites.
X	Quantity of PII	Provide explanation: There is a small quantity of PII. There are a limited number of photographic images that identify individuals.
X	Data Field Sensitivity	Provide explanation: Acquisition and performance ratings are collected. Driver's License, Passport, Alien Registration cards may be temporarily collected, but are destroyed when no longer necessary.
X	Context of Use	Provide explanation: OSPREY Permit data is used to generate permits for activity conducted within one of the ONMS sanctuary. UAV Data is used to produce wildlife maps. Photographs, Audio Recordings and Video recordings on Web Pages. Prior to publication individuals are informed of the use of their images on ONMS websites. GovDelivery Users who submit their email address can opt out at any time. HR Data ONMS uses HR data temporarily to assist with travel and in the hiring process. All HR data is stored in the DOC HR systems. Acquisitions ONMS uses acquisition BII in awarding contracts SAC ONMS uses information collected by the SAC application to evaluate candidates for open positions on the Sanctuary Advisory Council

X	Obligation to Protect Confidentiality	Provide explanation: Per the FAR, Procurement Integrity Act, and Economic Espionage Act
X	Access to and Location of PII	Provide explanation: OSPREY Data is stored in an encrypted database with restricted access to the database. Permit coordinators are granted access to the database after review by the IT manager, OSPREY manager and ISSO. UAV The UAV data is only transferred by a UAV operator and can only be transferred to an ONMS scientific workstation. Photographic Audio Recordings and Video recordings on Websites. Images of individuals are stored in access controlled, encrypted and isolated Network Access Server (NAS) devices. Access is limited to specific ONMS employees. Photographic images published on ONMS websites can only be updated by the ONMS web admin. All images published on ONMS websites are available to the general public. GovDelivery The GovDelivery database stores email addresses only and is managed by NOAA6001. HR Data ONMS uses HR data temporarily to assist with travel and in the hiring process. All HR data is stored in the DOC HR systems. Acquisitions ONMS uses acquisition BII in awarding contracts. SAC Data will be stored in a database with restricted access to the database. SAC coordinators are granted access to the database after review by the IT manager, SAC manager and ISSO.
X	Other:	Provide explanation: **GovDelivery** The GovDelivery database stores email addresses only.

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.)

ONMS re-evaluated the system impact level (FIPS-199) and upgraded the FISMA system impact level to Moderate. The data fields that are implemented were reviewed on multiple occasions to ensure that only the necessary data is collected, especially PII. The ONMS ISSO is included in all meetings.

OSPREY
The ONMS ISSO works closely with the OSPREY team to ensure the application only collects the minimal amount of data. The ONMS permit application specifically requests Business address, phone number and email address, however, due to the potential that an applicant may inadvertently supply PII, ONMS protects the OSPREY application at the higher more secure level.

UAV
The UAV has a low risk of threat to privacy since it is operated only in remote locations and they are not authorized above buildings or people. The UAV is operated by line of sight and or by using ship-based radar to insure no other vessels are in the vicinity.

SAC
The SAC application currently poses a low risk to privacy because it is still in development. The ONMS ISSO is working closely with the application owner and the application developer to insure proper security.

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.

Web Site Privacy Policy (on OSPREY internal site)

Privacy Policy

We are committed to the privacy of our visitors. We collect no personal information about you when you visit our Web site unless you choose to provide that information to us.

Here is how we handle information about your visit to our Web site:

Information Collected and Stored Automatically: If you do nothing during your visit but browse through the Web site, read pages or download information, we will gather and store certain information about your visit automatically. This information does not identify you personally. We automatically collect and store information like the following concerning your visit.

- The Internet domain (for example, "xcompany.com" if you use a private Internet access account, or "yourschool.edu" if you connect from a university's domain);
- Your IP address (an IP address is a number that is automatically assigned to your computer whenever you are surfing the Web) from which you access our Web site.
- The type of browser and operating system used to access our site;
- The date and time you access our site;
- The pages you visit; and
- If you linked to our Web site from another Web site, the address of that Web site. We use this information to help us make our site more useful to our visitors by allowing us to learn more about the number of visitors to our site and the types of technology our visitors use.

Information Protection

For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. If such monitoring reveals evidence of possible abuse or criminal activity, such evidence may be provided to appropriate law enforcement officials. Unauthorized attempts to upload or change information on this server are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act or other law.

