Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
NOAA6501
Office of Coast Survey (OCS 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

GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF.MARK.HYRUM.1514447892
Date: 2024.04.29 13:36:08 -07'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA// NOS/OCS Nautical Charting System (NOAA6501)

Unique Project Identifier: NOAA6501 (UII Code: 006-48-01-15-01-3401-00)

Introduction: System Description

Provide a brief description of the information system.

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

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. 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. OCS mission nautical data does not contain personally identifiable information (PII), but PII is collected from members of the public who submit nautical chart information. This submitted PII is contact information.

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 (HR)-related issues as well as workforce planning, operating budget, Continuity of Operations (COOP) activities, and documentation. OCS collects business identifiable information (BII) during the pre and post activities associated with the acquisition and management of contracts.

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 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.

(b) System location

- OCS headquarters, Silver Spring, MD

- NOS-OCS-AWS cloud, Herndon, VA
- Hydrographic Surveys Division (HSD) Atlantic Hydrographic Branch, Norfolk, VA
- HSD Pacific Hydrographic Branch, Seattle, WA
- External Data Center (EDC)-Ashburn, Ashburn, VA
- NOS OCS AZURE subscription (this is not a new location, but was inadvertently removed from the last SAOP approved PIA)

(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;
- NOAA0550 - NOAA Enterprise Network (NWAVE) – the NOAA campus backbone used to connect to the Internet;
- NOAA0900 - Consolidated cloud application;
- NOAA0700 - High Availability Enterprise Services (HAES) which supplies centralized Enterprise service for the ICAM component for the NOAA community; and
- NOAA0100 - NOAA Cyber Security Center (NCSC)
- NOS OCS AZURE subscription (utilized for external data backup) (this is not a new interconnection, but was inadvertently removed from the last SAOP approved PIA)

NOAA6501 utilizes NOAA VPN for remote connectivity and NOAA NWAVE for connection to AWS East/West FedRamp Cloud and NOAA Enterprise Data Center.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

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 Trusted Internet Connections (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.

(e) 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 directory, access controls and permission, etc.

Internal Common Access Card (CAC) authenticated users are able to utilize (based on permissions) data stored in PDF, files, and databases through networked client 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 navigational products through open websites. Final digital data products and services (i.e., Booklet Charts; Electronic Navigational 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 of other NOAA offices, United States Coast Guard (USCG), Federal Aviation Administration (FAA), the maritime community, and the general public.

(f) 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 Interconnection Security Agreement (ISA) for the transfer of data between government organizations. All information approved to be released to the public are posted on OCS external websites for distribution.

HR: NOAA6501 gathers and stores PII related to hired employees and contractors of the OCS, which is collected, stored and maintained for Human Resource-related issues as well as workforce planning, operating budget, COOP/ Disaster Recovery (DR) Operations, and documentation.

The documents containing PII are gathered on an ad-hoc basis 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 unmanned aerial systems (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 Office of Marine and Aviation Operations (OMAO) to use UAS (drones) for gathering aerial photos in order to assist with the accuracy of OCS nautical charts. It is anticipated that the 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.

(g) Any information sharing

The only information shared externally is mission specific and is non PII or BII data.

External Internet users are able to retrieve posted OCS nautical charts and navigational products through open websites. Final digital data products and services (i.e. BookletCharts; 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 of other NOAA offices, the USCG, FAA, the maritime community and the general public. Documented ISA will be utilized to document and approve any 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 utilized secure external hard drives. OCS utilizes DOC approved software for the transfer of any sensitive information between remote OCS individuals, off the internal network and not connected to the NOAA VPN.

Based on the NOAA user base, as listed in the NOAA 6501 Risk Assessment Report:

User Type	Type	Data access	Location	Connection
Authenticated OCS Users	Federal & NOAA Corps, contractors, associates	All mission data	All locations	LAN, NOAA VPN
Supervisor	Federal, or contractors	All mission data and PII data	All locations	LAN, NOAA VPN
IT Services staff	Federal & contractors (On-site)	Access to all IS Data is 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

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information.

