Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOAA6501, Nautical Charting System

Reviewed by: Mark Graff, Bureau Chief Privacy Officer

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Catrina D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2016.11.22 15:31:08 -05'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA/Nautical Charting System

Unique Project Identifier: UPI Code: 006-48-01-15-01-3401-00

Introduction: System Description

NOAA6501 is an enterprise information system for all actions requiring IT resources for the Office of Coast Survey's (OCS's) mission and organizational administrative functionality. NOAA6501 acquires, processes, and stores internal service delivery information and the following mission information: Geographic Information System (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, in order to produce nautical chart, services, and products. All relevant and significant source data received is registered into the internal Marine Chart Division's Data Registry (DREG) system. The OCS coordinates 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. The OCS mission nautical data does not contain PII, but PII is collected from members of the public who submit nautical chart information. This submitted PII is contact information.

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 Operations, and documentation. OCS collects BII during the pre and post activities associated with the acquisition and management of contracts.

Information Sharing

OCS collects and stores limited PII, specifically, name, telephone numbers and email addresses (voluntarily submitted by data providers and customers) to facilitate external coordination with data providers and to provide responses to customer service related requests from the diverse community of customers.

NOAA6501 as a General Support System for Office of Coast Survey, collects PII as part of the application and hiring of employees (electronic copies of resumes and hiring ranking are stored temporarily 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).

Sensitive PII, such as SSN or financial information, is entered by the employee either on printed form for NOAA Badging or directly into NFC, Travel, or Workforce management application outside of the boundary of NOAA6501.

OCS' employee data is collected, stored and maintained for internal OCS COOP, Human Resource, and workforce planning purposes (federal employee/contractor).

OCS collects BII during the pre and post activities associated with the acquisition and management of contracts. The storage is in the form of PDF forms or MS Word documents. There is no major application or database used to collect or store employee PII or BII information. OCS does not have a separate HR division since OCS utilizes the NOAA Workforce Management Office.

Final OCS mission 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, of other NOAA offices, United States Coast Guard, Federal Aviation Administration, the maritime community and the general public.

(a) a citation of the legal authority to collect PII and/or BII:
5 U.S.C. § 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

For PIAs covered, or also covered, by the SORN COMMERCE/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission, 15 U.S.C. § 1512 applies. It is an Organic Law which confers general powers and duties authority to executive agencies, vesting jurisdiction and control of departments, bureaus, offices and branches

The Federal Information Processing Standard (FIPS) 199 security impact category for the system is: *Overall: Moderate* [Confidentiality –Low/ Integrity-Moderate/ Availability-Moderate]

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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):					

__X___ This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID	x	f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport	x	k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: N/A					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	x	o. Medical Information	
d. Gender		j. Telephone Number	x	p. Military Service	
e. Age		k. Email Address	x	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): OCS utilizes NOAA for workforce management and NOAA Office of security for badging. General employee information is retained for teleworking agreements and COOP.					

Work-Related Data (WRD)					
a. Occupation	x	d. Telephone Number	x	g. Salary	x
b. Job Title	x	e. Email Address	x	h. Work History	x
c. Work Address	x	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs	x	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify): OCS does not capture photographs for badging since that is performed (and stored) by the NOAA Office of Security. OCS does utilize pictures of specific individuals (with written permission) as part of either internal or external website as part of OCS program, possible profile narrative, and/or presentation of OCS mission nautical activities.					

System Administration/Audit Data (SAAD)					
a. User ID	x	c. Date/Time of Access	x	e. ID Files Accessed	x
b. IP Address	x	d. Queries Run		f. Contents of Files	x

g. Other system administration/audit data (specify):

Other Information (specify) BII – Pre and Post Acquisition. This BII information would be obtained and utilized during the pre acquisition obtained through deliverable BIDS package and contain specific company information. BII information would be maintained on specific secure network folders during the execution of awarded contract and other information from companies not receiving awards would be deleted, when appropriate.