Information That You Voluntarily Provide

We do not collect personally-identifiable information unless you choose to provide it to us. If you provide us with personally identifiable information, for example by sending an e-mail or by filling out a form and submitting it through our Web site, we use that information only to respond to your message and to help us provide you with the information and services that you request. Submitting voluntary information constitutes your consent to the use of the information for the stated purpose. When a user clicks the "Submit" button on any of the Web forms found on our site they are indicating voluntary consent to use of the information they submit for the stated purpose. We do not collect or use information for commercial marketing.

How Information is Used

The information we collect is used for a variety of purposes (e.g., comments on proposed rules, license applications, to respond to requests for information about our regulations and policies

and to fill orders).

We make every effort to disclose clearly how information is used at the point where it is collected so that our users can determine for themselves whether they wish to provide the information.

Sharing of Information

We may share the information you give us with another government agency if your inquiry relates to that agency. In other limited circumstances, such as responses to requests from Congress and private individuals, we may be required by law to disclose information you submit. Before you submit personally identifiable information, such as on an online form, you will be advised as to the purpose and how the information will be used. We may also share information collected during your visit with non-federal entities, but only if your inquiry requires accessing data from that external entity. All of our sites that require such external access will be clearly identified to help you make an informed choice.

Third-party Social Media Tools

We use third-party social networking/social media tools as a supplemental channel to promote awareness of Office of National Marine Sanctuaries (ONMS) activities, events, news, and information. Those tools include:

Facebook

Facebook is a social networking website where users can connect and interact with other people. We typically post something new on our wall every workday to keep you up-to-date with ONMS news and information. Please note that you are subject to Facebook's privacy policy when visiting our Facebook page.

Instagram

Instagram is an photo- and video-sharing social network website and app where users can connect with others through imagery. We typically post to our Instagram account daily to give you a glimpse of the National Marine Sanctuary System. Please note that you are subject to Instagram's privacy policy when visiting our Instagram page.

Tumblr

Tumblr is a microblogging and social networking website. We typically post at least once a day to let you know what's new in the National Marine Sanctuary System and to bring you fun and interesting facts about your national marine sanctuaries and marine national monuments. Please note that you are subject to Tumblr's privacy policy when visiting our Tumblr.

YouTube

YouTube is a video sharing service. The videos we share on YouTube are copies of those that appear in the video gallery on the ONMS website. Please note that you are subject to YouTube's privacy policy when visiting our YouTube page.

Twitter

Twitter is a microblogging service to communicate and stay connected through the exchange of short, frequent posts. We typically tweet once each business day to keep you abreast of what's new in our National Marine Sanctuaries. Please note that you are subject to Twitter's privacy policy when visiting the ONMS Twitter page.

Flickr

Flickr is a photo sharing website. We post our daily Earth Is Blue photos here so you can easily access high-resolution images. Please note that you are subject to Flickr's privacy policy when visiting the ONMS Flickr page.

GovDelivery

This site uses the GovDelivery Communications Cloud service to deliver email bulletin messages to self- subscribed users. GovDelivery is a web-based email subscription management system that allows a member of the public (user) to subscribe to news and information on ONMS websites. A user's subscription profile consists of their email address and the topics they wish to receive email updates for. The user may customize and manage their subscription profile in order to receive exactly the types of information they desire, and they may cancel their subscriptions at any time. We only use the email addresses provided by subscribers to send email messages related to the topics selected by the user in the GovDelivery system. We do not use the GovDelivery service to send email messages unrelated to the topics selected by the subscriber or to seek personally identifiable information (PII) about subscribers.
Neither ONMS nor GovDelivery will share a user's subscription profile, including email address.

Google™ Earth/Google™ Maps

Google Maps and Google Earth map information and photographic imagery are used under license by Google. National Ocean Service data presented using Google Maps/Google Earth are in the public domain and made available in open standard KML/KMZ format. The map information and photographic imagery contain trade names, trademarks, service marks, logos, domain names, and other distinctive brand features. This does not imply an endorsement of Google, Google Maps, or Google Earth products or services by the National Ocean Service. Under the terms of the license, you are permitted to copy or use the Google Maps/Google Earth images on your site so long as Google Maps/Google Earth trade names, trademarks, service marks, logos, domain names, and other distinctive brand features are not deleted or in any manner altered. Please note that you are subject to Google's privacy policy when using this service.