Type of Information Collected	Applicable SORNS	Programmatic Authorities
Personnel Actions Including Training	COMMERCE/DEPT-1	31 U.S.C. 66a
		44 U.S.C. 3101, 3309
		Title 5 U.S.C.
	COMMERCE/DEPT-18	44 U.S.C. 3101
		Executive Orders 12107, 13164,
		41 U.S.C. 433(d)
		5 U.S.C. 5379
		5 CFR Part 537
		Executive Order 12564
		Public Law 100-71
		Executive Order 11246
		26 U.S.C. 3402
FOIA & Privacy Act Requests	COMMERCE/DEPT-5	5 U.S.C. 552, Freedom of Information Act
		5 U.S.C. 552a, Privacy Act of 1974 as amended
		5 U.S.C. 301
		44 U.S.C. 3101
System for Award Management (SAM)	GSA-GOVT-9	2 CFR, Subtitle A, Chapter I, and Part 25
		40 U.S.C. 121(c); FAR Subparts 9.4 and 28.2
		Executive Order 12549 (February 18, 1986
		Executive Order 12689 (August 16, 1989)
Federal Acquisition Regulation (FAR) Data Collection System	GSA-GOVT-10	E-Government Act of 2002 (Pub. L. 107–347) Section 204
		Davis-Bacon and Related Acts
		40 U.S.C. 3141–3148
		40 U.S.C. 276a
		29 CFR parts 1, 3, 5, 6 and 7
		Section 5 of the Digital Accountability and Transparency Act (DATA Act), Public Law 113–101
Badging & CAC Issuance	COMMERCE/DEPT-18	Electronic Signatures in Global and National Commerce Act, Public Law 106-229
		5 U.S.C. 301
System Administration/Audit Data (SAAD)	COMMERCE/DEPT-25	5 USC 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors

		Electronic Signatures in Global and National Commerce Act, Public Law 106-229
		28 U.S.C. 533-535
Emergency Preparedness/COOP	COMMERCE/DEPT-18	Executive Order 12656
		Federal Preparedness Circular (FPC) 65, July 26, 1999
Managing Access Accounts and Login Names	COMMERCE/DEPT-25	5 USC 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
		Electronic Signatures in Global and National Commerce Act, Public Law 106-229
		28 U.S.C. 533-535
Public Health Emergency Info & Reasonable Accommodation	COMMERCE/DEPT-31	Rehabilitation Act, 29 U.S.C. 701 et. seq
		Americans with Disabilities Act of 1990, as amended, 102(d), 42 U.S.C. 12112(d)
		29 CFR parts 1602, 1630, 1904, 1910, and 1960
		29 USC chapter 15 (e.g., 29 U.S.C. 668)
		Executive Order 12196
		5 U.S.C. 7902
Credit Card & Financial Information	COMMERCE/DEPT-1	31 U.S.C. 66a
		44 U.S.C. 3101, 3309
Financial Information	COMMERCE/DEPT-2	28 U.S.C. 3101-3105
		Debt Collection Act of 1982 (PL 97-365)
		26 U.S.C. 6402(d)
		31 U.S.C. 3711
		Federal Financial Assistance Management Improvement Act of 1999
		Public Works and Economic Development Act of 1965, as amended by the Economic Development Administration Reauthorization Act of 2004 (Pub. L. 108-373)
		4 CFR 102.4
		Chief Financial Officers Act (CFOs Act) of 1990, P.L. 101-576
		Federal Managers' Financial Integrity Act of 1982, P.L. 97-255 (31 U.S.C. 3512 et seq.);
		Office of Management and Budget (OMB) Circular A-127, Financial Management Systems

Travel Records	COMMERCE/DEPT-9	Budget and Accounting Act of 1921
		Accounting and Auditing Act of 1950
		Federal Claim Collection Act of 1966
		FPMR 101-7
		5 U.S.C. 5701-09
Contract / Grant Information	COMMERCE/DEPT-2	28 U.S.C. 3101-3105, Debt Collection Act of 1982 (Pub. L. 97-365)
System for Award Management (SAM)		26 U.S.C. 6402(d)
		31 U.S.C. 3711
	GSA/GOVT-9	FAR Subparts 4.11, 52.204
		2 CFR Subtitle A
		40 U.S.C. 121(c)
		FAR Subparts 9.4 and 28.2
		Executive Orders 12549, 12689
Visitor Logs & Permits for Facilities	COMMERCE/DEPT-6	5 U.S.C. 301
		44 U.S.C. 3101
Contact Information for the Public	NOAA-11	5 U.S.C. 301, Departmental Regulations
		15 U.S.C. 1512, Powers and duties of Department
	COMMERCE/DEPT-23	15 U.S.C. § 272
		15 U.S.C. § 1151
		15 U.S.C. § 1512
		15 U.S.C. § 1516
		E.O. 11625
Biographical Files and Social Networks	COMMERCE/DEPT-20	5 U.S.C. 301
		5 U.S.C. App.--Inspector General Act of 1978, section 2
		5 U.S.C. App.--Reorganization Plan of 1970, section 2
		13 U.S.C. section 2
		13 U.S.C. section 131
		15 U.S.C. section 272
		15 U.S.C. section 1151
		15 U.S.C. section 1501
		15 U.S.C. section 1512
		15 U.S.C. section 1516
		15 U.S.C. section 3704b

