Version Number: 01-2019

# U.S. Department of Commerce
# NOAA


## Privacy Threshold Analysis
## for the
## Office of National Marine Sanctuaries
## NOAA6602

# U.S. Department of Commerce Privacy Threshold Analysis

## Office of National Marine Sanctuaries

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

**Introduction:** This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

**Description of the information system and its purpose:** *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

*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 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*

The sites that constitute the ONMS are the Silver Spring HQ, Channel Islands, Cordell Bank, American Samoa, Florida Keys, Flower Garden Banks, Gray's Reef, Greater Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, Mallows Bay, and Thunder Bay National Marine Sanctuaries and the Papahanaumokuakea 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. ONMS maintains Azure based websites and Azure based applications that may contain non-sensitive PII such as Sanctuary Permit applications and images of people at Sanctuary events. ONMS websites are the only publically accessible location for ONMS information via the internet. Information on the ONMS sanctuary websites may be viewed, over the HTTPS protocol, by the general public.

*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 NOAA0200.
NOAA6602 Uses the Messaging Operations center NOAA0300.

*d) The purpose that the system is designed to serve*

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 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.

*e) The way the system operates to achieve the purpose*

**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 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.

**UAS**

ONMS recently acquired two PUMA AE Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (e.g. living marine resources and coastal mapping) and meteorological data. UAS requirements and procedures are documented in the ONMS Privacy Policy and Procedure V4.3 and the ONMS Unmanned Aircraft System Policy & Procedures V4.0. The policies and procedure are updated annually or when changes to the system 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 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, 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 V4.3. The Privacy Policy and Procedure is updated annually or when changes to the system occur.

**ONMS Public Websites**

ONMS websites are the only publically accessible location for ONMS information. Information on the ONMS sanctuary websites may be viewed, over the HTTPS protocol, by the general public.

*f) A general description of the type of information collected, maintained, use, or disseminated by the system*

Geographic Information Systems (GIS) are used to process bathymetric and other cartographic data to generate maps that provide a great deal of information about marine sanctuaries.

**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.

**UAS**

ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does 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 preforming 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.

**OSPREY**
The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries.

**HR Data**
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation.

**ONMS Public Websites**
ONMS websites are the only publically accessible location for ONMS information. Information on the ONMS sanctuary websites may be viewed, over the HTTPS protocol, by the general public. All Data on the ONMS Websites is uploaded by approved ONMS employees. The general public cannot upload information to any of the ONMS websites.

**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 kept within the system. Staff use this application to generate and send out newsletters and other materials. Users may opt out of the Gov Delivery system at any time by clicking the link in each email.

*g) Identify individuals who have access to information on the system*

NOAA6602 maintains scientific data that is freely available to the general public.
All access to ONMS information is limited to only the information needed by the specific employee. Access is limited to only information needed by the employee to complete their job. User access is reviewed by the employee's supervisor, System ISSO and the system IT Manager.

**OSPREY**
NOAA6602 also maintains permit data. OSPREY data is only accessible by ONMS permit coordinators. All permit coordinators must be approved by the ONMS IT Manager, ONMS ISSO and the Osprey system manager.

**UAS**
Currently the UAS is not operational and had not data that to access. Currently ONMS is trying to transfer the UAS to another NOAA system that has the capability to operate the UAS.

**Acquisitions**
Contract information is only accessible by the ONMS contracting officer and the IT manager. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

**HR Data**
ONMS HR data is only accessible by the ONMS HR representative and the ONMS deputy Director. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

*h) 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 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.

**UAS**
Data on the UAS is captured by the UAS on encrypted internal media. The data is retrieved by the ONMS UAS director when the data is directly connected to laptop dedicated to the UAS. The laptop dedicated to the UAS is not connected to any computer network. Data is first reviewed by the director on the UAS to remove any inadvertent PII prior to the non-PII data being transferred to the laptop dedicated to the UAS. The UAS director then hand carries the Non PII data to an ONMS computer. UAS requirements and procedures are documented in the ONMS Privacy Policy & Procedure V4.3 and the ONMS Unmanned Aircraft System Policy & Procedures V4.0. The UAS is also only operated in remote locations to avoid the potential to capture PII. The UAS is flown with Line Of Sight and 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.

**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.

**ONMS Public Websites**
ONMS websites are the only publically accessible location for ONMS information. Information on the ONMS sanctuary websites may be viewed, over the HTTPS protocol, by the general public.

**GovDelivery**

Is managed by NOAA6001. GovDelivery is a tool used by ONMS to automatically send emails to constituents that have provided their email address. Constituents my remove their email address at any time by following the unsubscribe link in received emails from GovDelivery.

*i) 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.

**UAS**
The UAS is hand carried from UAS to dedicated laptop.

**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 ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network

**ONMS Websites**
ONMS websites are the only publically 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 kept within the system. Staff use this application to generate and send out newsletters and other materials.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*
_X_ This is an existing information system with changes that create new privacy risks.
*Complete chart below, continue to answer questions, and complete certification.*

| **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): A video security system was added at our Flower Garden Banks Sanctuary. | | | | | |

____ 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. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015). *Continue to answer questions and complete certification.*

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

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

_X_ Yes. *(Check all that apply.)*

| **Activities** | | | |
|---|---|---|---|
| Audio recordings | | Building entry readers | |
| Video surveillance | X | Electronic purchase transactions | |
| Other (specify): | | | |

**UAS**

The ONMS UAS has the potential to inadvertently capture PII, however, the UAS is also only operated in remote locations to avoid the potential to capture PII. The UAS is flown with Line Of Sight and Ship based Radar is used to verify that there are no other vessels in the vicinity.

**Security System.** ONMS Flower Garden Banks office recently installed a new 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. The system adds minimal new privacy risk.

____ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is]

privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

X Yes, the IT system collects, maintains, or disseminates BII.

ONMS collects and stores limited BII from businesses or other entities that are providing proprietary information in support of a grant application or federal acquisition actions.

Occasionally financial information is included with the acquisition package.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

X Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

X DOC employees
____ National Institute of Standards and Technology Associates
X Contractors working on behalf of DOC
____ Other Federal Government personnel
X Members of the public

____ No, this IT system does not collect any PII.

***If the answer is "yes" to question 4a, please respond to the following questions.***

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

| Provide an explanation for the business need requiring the collection of SSNs, including truncated form. |
|---|
| |

| Provide the legal authority which permits the collection of SSNs, including truncated form. |
|---|
| |

_X_ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

_X_ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

***If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.***

# CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the ONMS and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the ONMS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

James Cooperman (ISSO):

Signature of ISSO or SO: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2020.08.03 09:22:53 -04'00' Date: _____

John D. Parker (ITSO): _____

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2020.08.03 13:38:17 -04'00' Date: _____

Adrienne Thomas (PAO): THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2020.08.04 09:30:40 -04'00'

Signature of PAO: _____ Date: _____

John Armor (AO): ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2020.08.03 13:26:36 -04'00'

Signature of AO: _____ Date: _____

Mark Graff (BCPO): GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2020.08.04 17:29:13 -04'00'

Signature of BCPO: _____ Date: _____