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

Privacy Threshold Analysis
for the
Office of National Marine Sanctuaries
NOAA6602

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/ NOS/ Office of National Marine Sanctuaries

Unique Project Identifier: NOAA6602

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 publicly 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 NOAA0550. NOAA6602 Uses the Messaging Operations center NOAA0700. Microsoft - Azure Commercial Cloud Package ID F1209051525.

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 provided 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 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 publicly accessible location for ONMS information. 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.

f) A general description of the type of information collected, maintained, used, 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.

UAV
ONMS owns multiple UAV for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS use of the UAV is covered by the DOC SORN, ONMS UAV policy and the NOAA Policy. The UAV 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 publicly 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.

SAC
The SAC application will collect Name, Address, phone number, and email address. The applicant is also requested to provide a reason why they wish to serve on the committee and any qualifications.

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.

UAV
Only the ONMS UAV operator has access to UAV data prior to review. Once all mission data is reviewed and verified that all PII has been removed then the UAV data will be posted on an ONMS scientific workstation for processing.

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.

SAC
The only individuals with access to the SAC application will be the site Superintendent, SAC Coordinators, the Headquarters National SAC Coordinator, and ONMS Deputy Directory. The NOS general counsel will also review the application and verify the information.

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.

UAV
Data on the UAV is captured by the UAV on encrypted internal media. The data is retrieved by the ONMS UAV director when the data is directly connected to a laptop dedicated to the UAV. The laptop dedicated to the UAV is not connected to any computer network. Data is first reviewed by the operator of the UAV to remove any inadvertent PII prior to the non-PII data being transferred to the laptop dedicated to the UAV. The UAV director then hands the Non PII data to an ONMS computer. UAV requirements and procedures are documented in the ONMS Privacy Policy & Procedure V4.3 and the ONMS Unmanned Aircraft System Policy & Procedures V4.0. 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 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 HTPPS 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 Counsel, 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.

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.

UAV

The UAV is hand carried from UAV 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 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 kept within the 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.

Questionnaire:

1. Status of the Information System

1a. 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): ONMS is developing a new application for the Sanctuary Advisory Council applications. The SAC application will collect Name Address Phone number and email address. We are still early in the development but the SAC application has the potential to be in production this year.					

_____ 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 or 01-2017). *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 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

_____ Yes. This is a new information system.

_____ Yes. This is an existing information system for which an amended contract is needed.

_____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

__X__ No. This is not a new information system.

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): **UAV**
The ONMS UAV has the potential to inadvertently capture PII, however, 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 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
    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 SAOP 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.

Information System Security Officer or System Owner	**Information Technology Security Officer**
Name: James Cooperman Office: Office of National Marine Sanctuaries Phone: 240 533-0680 Email: James.Cooperman@noaa.gov Signature: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2021.05.11 10:03:13 -04'00' Date signed: _____	Name: John Parker Office: NOS Information Management Office Phone: 240-533-0832 Email: john.d.parker@noaa.gov Signature: PARKER.JOHN.DARYL.1365835914 Digitally signed by PARKER.JOHN.DARYL.1365835914 Date: 2021.05.14 10:13:51 -04'00' Date signed: _____
Privacy Act Officer	**Authorizing Official**
Name: Adrienne Thomas Office: NOAA OCIO Phone: 240-577-2372 Email: Adrienne.Thomas@noaa.gov Signature: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2021.05.14 09:19:17 -05'00' Date signed: 600	Name: John Armor Office: Office of National Marine Sanctuaries Phone: 240-533-0681 Email: john.armor@noaa.gov Signature: ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2021.05.11 12:56:33 -04'00' Date signed: _____
Bureau Chief Privacy Officer	
Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5751 Email: mark.graff@noaa.gov Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2021.05.24 15:35:53 -04'00' Date signed: 514447892	