		16 U.S.C. section 1431
		35 U.S.C. section 2
		42 U.S.C. section 3121 et seq.
		44 U.S.C. 3101 and Reorganization Plan No. 5 of 1950
		47 U.S.C. section 902; 50 U.S.C. App. section 2401 et seq.
		E.O. 11625
		77 FR 49699
		Presidential Memorandum to the Heads of Executive Departments and Agencies on Transparency and Open Government, January 21, 2009
		OMB Open Government Directive, M-10-06, December 8, 2009
		OMB Guidance for Online Use of Web Measurement and Customization Technologies, M-10-22, June 25, 2010
		OMB Guidance for Agency Use of Third-Party Web sites and Applications, M-10-23, June 25, 2010

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

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):					

____ 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.

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.

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*		f. Driver's License		j. Financial Account	X
b. Taxpayer ID		g. Passport	X	k. Financial Transaction	
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card	X	m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					

*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:
Identified PII associated with HR for standard Federal employment or BII associated with contracts and/or acquisitions within NOAA6501 are NOT mission data.

OCS gathers SSN (temporarily obtained but not stored in NOAA6501), Name and Address which is entered into the Contractor Verification System Application run by DoD outside NOAA6501 for incoming employee badging. All HR in-bound for new employees is handled by Office of Human Capital Services (OHCS) who shares PII, by necessity, with the NFC (run by Agriculture) and OPM. Our payroll is handled by NFC. OCS Management issued an email stating that SSN must be removed from all PDF and forms and not stored with NOAA6501. Credit card information is directly associated with issued Government bank cards. Finance account information is directly associated with acquisitions.

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	
b. Maiden Name	X	i. Place of Birth	X	p. Medical Information	
c. Alias	X	j. Home Address	X	q. Military Service	X
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Marital Status	
f. Race/Ethnicity		m. Education	X	t. Mother's Maiden Name	
g. Citizenship		n. Religion			

u. Other general personal data (specify):
Identified PII associated with HR for standard Federal employment or BII associated with contracts and/or acquisitions within NOAA6501 are NOT mission data.

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	X
c. Work Address	X	g. Work History	X	k. Procurement/contracting records	X
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		

l. Other work-related data (specify):

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs	X	j. Weight		o. Dental Profile	

p. Other distinguishing features/biometrics (specify):
OCS does not capture photographs for badging since that is performed (and stored) by the NOAA Office of Security (OSC). OCS does utilize staff pictures (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. 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. Any PII collected is incidental, unintentional, and not retained.

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	

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

Other Information (specify)
BII information obtained and utilized during pre-acquisition evaluation and through deliverable bids packages, may contain specific company information. BII information is kept on specific restricted network drive folders during the execution of the awarded contract. Information from other firms not receiving the award may be deleted, when appropriate. This information is protected under 41 USC

253, the FOIA exemption 3 statute for contract proposal and associated information collection.

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	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

Mission data
OCS mission data is posted after completing quality assurance validation. All incoming mission data undergoes complete quality assurance prior to be incorporated into the mission business process. Submitted public customer contact information does not undergo validation and is deleted if the email is invalid.

Acquisitions
Acquisition data is reviewed by the contracting officer. Data is verified by the contracting officer contacts via Email and phone calls; this process is used to verify information provided by the vendor.

HR Data
HR data is validated at the time of receipt by the HR representative. The HR representative compares picture ID and other information to validate the applicant's identity. For travel, the HR representative also validates the information at the time of collection. This includes comparison of Driver's license and Passport. HR data for travel is only used to assist the employee in making travel arrangements and is not stored. Applicant data is only maintained during the hiring process.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0648-0007 OCS Nautical Discrepancy Reporting System (webpage: ASSIST) 0648-0762, 3D Nation Elevation Data Requirements and Benefits Study 0648-0508, Application and Certification Requirements for Distributors of NOAA Electronic Navigational Charts / NOAA Hydrographic Products Grant forms: 4040-0001, 4040-0004, 4040-0010, 4040-0020
	No, the information is not covered by the Paperwork Reduction Act.

