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

Privacy Threshold Analysis for the
NOAA6501
Office of Coast Survey (OCS) Nautical Charting System

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NOS/OCS Nautical Charting System

Unique Project Identifier: NOAA6501

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: *Provide a brief description of the information system.*
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).

NOAA6501 is an enterprise information system (General Support System) for NOAA, National Ocean Services, Office of Coast Survey. NOAA6501 is utilized to acquire, process, and store mission data and applications related to hydrographic processing, hydrographic and cartographic research and development, marine modeling, customer outreach, and nautical products/services along with providing all IT resources necessary to support a Federal organization.

Address the following elements:

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

NOAA6501 is an enterprise information system (General Support System) for NOAA, National Ocean Services, Office of Coast Survey. NOAA6501 is utilized to acquires, processes, and stores mission data and applications related to hydrographic processing, hydrographic and cartographic research and development, marine modeling, customer outreach, and nautical products/services along with providing all IT resources necessary to support a Federal organization.

b) *System location-*

- OCS headquarters, Silver Spring, MD
- NOS-OCS-AWS cloud, Herndon, VA
- NOS-Azure-OCS Subscription
- HSD Atlantic Hydrographic Branch, Norfolk VA
- HSD Pacific Hydrographic Branch, Seattle WA
- EDC-Ashburn, Ashburn VA

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

NOAA6501 interconnects to NOAA6001 (NOS Enterprise Information System) for connections to NOS hosted applications, and NOS OCS AZURE subscription; and NOAA campus backbone used to connect to the Internet, NOAA0550 NOAA NWAVE, and NOAA0900 Consolidated cloud application. NOAA6501 utilizes NOAA VPN for remote connectivity and NOAA NWAVE for connection to AWS East/West FedRamp Cloud and NOAA Enterprise Data Center, and NOAA0100 NOAA Cyber Security Center. NOAA6501 connects to *NOAA0700 High Availability Enterprise Services which supplies centralized Enterprise service for the ICAM component for the NOAA community.

*Note: NOAA0700 is not a new connection, this section has simply been updated to match CSAM.

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

NOAA6501 encompasses all IT resources necessary to support the Office of Coast Survey's mission and organizational administrative functionality. The information system contains servers, applications, storage, network devices, and externally facing websites for the distribution of nautical charts and other products. NOAA6501 utilizes externally facing websites as a distribution point for nautical scientific data, charts, and other nautical products and applications. OCS has several social media sites (Facebook and Twitter) which are used to convey information to different audiences like Federal, State, and university partners as well as the public.

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

NOAA6501 encompasses all IT resources necessary to support the Office of Coast Survey's mission and organizational administrative functionality. The information system contains servers, applications, storage, network devices, and externally facing websites for the distribution of nautical charts and other products. NOAA6501 operates network infrastructure, virtual / physical servers, workstations, storage and other general IT resources to support the business processes used to produce nautical charts and products along with typical government administrative process. NOAA6501 utilizes externally facing websites as a distribution point for nautical scientific data, charts, and other nautical products and applications. OCS utilizes NOAA Google services for email, NOAA VPN service for remote access, and NOAA TIC for secure internet traffic. OCS has several social media sites (Facebook and Twitter) which are used to convey information to different audiences like Federal, State, and university partners as well as the public.

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

Mission Distribution / contacts

OCS's contact information (members of the public, other federal, state and private organizations) is collected to provide a means for the Office of Coast Survey to communicate and respond to needs and requests. OCS mission data is shared with multiple external federal and state organizations as well as multiple private entities to receive navigational relevant and significant data which is used to update the charting databases. In addition, OCS system communicates with the diverse community of national and international chart product and services users. Collected from the public, federal-state-local government or foreign nationals.

On Public websites as well as several social media accounts (Facebook and Twitter), OCS does utilize staff pictures (with written permission) as part of OCS programs (such as federal government organizational charts and leadership), profile narratives, presentations of OCS mission nautical activities, public outreach, communication, and employee/partner recognition which may include photos, biographies, and award recognition.