Google Analytics

This site uses Google Analytics, a third-party web measurement and customization technology as defined and organized by the Office of Management and Budget (OMB), "Guidance for Online Use of Web Measurement and Customization Technologies" (OMB M-10-22). Google Analytics places a small file on your computer, commonly called a "cookie," so that it can recognize your computer if you visit https://sanctuaries.noaa.gov in the future. This cookie does not collect personal identifying information. This is considered a Tier 2 service in the OMB guidance. Google Analytics does not collect personally identifiable information through their cookie and does not combine, match, or cross- reference https://sanctuaries.noaa.gov information with any other information. Please review the provider's privacy policy for additional information, http://www.google.com/analytics/learn/privacy.html.
Visitors who choose to disable this web measurement will still have full access to https://sanctuaries.noaa.gov. While the details vary from browser to browsers, most modern browsers can be set up to accept, reject, or request user intervention when a site asks to set a

cookie. Google Analytics uses a cookie that begins with: _utm

Retention of Information

We destroy the information we collect when the purpose for which it was provided has been fulfilled unless we are required to keep it longer by statute or official policy. Electronically submitted information is maintained and destroyed according to the principles of the Federal Records Act and the regulations

and records schedules approved by the National Archives and Records Administration, and in some cases information submitted to us may become an agency record and therefore might be subject to a Freedom of Information Act request.

Links to Other Sites

This site may have links to the Web sites of other federal agencies. There may be links to private organizations, with their permission. Once you go to another site, you are subject to the privacy policy of the new site. It is always a good idea to read the Privacy Policy of any Web site that you visit.

Cookies

"Cookies" are small bits of text that are either used for the duration of a session ("session cookies"), or saved on a user's hard drive in order to identify that user, or information about that user, the next time the user logs on to a Web site ("persistent cookies"). This Web site does not use persistent cookies or any other persistent tracking technology. One or more of our component sites may use session cookies to provide streamlined navigation. These session cookies are deleted from the component's server after your session ends and information from them is not collected or saved.

Interaction with Children

This Web site may offer educational content to children under 13. No personally identifiable information is collected from them unless voluntarily submitted as a request for information or services. The information collected is used to respond to user inquiries or to provide services requested by our users.

Rights under the Privacy Act

The Privacy Act of 1974 provides safeguards against invasion of personal privacy through the misuse of records by Federal Agencies.

The Privacy Act was passed in 1974 to establish controls over what personal information is collected, maintained, used and disseminated by agencies in the executive branch of the Federal government.

The Privacy Act guarantees three primary rights:

- The right to see records about oneself, subject to Privacy Act exemptions;
- The right to request the amendment of records that are not accurate, relevant, timely or complete; and
- The right of individuals to be protected against unwarranted invasion of their privacy resulting from the collection, maintenance, use, and disclosure of personal information.

If you are a citizen of the United States or an alien lawfully admitted for permanent residence, you may make a request for personal information on yourself under the Privacy Act. Go to the Request page for more information.

Requests made under the Privacy Act will be processed under both the Privacy Act and the Freedom of Information Act (FOIA) to ensure the greatest access to your personal records.

NOAA's National Ocean Service
Office of the CIO

Web Application Privacy Policy

The term "NOS OCIO Web Applications" in this policy refers to all web applications hosted and managed by the NOAA National Ocean Service (NOS) Office of the Chief Information Officer (OCIO). The following discloses the information gathering and dissemination practices for NOS OCIO Web Applications.

Most NOS OCIO Web Applications adhere to the NOAA web privacy policy. This document is in place to define policy for those applications and sites which, by virtue of their mission, depart in any way from the NOAA policy.

The NOS OCIO Web Applications primarily collect, store and display data for these basic purposes:

- Administrative functions (replacing a manual process);
- Tracking of some action, information, request, task, or process related to the NOS/NOAA mission;
- Providing a channel of information regarding NOS and NOAA to the general public;
- Response to a direct request initiated by a private individual;
- Point of contact information for participants in and sponsors of programs or events offered by NOS.

The NOS OCIO is committed to protecting the privacy of site visitors and application users as well as any personal information that users may provide.

Links to NOAA/NOS Websites

NOS OCIO Web Applications contain links to other NOAA/NOS websites. The privacy practices of other websites may vary with the purpose of the page. Consult the privacy policy on each site.

Links to External Websites

NOS OCIO Web Applications contain links to other external sites. NOS OCIO office is not responsible for the privacy practices or the content of such websites.