2.5 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): The utilization of UAS (drones) to gather aerial photos to assist with the accuracy of the OCS nautical charts. Although the OCS UAS has the potential to collect PII via patterned single images taken during the drone flight, it is not the purpose of the device and any inadvertently PII captured will be immediately deleted, when identified during the data processing stage.			

	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			
For a Computer Matching Program		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)	X

Other (specify):

Mission data

Stakeholder or public-user-submitted contact information would be collected through emails or submitted on forms on OCS public websites. This contact information would be stored in both email and database for later use to contact the individual as follow-up or distribution of OCS nautical products and charts. The data would only be disseminated or available by technical permissions to those individuals assigned specific roles and responsibilities associated with those mission projects.

On public websites, OCS utilizes staff pictures (with written permission) as part of either internal or external website as part of OCS program (such as federal government organizational charts and leadership), possible profile narrative, and/or presentation of OCS mission nautical activities.

HR Data

OCS collects PII within documents or PDF, on an ad-hoc basis, as part of the application and hiring of employees. This include electronic copies of resumes stored temporarily during the hiring phase. Also stored temporarily are standard HR information such as travel authorization and vouchers, passports and international travel forms, and information for transmitting the security badge request email, which includes only an email address and possibly a phone number. OCS established a centralized folder structure specifically maintaining HR documents separate from general mission project folders. The permissions were established for read or modify rights based on assigned roles and responsibilities within the organization. Dissemination is performed only based on required HR business process within OCS, NOAA, and DOC.

Acquisitions

BII information obtained and utilized during pre-acquisition evaluation and through deliverable BIDS packages may contain specific company information. BII information is kept on specific restricted network drive folders during the execution of the awarded contract. Information from other firms not receiving the award may be deleted, when appropriate. Dissemination is based on assigned roles and responsibilities for vetting panel or appropriate COR.

UAS

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 OCS nautical charts. It is anticipated that the 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. Any PII collected is incidental, unintentional, and not retained. UAS would be maintained in separate folder, mission data validated for incorporation into OCS mission nautical charts. The UAS would not be disseminated as collected data but relevant data incorporated into OCS products.

Information sharing

NOAA6501 has multiple public websites using multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. 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). Information shared within OCS, NOS, and NOAA is scientific data only.

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).

Mission Distribution / contacts
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. 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 utilizes 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
OCS 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, HR, 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 the 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 contains 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 a 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 would be incorporated into OCS products. Any PII collected is incidental, unintentional, and not retained. It is anticipated that the 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.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Insider threat is a potential threat to privacy; however, users are required to take security and privacy awareness training annually in an effort to mitigate this threat.

Mission Data
Mission data does not contain PII or BII. Most mission data is posted for public consumption. Contact information contains names, emails, and possibly phone numbers. This contact information could be used by unauthorized personnel to SPAM an individual.

- Users take privacy training at least annually in the required annual security awareness course.
- Users sign rules of behavior to ensure they understand their responsibilities.

HR
If users print information from the system (administrative data or contact information), there is a chance that privacy data will be viewed by unauthorized individuals within OCS if the document is left in plain sight.

- Supervisors are assigned local printers to reduce visibility to others.
- Old data is purged from the systems per retention schedule.
- Users take privacy training at least annually in the required annual security awareness course.
- Users sign rules of behavior to ensure they understand their responsibilities.
- Users "need to know" is validated by security staff before user added to specific restricted folders or files.

Acquisition
If authorized individuals copy or print BII information, there is a chance that BII could be viewed by unauthorized OCS employee.

- Old data is purged from the systems per retention schedule.
- Users take privacy training at least annually in the required annual security awareness course.
- Users sign rules of behavior to ensure they understand their responsibilities.
- Users "need to know" is validated by security staff before user added to specific restricted folders or files.

UAS
Any PII collected is incidental, unintentional, and not retained. It is anticipated that the 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.