Administrative, HR
Office of Coast Survey, collects PII as part of the application and hiring of employees, (electronic copies of resumes and hiring ranking are stored temporary during the hiring phase), including standard HR information (such as Travel authorization and vouchers, passports and international travel forms, information for security badging process, and performance appraisal ranking). OCS' employee data is collected, stored and maintained for internal OCS COOP, Human Resource, and workforce planning purposes (federal employee/contractor). The storage is in the form of PDF forms or MS Word documents in a secure folder on OCS network. Collected from federal employees, contractors, or public applying for employment with OCS.

Acquisition
Pre and Post Acquisition BII is collected and utilized during the pre-acquisition through deliverable BIDS packages and contain specific company information. BII information is maintained on a restricted access network folder during the execution of an awarded contract and other information from companies not receiving awards is deleted, when appropriate.

UAS
OCS is researching and piloting with NOAA OMAO the use of UAS (drones) to gather aerial photos to determine if this data (coastal mapping, nautical channels) could assist with the accuracy of OCS nautical charts. UAS would be maintained in separate folder (secured through technical permission) until validated for incorporation into OCS mission nautical charts. The UAS would not be disseminated as collected data but relevant data incorporated into OCS products. Any "PII" collected is incidental, unintentional, and not retained. It is anticipated that the Unmanned Aerial System (UAS) collected imagery will be at a resolution to meet organizational needs but it would not have the ability (resolution or clarity) to uniquely identify any individuals.

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

NOAA6501 User Base, as listed in the NOAA6501-Risk Assessment Report:

User Type	Type	Data access	Location	Connection
Authenticated OCS Users	Federal & NOAA corp., contractors, associates	All mission data as authorized based on role and responsibilities within assigned division.	All locations	LAN, NOAA VPN
Supervisor	Federal, or	All mission data and PII data	All locations	LAN, NOAA VPN

	contractors	stored in central location on file servers.		
IT Services staff	Federal & contractors (On-site)	Access to all IT Data based on assigned Roles and Responsibilities.	All locations	LAN, NOAA VPN
Database administrator	Federal & contractors (On-site)	Access to support databases of Mission data.	All locations	LAN, NOAA VPN
Programmers	Federal & contractors (On-site)	Access to specific development, staging, and production data	All locations	LAN, NOAA VPN
Offsite Contractor	Contractors	Contractors employed by OCS to carry out the mission work from non-NOAA facilities	Off-site Location	N/A
Web Visitors	Public	Access to mission data published on public websites	Public	Public space, websites

As listed in the NOAA6501-PIA.
The only information shared externally is mission related which is non PII or BII data.

External Internet users are able to retrieve posted OCS nautical charts and navigations products through open websites. Final digital data products and services (i.e., Booklet Charts; ENCs; Online Chart Viewer) are delivered to our partners and customers through the downloading of the products and services from OCS's public Web site, http://www.nauticalcharts.noaa.gov. These entities consist, for example, other NOAA offices, United States Coast Guard, Federal Aviation Administration, the maritime community, and the general public. Documented ISA will be utilized to document and approve any the direct transfer of mission data between government organizations.

Internal authenticated users are able to utilize (based on permissions) HR data stored in PDF documents that are shared based on roles and responsibilities. Acquisition data is not shared.

NOAA6501 utilizes the infrastructure operated by NOAA NWAVE and NOS Line Office backbone and network devices to securely transfer data between OCS Office locations or utilizes secure external hard drives. OCS utilizes the agency Secure Transfer Application for the transfer of any sensitive information between remote OCS individuals, off the internal network and not connected to the NOAA VPN.

h) How information in the system is retrieved by the user

All internal data and resources are retrieved using Government Furnished Equipment (GFE) through approved applications to open, review, verify, and securely delete information. Internal resources are secured through defense in depth with layered security such as physical access, firewalls, active director, access controls and permission, etc.).

Internal CAC authenticated users are able to utilize (based on permissions) data stored in PDF, Files, and databases through networked clients devices, NOAA VPN service for remote access and NOAA TIC for secure Internet traffic. OCS utilizes NOAA Google services for email and collaboration services.