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	x	Hard Copy: Mail/Fax	x	Online	x
Telephone	x	Email	x		
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify) :					

Non-government Sources					
Public Organizations	x	Private Sector	x	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): OCS does not acquire PII from other non-government sources. These non-government sources would be only for BII associated with Pre/Post Acquisition Sensitive Information obtained through delivered bids on OCS Acquisitions.					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

x	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	

Video surveillance		Electronic purchase transactions	
Other (specify):			

x	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	x
For administrative matters	x	To promote information sharing initiatives	x
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Collected BII would be associated with determine qualification/eligibility for open acquisitions. PII would be collected for OCS administrative actions, for HR and Workforce management.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

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 and contractor 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. No SSN is collected or stored within NOAA6501. Sensitive PII, such as SSN or financial information, is entered by the employee either on printed form for NOAA Badging or directly into NFC, Travel, or Workforce management application outside of the boundary of NOAA6501.

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, the OCS system communicates with the diverse community of national

and international chart product and services users.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	x		
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

Internal OCS employees' PII is collected for appropriate Human Resource records, COOP Operations /documentation and workforce planning internal to OCS. Since OCS is a NOAA program office under the NOS Line Office, some HR related information will be shared with NOS and NOAA workforce management offices as required to handle HR activities and workforce management.

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

x	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. NOAA6501 is connected to the NOS Line Office information system NOAA6001 and other NOAA information systems for VPN, Security and Network Operations. ***NOAA6501 does NOT share or received PII or BII through these technical infrastructure (backbone) connections.*** OCS established security permissions based on NOS Active Directory Network account (enforced 2FA when possible), restrictions in firewall ACL and security permissions on specific network folders where documentation is stored.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	x
Contractors	x		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
x	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: _ http://www.nauticalcharts.noaa.gov/staff/privacy_policy.htm. *A Privacy Act Statement is being processed through OCS and NOS website governance and the OCS Configuration Management process in order to incorporate it into applicable OCS Web pages.*	
x	Yes, notice is provided by other means	Specify how: The contact information is collected through NOAA6501 Web-based applications: CCWEB and Nautical Discrepancy Report System. The Web-based applications request user email address via a Web-based form to facilitate communication and OCS response. b. Notice was provided to partners and customers for the following: • CCWeb data collection; Federal Register Vol. 69, No. 189 Sept. 30, 2004 • ChartFacilities data collection from Marina Owners or Marina Operators; • Register Vol. 69, No. 85 May 3, 2004 (Planned Data Collection). These information collections are voluntary. By

		providing the data through the CCWeb site, the individual consents to its use. United States Power Squadron (USPS) users can access OCS information only by entering in their USPS certificate numbers and a DOC-compliant password which is validated as part of the authentication control. As of 5/1/2016, the CCWEB site was removed, but information is being included in the PIA in case the organization re-establishes the website. Nautical Discrepancy Report System is still available to the public at http://ocsdata.ncd.noaa.gov/idrs/discrepancy.aspx Employees are given notice on the applicable HR forms.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

x	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Navigational information collections are voluntary. By providing the data through the email or online forms, the individual consents to its use for the purpose of follow-up contact on information provided. OCS administrative PII is collected through the employee's application for employment and workforce management. The employee is fully informed of how the information will be utilized when collected, during the onboarding process. The employment application contains the Privacy Act notice. Applicants have the opportunity to decline to provide PII, in writing, to the HR representative or to their supervisors, but it might affect the overall processing of their employment. BII can be declined to be provided as part of the acquisition package but could impact evaluation of bid.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Navigation information collections are voluntary. By providing the data through the email or online forms, the individual consents to its use for the purpose of follow-up contact on information provided. OCS administrative PII is collected through the employee's application for employment and workforce management. The employee is fully informed of how the information will be utilized when collected. The employment application contains the Privacy Act notice. Applicants have the opportunity to consent to only particular uses of their PII, in writing, to the HR representative or to their supervisors, but it might affect the overall processing of their employment. BII are submitted for a specific purpose which consent is implied with the submittal of the package.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

x	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Those accessing information can contact OCS directly by email or phone as listed in the Privacy policy on the NauticalCharts.Noaa.Gov page OCS Employees can contact HR staff or the federal employee personnel page to update their information, as they are informed as part of new employee orientation.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreements.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.

x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to the PII/BII is restricted to authorized personnel only.
x	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access to storage folders are restricted by ACL but since PII is not centralized in a database it cannot be easily monitored for access.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 4/22/2016 (next is 12/1/2016) ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
x	Other (specify): All appropriate contractors and contract clauses include non-disclosure, but not all federal employees sign a confidentiality agreement or non-disclosure agreement.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

All information is stored within the accredited boundaries of NOAA6501 in network data shares controlled by established permission based on the organizational, project, or employee access rights. Any access to specific restricted files or folders must be requested through an Access Change request which is reviewed and documented by the OCS Information System Security Officer for authorization and mission 'need-to-know' requirement prior to implementation. Least privilege was implemented through file share permissions to ensure privacy and open only to those demonstrating a "need to know".