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	x		
Federal agencies	x		
State, local, tribal gov't agencies			
Public	X (see note)		
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.
NOTE:	Internal OCS employees' PII is collected for appropriate HR records, COOP 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. OCS gathers SSN, names and addresses which are entered into the Contractor Verification System run by DoD. SSN is not authorized to be stored on NOAA6501. OCS could share, case by case, information with other federal agencies such as OPM, DoD or maybe investigative units should the need arise. Public: On public websites, as well as several social media accounts (Facebook and Twitter), OCS utilizes 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.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

X	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NOAA6501 interconnects to: • NOAA6001 - NOS Enterprise Information System - for connections to NOS hosted applications; • NOAA0550 - NOAA Enterprise Network (NWAVE) – the NOAA campus backbone used to connect to the Internet; • NOAA0900 - Consolidated cloud application; • NOAA0700 - High Availability Enterprise Services (HAES) which supplies centralized Enterprise service for the ICAM component for the NOAA community; and • NOAA0100 - NOAA Cyber Security Center (NCSC) • NOS OCS AZURE subscription (utilized for external data backup) NOAA6501 utilizes NOAA VPN for remote connectivity and NOAA NWAVE for connection to AWS East/West FedRamp Cloud and NOAA Enterprise Data Center. NOAA6501 does not share or receive 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 access control lists (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.

6.4 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	X (see note)	Government Employees	x
Contractors	x		
Other (specify): NOTE - Public: OCS utilizes staff pictures (with written permission) as part of either internal or external website as part of OCS program (such as federal government organizational charts and leadership), possible profile narrative, and/or presentation of OCS mission nautical activities.			

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: https://nauticalcharts.noaa.gov/about/privacy-policy.html .	
x	Yes, notice is provided by other means.	Specify how: ● Nautical Discrepancy Report System is available to the public at https://www.nauticalcharts.noaa.gov/customer-service/assist/ ● Privacy notice link is at the bottom of the page which displays: https://nauticalcharts.noaa.gov/about/privacy-policy.html ● Employees are given notice on the applicable HR forms. For telephone PII collection: phone PII callers are directed to the webpages where they can view the PAS.
	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 as described in the website privacy policy or listed on the form. OCS administrative PII is collected through the employee's application for employment and other requests such as a COOP calling tree. 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 decline to provide PII, in writing, to the HR representative or to their supervisors, but it might affect the overall processing of their employment. For the COOP calling tree, employees may decline to provide their PII (in person or in writing, to their supervisors) but they will then not be notified of emergencies through this process. BII provided for acquisition consideration is not mandatory. However, declining to provide the information necessary to evaluate them for an acquisition could result in non-award. Staff members are notified upon request in writing for collection of identifying information, such as photo used for external purposes. They may decline to provide the information via email or verbally, to their supervisors.

	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 applications are submitted via OPM and NOAA OHCS and have explicit Privacy Act notices. 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. For training/webinars, requests of name and email are voluntary, and are used only with regard to this purpose. The purpose for internally collected PII (contact information) for the COOP call tree or emergency contact information is identified in the email/ request for information submitted to the individual who can chose to submit or not. OCS administrative PII may be collected with respect to ongoing business tasks e.g., travel, and is only used for that specific task. For telephone PII collection: phone PII callers are directed to the webpages where they can view the PAS. BII provided for an acquisition consideration is not mandatory; however, declining to provide the information necessary to evaluate an acquisition may result in a non-award. Staff members are notified upon request in writing for collection of identifying information, such as photo used for external purposes. They may decline to provide the information via email or verbally, to their supervisors.
	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 individuals who submitted contact information may 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. OCS employees may contact HR Staff, supervisors or the Employee Personnel Page (MyEPP) or Personnel Office files (ePO) to review/update their information, as they are informed as part of new employee orientation. Staff members are notified upon request in writing for collection of identifying information, such as photo used for external purposes. They can request that any posted image of them be taken down and the image will be removed promptly.
	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.)*

x	All users signed a confidentiality agreement or non-disclosure agreement.
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.
	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 the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 06/27/2023 ☐ 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 controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
x	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
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 DOC ownership rights over data including PII/BII.
x	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

All information is stored within the accredited boundaries of NOAA6501 and stored 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 OCS Information System Security Officer (ISSO) 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 that is transmitted electronically must follow the federal government and NOAA standard procedure of secure packaging such as utilization of Agency DOC/NOAA Secure File Transfer application for encryption in transit.

OCS NOAA6501 is categorized as a Moderate IT System using the FIPS-199 standards where Mission data is documented as Confidential and Low, and internal HR, Acquisition and Security data/information Confidential as Moderate. NOAA6501 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). In compliance with NIST Special Publication 800-53R4, 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 by an 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 Is the PII/BII searchable by a personal identifier (e.g,, name or Social Security number)?

X Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 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, number, and link. *(list all that apply)*: • Commerce/DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons • Commerce/DEPT-2, Accounts Receivable • Commerce/DEPT-5, Freedom of Information and Privacy Request Records • Commerce/DEPT-6, Visitor Logs and Permits for Facilities Under Department Control • Commerce/DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons • Commerce/DEPT-18, Employees Personnel Files not covered by Notices of Other Agencies • Commerce/DEPT-20, Biographical Files and Social Networks • Commerce/DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs. • Commerce/DEPT-25, Access Control and Identity Management System • Commerce/DEPT-31 Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations • NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission • GSA-GOVT-9, System for Award Management • GSA-GOVT-10, FAR Data Collection System
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

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. The retention period for OCS 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. NOAA6501 records are not stored in an automated application, which would allow for automated removal based on retention schedule. Documents are manually removed by responsible parties when identified. For OCS administrative PII data, the records would be covered under the following NARA general records schedules: • GRS 2.4 – Employee Compensation & Benefits Records • GRS 2.5 – Employee Separation Records • GRS 3.1 – General Technology Management Records • GRS 3.2 – Information System Security Records • GRS 4.1 – Records Management Records • GRS 4.2 – Information Access & Protection Records • GRS 5.1 – Common Office Records • GRS 5.2 – Transitory & Intermediary Records 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. 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 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) <u>Applicable NOAA Records Schedules</u> ● Chapter 100 - General ● Chapter 200 - Administrative and Housekeeping Records ● Chapter 300 - Personnel ● Chapter 400 - Finance ● Chapter 700 - Procurement Supply and Equipment Maintenance ● Chapter 900 - Facilities Security and Safety ● Chapter 1200 - Scientific Research ● Chapter 1600 - Ocean Programs ● Chapter 2300 - General Information Technology Management Records ● Chapter 2400 - Information System Security Records
	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 Level

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. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals (employees, contractors, the public) could be identified based on the information collected.
X	Quantity of PII	Provide explanation: OCS has a limited quantity of PII necessary for HR actions and management. Most PII is only stored for a temporary amount of time and with limited number of individuals authorized to access this information. Travel documents and some acquisition documents are retained for auditing purposes.
X	Data Field Sensitivity	Provide explanation: OCS has a limited quantity of PII necessary for HR actions and management stored as PDF or word documents. NOAA6501 does not have an application or database of administrative PII data. OCS Management released an email stating that no SSN can be stored on OCS resources in a files or forms.
X	Context of Use	Provide explanation: There is limited PII with a specific HR purpose utilized by HR personnel or supervisors and limited BII data used by specific individuals for acquisition processing. All individuals and supervisors undergo training for use, restrictions, storage, and protection of privacy related use.
X	Obligation to Protect Confidentiality	Provide explanation: Supervisors and administrative officers are trained on their roles and responsibilities to protect internal OCS administrative data. Those assigned a role and responsibilities associated with acquisitions are notified of their obligations at the start of the process by the contracting officer. Programmers and website support are informed of the correct processing of PII obligations during the Software Development Life Cycle (SDLC) security evaluation by the ISSO along with general privacy awareness training.
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. Any requested changes or additions of individuals to restricted folders must be approved by the supervisor along with the security team representative as part of the change management process.
X	Other:	Provide explanation: The loss of a single individual's PII would have an impact on that individual and OCS as a government identity but it would not have an impact on the OCS mission dealing with nautical data, products, and services. Stored PII is associated with HR for standard Federal employment or stakeholder / public contact information (Name, phone, email address). Stored BII associated with contracts and/or acquisitions. OCS gathers SSN (temporarily obtained but not stored in NOAA6501), for incoming employee processing in the form of Adobe PDF and/or Word documents. Credit card information is

		directly associated with issued Government bank cards. Finance account information is directly associated with acquisitions.

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

OCS internal administrative HR and acquisition data is collected based on the requirements associated with employment with the federal government or doing business with the federal government. All necessary information is obtained, securely maintained, and disposed of based on NARA retention schedules. OCS management issued restrictions that no SSN can be stored in files stored within NOAA6501 to reduce the privacy risk. OCS created a centralized restricted HR folder structure to reduce privacy HR documents being stored in unsecure folders or unknown locations within shared resources.

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

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 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.