U.S. Department of Commerce
National Ocean Service

Privacy Threshold Analysis
for the
Office of National Marine Sanctuaries (ONMS)
NOAA6602

U.S. Department of Commerce Privacy Threshold Analysis

Office of National Marine Sanctuaries (ONMS) NOAA6602

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 of the information system in a way that a non-technical person can understand.
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 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 Headquarters, 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 purpose that the system is designed to serve**

The purpose of the Office of National Marine Sanctuaries (ONMS) is to serve as the trustee for the nation's system of marine protected areas, i.e., to conserve, protect, and enhance their biodiversity, ecological integrity, and cultural legacy.

Unmanned Aviation System (UAS)
The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Currently the UAS is not operational.

The ONMS Permit System (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.

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.
This information is used to award contracts that are in support of the ONMS mission.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. Travel data is used to assist ONMS employees in the performance of their duties. Hiring data is used by ONMS to hire qualified personnel to meet the ONMS job requirements.

e) 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.

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.

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.

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

NOAA6602 maintains scientific data that is freely available to the general public.

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 data is only used internally by ONMS and entered or retrieved from the permit application over the HTTPS protocol.

UAS

Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation.

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.

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 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

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): ONMS purchased a UAS that will only be in the system temporarily. The risk would be only if and when the UAS is in operation, which it is currently not.					

____ 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 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. *Please describe the activities which may raise privacy concerns.*

UAS
The ONMS UAS has the potential to inadvertently capture PII, when in operation.

____ 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 about: *(Check all that apply.)*

__X__ Companies
__X__ Other business entities.
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

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__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
__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 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.

4c. 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, and/or 4c 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 NOAA6602 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 NOAA6602 ONMS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

James Cooperman ISSO____

COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2018.03.08 09:39:16 -05'00'

Signature of ISSO or SO: ____ Date: ___________

John D Parker (ITSO): _______________________________

PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.08 15:01:04 -05'00'

Signature of ITSO: ____ Date: ___________

John Armor (AO): ____

ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2018.03.08 14:23:20 -05'00'

Signature of AO: ____ Date: ___________

Mark Graph (BCPO): GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892
Date: 2018.03.09 09:40:32 -05'00'

Signature of BCPO: ____ Date: ___________

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.09 07:43:57 -05'00'