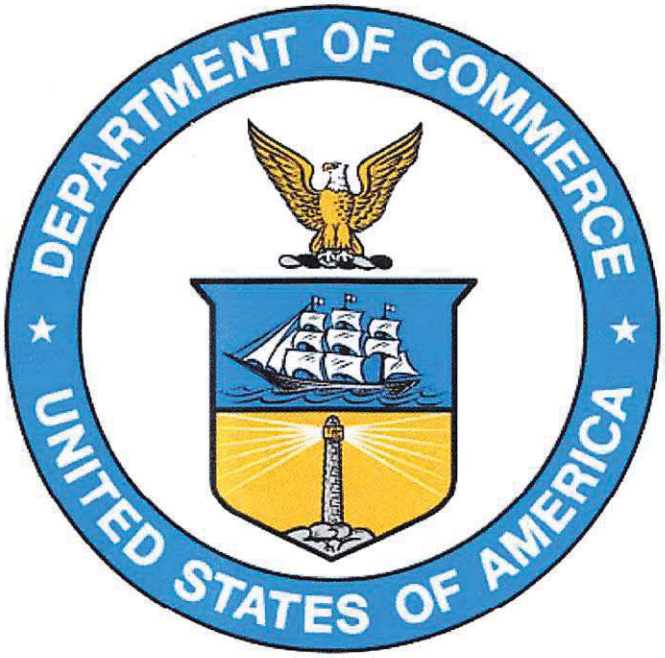
Version Number: 01-2017

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:
a) NOAA6501 is an enterprise information system (General Support System) for NOAA, National Ocean Services, Office of Coast Survey.

b) OCS headquarters is located in Silver Spring, MD (SSMC3), with field branch offices located in Norfolk VA and Seattle WA and remote individuals throughout the United States.

c) 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) 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) 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) 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.

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.

Mission data and applications are related to hydrographic processing, hydrographic and cartographic research and development, marine modeling, customer outreach, and nautical products and services. 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. OCS is researching and piloting with NOAA OMAO the use of UAS (drones) to gather aerial photos to determine if this data could assist with the accuracy of the OCS nautical charts. The data gathered from the units would be initially processed by OMAO on their ships and transferred to OCS following standard procedures used for survey data. 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 reviewing all documents posted on the UAS.noaa.gov site along with the NOAA Unmanned Aircraft System Privacy Policy.

g) 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	Federal &	Access to support	All	LAN,

administrator	contractors (On-site)	databases of Mission data.	locations	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

h) Internal authenticated users are able to utilized (based on permissions) data stored in PDF, Files, and databases. 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. This Web site is supported by the NOAA Web Operations Center, WOC (NOAA0100). These entities consist, for example, other NOAA offices, United States Coast Guard, Federal Aviation Administration, the maritime community and the general public.

i) NOAA 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 approved software 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.

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 Data Collection	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): 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 Coast Survey datasets will be conducted, and any PII inadvertently collected will be deleted within 30 days. 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					

____ 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). *Continue to answer 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. *Please describe the activities which may raise privacy concerns.*

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

__X__ Companies
____ Other business entities

____ 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 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: Mary Louise Kurchock Date: 7/30/19

Name of NOAA6501 System Owner: Kathryn Ries

Signature of SO: Kathryn Ries Date: 7/30/19

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: 2019.07.30 15:08:30 -04'00' Date: _____

Name of Authorizing Official (AO): RDML Shepard Smith

Signature of AO: Shepard M. Smith Date: 7/30/2019

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

Signature of 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: 2019.07.31 10:14:24 Date: _____