Cookies

A cookie is a text file that lives on the client user's computer. Cookies are either stored in memory (session cookies) or placed on users' hard disk (persistent cookies). A persistent cookie can keep information in the user's browser to a long lifespan until deleted.

Some sites may use cookies to store the unique internal user ID of an authenticated user for the purposes described in the section on **Authentication**.

NOS OCIO Web Applications only use session cookies. Persistent cookies are prohibited.

When an authenticated user logs off, cookies are emptied. Sensitive information, including user credentials, is not stored in cookies.

Users may determine how their browser handles cookies, and may disable cookies being stored. However, by disabling cookies certain web applications' features and functionality may no longer work properly, or function at all.

Session Management

Session information is stored on the server. It is typically stored in web server memory and exists for 20 minutes by default. Sessions work like a token, allowing access and passing information while the user has the browser open. When users close their browsers they also lose their sessions.

A unique session ID is generated for users when they log on to a NOS OCIO Web Application. The session ID is not associated with the user's computer or with the user individually. It is also not related to the unique user ID that may be generated when a user authenticates.

The session ID may be used to track a user's actions in the application. This is used for security and error resolution purposes only.

For applications requiring user credentials, user information stored in session may be used as explained in the section on **Authentication**.

When an authenticated user logs off, all information stored by a NOS OCIO Web Application in session memory is deleted. The session itself is deleted when a user's browser is closed.

Authentication

Some NOS OCIO Web Applications require user authentication. Authentication may be based on the existence of an entry in the NOAA LDAP directory or on the presence of application-specific credentials stored in a NOS OCIO database. Credentials stored in a database are not related to credentials stored elsewhere and are not used for purposes other than authentication.

The purpose of authentication is to control access to protected data and restrict actions that may be performed. Once a user has been authenticated, a unique internal user ID is stored, usually in session but possibly in cookies (see the sections on **Cookies** and **Session**). This ID is stored only as long as the user session is valid. This unique internal user ID is based on internal database record keys and is not related in any way to any other identification owned by or assigned to the user.

The stored internal user ID may be used to track a user's actions while logged in to the application:

- Stored internal user IDs are used to ensure that users only visit data they are allowed to see.
- The internal user ID of an authenticated user may be logged when an error occurs during that user's session.
- The internal user ID of an authenticated user may be logged in a log tracking session activities.
- Other user information, such as name, may also be stored in session to be used as above or to provide a customized user interface.

A user's password is not stored in session or in cookies. Once the user has logged off, all user information stored outside of the authentication source is deleted.

Access & Audit Logs

A user's actions may be logged as follows:

- Some NOS OCIO Web Applications record a users' login name and last access time for auditing purpose.
- If a user is authenticated, the user's name or unique internal user ID along with the user's actions during a session may be logged to an application audit file.
- The server's system and tracking log files may record page hits and errors along with the IP address of the user who performed an action.

Access to log files is restricted to system administrators and application administrators. They may be shared with appropriate IT security officials when necessary.

Private Data Collection

Any information gathered by NOS OCIO Web Applications is limited to that data needed to provide users with accurate and appropriate service. User information is only used for particular project purposes and is not shared outside the Federal government. Accordingly, the privacy and personal information visitors provide is stored in a secure location accessible only by designated staff, and is used only for the purposes for which visitors provide the information.

Personally identifiable information (PII) collected or stored by applications in the NOS OCIO Web Applications is limited to: name, address, phone, e-mail address, organization name, organization address, and position. In some limited-access applications, the PII is collected using some other method (mail, e-mail, fax, business card, etc.) and is entered by authorized NOS staff.

The information is collected from NOAA/NOS staff, NOAA/NOS partners, and members of the general public.

NOS OCIO Web Applications have reasonable security measures in place to protect the loss, misuse, and alteration of the information under our control. These measures include administrative, technical, physical and procedural steps to protect users' data from misuse, unauthorized access or disclosure, loss, alteration, or destruction.

The current Privacy Impact Assessment for NOS OCIO Web Applications, referenced as the *National Ocean Service Web Application Subsystem*, is reachable from the page linked here: http://www.cio.noaa.gov/services_programs/privacy.html

Rights under the Privacy Act

Your rights under the Privacy Act can be found at the following address: https://www.justice.gov/opcl/privacy-act-1974

Updates to This Privacy Policy

In case an update to this privacy policy becomes necessary, we will announce both the changed version and its effective date on NOS OCIO Web Applications.

Contact Information

If you have any questions about this privacy policy, please contact nos.webdb@noaa.gov.