External Internet users (public) are able to retrieve posted OCS nautical charts and navigations products through open websites. Final digital data products and services (i.e., Booklet Charts; ENCs; Online Chart Viewer) are delivered to our partners and customers through the downloading of the products and services from OCS's public Web site, http://www.nauticalcharts.noaa.gov. These entities consist, for example, other NOAA offices, United States Coast Guard, Federal Aviation Administration, the maritime community, and the general public.

i) How information is transmitted to and from the system

MISSION:
NOAA6501 utilizes the infrastructure operated by NOAA NWAVE and NOS Line Office backbone and network devices to securely transfer data between OCS Office locations or utilize secure external hard drives. OCS utilizes DOC Secure Transfer Application/solution for the transfer of any sensitive information between individuals when outside NOAA6501. OCS employees also utilize secure and documented ISA for the transfer of data between government organizations. All information approved to be release to the public are posted on the OCS external websites for distribution.

HR: NOAA6501 gathers and stores PII related to hired employees and contractors of the Office of Coast Survey, which is collected, stored and maintained for Human Resource-related issues as well as workforce planning, operating budget, COOP/ DR Operations, and documentation. The documents containing PII are gathered 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.

ACQUISITION: OCS collects BII during the pre and post activities associated with the acquisition and management of contracts. PII and BII are not shared or distributed externally to OCS and only authorized individuals are given permission to the stored documents or PDFs.

UAS: As outlined in DEPT-29, the use of UAS for NOS Coast Survey purposes has the potential for inadvertent collection of PII, such as images of individuals along the coastlines that are within the area of study by the UAS vehicle. However, no retrieval of information using any unique identifier within UAS Coastal Survey datasets will be conducted, and any PII inadvertently collected will be deleted within 30 days. NOAA6501 does not contain any application capable of facial recognition within any captured images. OCS is working with NOAA OMAO to use UAS (drones) for gathering aerial photos in order to assist with the accuracy of the OCS nautical charts. It is anticipated that the Unmanned Aerial System (UAS) collected imagery will be at a resolution to meet organizational needs but it would not have the ability (resolution or clarity) to uniquely identify any individuals... If the drone goes down during flight, the retrieval of the unit would be at the discretion of the operator based on safety and technical factors. Inadvertently obtained PII captured during the flight could be retrieved by others if technically possible from the damaged drone. OCS is compliant with all policies and procedures posted on the UAS.noaa.gov site along with the NOAA Unmanned Aircraft

System Privacy Policy.

PUBLIC WEBSITES: 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."
- 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.

Based on user submitted information to OCS through websites, email and user name could be captured and stored in OCS databases and emails to maintain contact lists of customers or those submitted documents or data to OCS.

On Public websites as well as several social media accounts (Facebook and Twitter), OCS does utilize staff pictures (with written permission) as part of OCS programs (such as federal government organizational charts and leadership), profile narratives, presentations of OCS mission nautical activities, public outreach, communication, and employee/partner recognition which may include photos, biographies, and award recognition.

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.*

____ 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):					

____ 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.*

_X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment. *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 tothose 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.

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

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

_X 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.

*NOTE: OCS only collects and maintains (does not disseminate) BII for internal OCS purposes associated through the Pre-Acquisition process received in submitted technical /financial proposes for OCS contracts.

____ 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
_X_ 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 The criteria implied by one or more of the questions above **apply** to the NOAA6501 and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_____ The criteria implied by the questions above **do not apply** to the NOAA6501 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Rebecca Banghart Office: NOS, Office of Coast Survey Phone: 3029272332 Email: rebecca.banghart@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system Signature: BANGHART.REBECCA.GAIL.1589418430 Digitally signed by BANGHART.REBECCA.GAIL.1589418430 Date signed: Date: 2022.05.19 15:26:40 -04'00'	**Information Technology Security Officer** Name: John D. Parker Office: National Ocean Services Phone: 240-533-0832 Email: John.D.Parker@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: PARKER.JOHN.DARYL.1365835914 Digitally signed by PARKER.JOHN.DARYL.1365835914 Date signed: Date: 2022.05.20 10:51:07 -04'00'
Privacy Act Officer Name: Robin Burress Office: NOAA OCIO Phone: 828-271-4695 Email: Robin.Burress@noaa.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date signed: Date: 2022.05.23 09:59:48 -04'00'	**Authorizing Official** Name: Benjamin K. Evans Office: NOS, Office of Coast Survey Phone: 240-533-0917 Email: benjamin.k.evans@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system Signature: EVANS.BENJAMIN.K.1237217094 Date signed: 2022.05.17 20:29:46 -04'00'
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date signed: Date: 2022.06.06 11:57:17 -04'00'	