Any PII information which is transmitted electronically must follow the federal government and NOAA standard procedure of secure packaging such as utilization of DOC Accellion for encryption in transit.

OCS implements those security controls listed in NIST Special Publication 800-53 R4 required for a Moderate System. NOAA6501 is under a current Authorization To continue to Operate (ATO) signed 4/22/2016. In compliance with NIST Special Publication 800-53, the Office of Coast Survey has a full security program, with performance measures and goals, in order to complete continuous monitoring activities (annual security control reviews, quarterly vulnerability scanning, monthly review of security access control list, weekly review of audit logs, daily handling of Access Change Requests and involved in OCS Change Board activities). The risk assessment included the possible threats and vulnerability to the confidentiality, integrity, and availability of mission and sensitive PII data along with the countermeasures.

Every year the IT system undergoes a thorough Continuous Monitoring for the Assessment and Authorization (A&A) process that is performed independent contractor. The A&A process ensures that the security plan and operational, management, and technical controls meet Department of Commerce (DOC) guidelines for continued operation.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

x	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission. DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons DEPT-18, Employees Personnel Files Not Covered By Notices of Other Agencies
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

x	There is an approved record control schedule. Provide the name of the record control schedule: The retention period for these records is guided by the General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the federal government. In accordance with GRS 20, item 3, electronic versions of records scheduled for disposal may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. In accordance with GRS 20, item 3, the data is presently being retained indefinitely. For OCS administrative PII data, the records would be covered under the following NARA general records schedules: GRS 2 – payroll and pay administrative records GRS 20 – electronic records GRS 23 – records common to most offices within agencies OCS's contact information (contractor, partner, and customer) are collected to provide a means for the Office of Coast Survey to communicate and respond to needs and requests. This data would be retained as long as the individual continued to request contact and

	information. It is technologically possible to delete information at the request of the individual. There is no scheduled records retention for this information. OCS mission data is associated with Water Transportation and Navigation and does not contain PII data. Only the "historical" chart information is retained indefinitely due to the nature of the information. All other mission data would be retained as long as the information is required to produce the OCS deliverable and each project would establish the records retention scheduled based on the project, model, or deliverable. All mission data is releasable as "public-accessible" information and does not contain PII. NOS Records Disposition schedule for the information system for mission data: N1-370-00-3 Nautical Mapping and Charting 1604-01 to 1604-13 (PII not contained in this record set)
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
x	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	x	Overwriting	x
Degaussing		Deleting	x
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
x	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

x	Identifiability	Provide explanation: Administrative PII is not stored in a centralized database, application or location. Most MS Word documents would be stored across the OCS network and would

		require time to search all network resources to locate PII.
x	Quantity of PII	Provide explanation: OCS has a limited quantity of PII necessary for HR actions and management.
x	Data Field Sensitivity	Provide explanation: OCS has a limited quantity of sensitive PII information necessary for HR actions and managementOCS does not store SSN.
x	Context of Use	Provide explanation: This is only limited PII with a specific HR purpose utilized by HR personnel or supervisors.
	Obligation to Protect Confidentiality	Provide explanation:
x	Access to and Location of PII	Provide explanation: Documents are stored to restricted shared networks, restricted based on single individual or OCS division based on need to know basis.
x	Other:	Provide explanation: The loss of a single individual's PII would have an impact on that individual through possible identify theft and OCS as a government identity BUT it would not have an impact on the OCS mission dealing with nautical data, products, and services.

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: A Privacy Act statement added to the OCS Web site. *No change to current OCS business processes, but OCS will be issuing formal policy to reinforce that the storage or retention of SSN is not authorized on any component within NOAA6501.*
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
x	No, the conduct of this PIA does not result in any required technology changes.