Version Number: 01-2018

U.S. Department of Commerce
National Ocean Service

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

Reviewed by: Mark Graff, Bureau Chief Privacy Officer

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

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

LISA MARTIN

Digitally signed by LISA MARTIN
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=LISA MARTIN, 0.9.2342.19200300.100.1.1=13001000105292
Date: 2018.03.15 15:42:59 -04'00'

03/15/18

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

U.S. Department of Commerce Privacy Impact Assessment
Office of National Marine Sanctuaries (ONMS)
NOAA6602

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: System Description

Provide a description of the system that addresses 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 fourteen ONMS 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**: The sites that constitute the ONMS are the Silver Spring HQ, Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Each site maintains a file server for storage of scientific data and research. All sensitive data is stored on an ACL controlled file share.

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

NOAA6602 does not interconnect with other systems.

d) The way the system operates to achieve the purpose 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 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 ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted.

UAS
ONMS recently acquired a Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. **However, it is currently not in operation.**

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 OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

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 temporarily maintains PII data during the hiring process or to assist employees with travel preparation. All digital PII received is stored temporarily in Access Controlled files shares used by the HR department. All paper copies of PII is stored within access controlled locked file cabinets. All HR data is stored temporarily and destroyed when no longer needed.

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.

OSPREY
Permit data is only used internally by ONMS and entered or retrieved from the permit application using encryption for data in transit.

UAS
Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation. **However, it is currently not in operation.**

HR
HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal

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.

f) How information is transmitted to and from the system

OSPREY
All communication, by the permit coordinators, to and from the OSPREY application is using encryption for data in transit.

UAS
The UAS is hand carried from UAS to Scientific workstation.

HR
HR data is stored on the NOAA HR system. 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 ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network.

g) Any information sharing conducted by the system

OSPREY
NOAA6602 only shares scientific data. Permit data is used internally. Any permit data shared does not include PII.

UAS data is processed then shared internally only. **However, it is currently not in operation.**

Acquisition data is not shared.

Employee information is shared internally and also with DOC and federal agencies in case of breach.

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

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 Unmanned 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.

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

ONMS is a FIPS 199 Moderate Security risk.

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.
_X__ 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): ONMS purchased a UAS that will only be in the system temporarily.					

____ 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.

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*		e. File/Case ID		i. Credit Card	

b. Taxpayer ID		f. Driver's License	X	j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID		h. Alien Registration	X	l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

The above information is only collected to assist employees with making travel arrangements. Paper copies are temporarily stored in a locked file cabinet and destroyed when no longer needed.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	X
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	

s. Other general personal data (specify):

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 **UAS** does not collect any of the above data types.

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			

i. Other work-related data (specify): Performance appraisals

The OSPREY application collects the above checked data types.
The UAS does not collect any of the above data types. It is also not in operation.
HR related data is stored in the NOAA HR system. but is temporarily stored locally in an access controlled file share prior to being moved to the NOAA HR system..

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

j. Other distinguishing features/biometrics (specify):

ONMS does not collect any of the above data types.

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	

g. Other system administration/audit data (specify)

The NOAA6602 OSPREY application uses the NOAA LDAP 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 and date and time of access to the OSPREY system.

Other Information (specify)
UAS Currently the UAS is not authorized to operate. No data has been collected or stored on or with the device. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1

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			
Other (specify):					

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

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): Procurement data is provided in proposals and other procurement documents					

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

HR data is validated at the time of receipt 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 information at the time of collection. This includes comparison of Driver's License and Passport.

HR data for travel is only used to assist the employee in making travel arrangements and is not stored. Applicant data is only maintained during the hiring process.

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 No. 0648-0141, National Marine Sanctuary Permits
	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):ONMS recently purchased a UAS. The UAS has the potential to temporarily contain PII. **However, it is currently not in operation,**			

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

Section 3: System Supported Activities

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

Activities			
Audio recordings		Building entry readers	
Video surveillance	X	Electronic purchase transactions	
Other (specify): **UAS Only** Although the ONMS UAS 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 UAS is also only operated in remote locations to avoid the potential to capture PII. **However, it is currently not in operation.**			

	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 stores PII on an ad-hoc basis as part of the application and hiring of employees. 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. 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 cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics). Information shared is scientific data only.			

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. *Collected from the public.*

ONMS stores PII on an ad-hoc basis as part of the application and hiring of employees. 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.

