

U.S. Department of Commerce
NOAA



Privacy Threshold Analysis
for the
NOAA6501, Nautical Charting System
Office of Coast Survey, NOS, NOAA

U.S. Department of Commerce Privacy Threshold Analysis

NOAA6501, Nautical Charting System Office of Coast Survey, NOS, NOAA

Unique Project Identifier: NOAA6501

UPI Code: 006-48-01-15-01-3401-00

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*

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 is located in Silver Spring, MD (SSMC3), with field branch offices located in Norfolk VA and Seattle WA, NOS Enterprise Azure cloud, AWS cloud purchased through NOAA CIO, and remote individuals throughout the United States.

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

NOAA6501 is utilized as an IP address segregated information system but it is located within the NOAA campus under the NOS Line Office which provide the infrastructure backbone for connection to the NOAA TIC (Internet) and connection to other NOAA6501 office location. OCS utilizes NOAA VPN

for remote connectivity. OCS is establishing Interconnection Service Agreements for the exchange of nautical charting data between US Coast Guard and NOAA OMAO.

d) The purpose that the system is designed to serve

NOAA6501 is an enterprise information system (General Support System) for all actions requiring IT resources for 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.

e) The way the system operates to achieve the purpose

NOAA6501 is an enterprise information system (General Support System) for all actions requiring IT resources for 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 information system is compliant with NOAA's requirement for CAC authentication and utilizes NOS enterprise Active Directory to maintain authorized account and client computers. NOAA6501 follows the standard architecture for internal TCN2 and externally facing resources on TCN1. OCS utilizes NOAA Google services for email and NOAA VPN service for remote access and NOAA TIC for secure internet traffic.

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

NOAA6501 acquires, processes, and stores internal service delivery information and the following mission information: GIS Application Development, Marine Modeling Applications, Hydrographic Processing Applications, Modeling Data, Geographic Information System Application and Geographic Information System Data. Applicable mission information, data, and products/services is released to the public through websites. 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

The OCS collects National and International navigationally relevant and significant source data as required by NOAA's nautical charting and International Hydrographic Office policy and procedures. All relevant and significant source data received is registered into NCS Data Registry (DREG) system. The OCS interfaces 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.

As a federal organization, 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. 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.

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. OCS is compliant with all policies and procedures posted on the UAS.noaa.gov site along with the NOAA Unmanned Aircraft System Privacy Policy.

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 contractors	All mission data and PII data stored in central location on file servers.	All locations	LAN, NOAA VPN
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.

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 established by NOAA Trusted Campus and NOS Line Office backbone and network devices to securely transfer data between OCS Office locations or utilized 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

Internal CAC authenticated users are able to utilized (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 established by NOAA Trusted Campus and NOS Line Office backbone and network devices to securely transfer data between OCS Office locations or utilized 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 retrieve of the unit would be at the discretion of the operator base on safety and technical factors. Inadvertently obtain 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](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.

Questionnaire:

1. 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.*

_____ 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.*

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 (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.

_____ 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.).”

Yes, the IT system collects, maintains, or disseminates BII.
(NOTE: only collect and maintain BII for internal OCS purpose.)

Companies (NOTE: only collected through the Pre-Acquisition process through submitted technical/financial proposals for OCS contracts.)

Other business entities

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."

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

DOC employees

National Institute of Standards and Technology Associates

Contractors working on behalf of DOC

Other Federal Government personnel

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.

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?

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.

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 NOAA, NOS, Office of Coast Survey, NOAA6501 *Nautical Charting System* 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 [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO): Mary Louise A. Kurchock

Signature of ISSO: KURCHOCK.MARY
 LOUISE.A.1388550917 Digitally signed by KURCHOCK.MARY
 LOUISE.A.1388550917
 Date: 2020.03.18 14:29:12 -04'00' Date: _____

Name of Information System Owner (SO): Kathryn Ries

Signature of SO: RIES.KATHRYN.L.13
 65880456 Digitally signed by
 RIES.KATHRYN.L.1365880456
 Date: 2020.03.18 16:23:29 -04'00' Date: _____

Name of Information Technology Security Officer (ITSO): John D. Parker

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914
 Date: 2020.03.20 09:51:01 -04'00' Date: _____

Name of Privacy Act Officer (PAO): Adrienne Thomas

Signature of PAO: THOMAS.ADRIENNE.M.13
 65859600 Digitally signed by
 THOMAS.ADRIENNE.M.1365859600
 Date: 2020.04.20 16:30:51 -04'00' Date: _____

Name of Authorizing Official (AO): RDML Shepard Smith

Signature of AO: SMITH.SHEPARD.M
 ORGAN.1006778930 Digitally signed by
 SMITH.SHEPARD.MORGAN.100677893
 Date: 2020.04.03 09:07:32 -04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYR
 UM.1514447892 Digitally signed by
 GRAFF.MARK.HYRUM.1514447892
 Date: 2020.05.18 17:28:40 -04'00' Date: _____