The travel information collected is kept in both hard and soft forms. The hard copies are kept in a locked file cabinet and the soft copies are kept on the shared drive in a folder accessible only to travel admins. The travel documents contain only the traveler's name, home address, and a truncated vendor number associated to the traveler's name. There are no social security numbers or dates of birth. *Collected from the public, federal employees and contractors.*

UAS

ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does not intend to keep the UAS within its boundary and is currently in discussion with another NOAA line office to take possession of the device in return for performing the required mapping. ONMS use of the UAS is covered by the DOC SORN and the NOAA Policy. The UAS would be exclusively operated in remote areas and is not authorized to operate above people or structures. Any privacy data that is inadvertently collected will be immediately deleted. **However, it is currently not in use.**

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 fall into this category. This category also includes requests for authorizations of other 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.

(d) 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.

(e) 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).

(f) 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.

(g) 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.

(h) 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.

Collected from the public.

5.2 Describe any potential threats to privacy 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.

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.

UAS
The UAS is currently grounded but **if operational** has the potential to collect PII if it inadvertently flies over an individual.

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

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII. The UAS comes with its own remote control. The communication is encrypted digital transmission. All data recorded by the UAS is stored internally on the UAS encrypted SD Card and is not transmitted to the controlling device.

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

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify): **OSPREY** The PII is only accessed by ONMS employees.			

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/management/permits/welcome.html	
X	Yes, notice is provided by other means.	Specify how:

		OSPREY: see above link to site with PAS. **UAS** The ONMS UAS is operated remotely and does not have the ability to provide notice or consent. **However, currently not in operation.** **COOP** 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: all federal forms provide notice, including Privacy Act Statements. Acquisition: Notice is given through solicitations.
	No, notice is not provided.	Specify why not:

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

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: **OSPREY** If individuals do not want to provide the PII, they will not submit a permit application. **UAS** The UAS does not have the ability to provide notice and consent. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **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 their business cards.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: **OSPREY** There is only one use, the generation of the permit. **UAS** The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Applicants for positions who have applied through the USAJobs 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).
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: **OSPREY** Individuals may provide their permit coordinators with updated information. **UAS** The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **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.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	

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 WFMO. 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 save it on their own ACL-restricted folders on the shared drive. Policy also requires users to remove all PII from their file share when no longer needed.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 03/16/2017 ☐ 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 supporting 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 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 ONMS Permit application (OSPREY) is hosted on a data base. 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.

UAS
The UAS system stores data on an encrypted SD card. All data is over written or the SD card is destroyed once the data is removed from the SD card. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.**

HR
Digital HR data may be temporarily stored on ACL protected network file share accessible only by HR personnel. HR related data is permanently stored in the NOAA HR system. Paper copies of HR related material is stored in access controlled file cabinets.

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.

All PII and BII are encrypted at rest.

Section 9: Privacy Act

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

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/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-1, General Personnel Records; OPM/GOVT-5, Recruiting, Examining, and Placement Records
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

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

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Schedules Chapter 1609 Marine Sanctuaries **UAS** All data is over written or the SD card is destroyed once the data is removed from the SD card. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.**
	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

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 as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

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

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

X	Identifiability	Provide explanation: Individuals may be identified by the provision of their contact information
X	Quantity of PII	Provide explanation: There is a small quantity of PII.
X	Data Field Sensitivity	Provide explanation: Acquisition and performance ratings.
X	Context of Use	Provide explanation: **OSPREY** permit data is used to generate permits for activity conducted within one of the ONMS sanctuary. **UAS** Data is used to produce coastal and wildlife maps. **However, currently not in operation.** **Acquisition** People or organizations provided their information voluntarily.
X	Obligation to Protect Confidentiality	Provide explanation: **Acquisition** Per the FAR, Procurement Integrity Act, and Economic Espionage Act
X	Access to and Location of PII	Provide explanation: **OSPREY** Data is stored in a 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. **UAS** The UAS data is only transferred by a UAS pilot and can only be transferred to a ONMS scientific workstation. **However, currently not in operation.**
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data,

include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

OSPREY was recently migrated to the new application. The old OSPREY application has been deactivated. ONMS re-evaluated the system impact level (FIPS-199) and upgraded the FISMA system impact level to Moderate. Many of the privacy controls, although in place, were not properly documented at the time of the initial assessment. 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 development meeting with the database administrator, application programmer and IT manager. The ONMS ISSO is also included in OSPREY permit coordinators meetings and training. **UAS** The UAS has a low risk of threat to privacy since it is operated only in remote locations and is not authorized above buildings or people. **However, currently not in operation.**

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.