Version Number: 01-2019

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
National Geodetic Survey General Support System
(NOAA6401)

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

for Dr. Catrina D. Purvis LISA MARTIN Digitally signed by LISA MARTIN Date: 2020.03.27 14:45:56 -04'00' 03/27/2020

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/National Geodetic Survey General Support System

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

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

General Support System

(b) System location

NGS's primary facility is in Silver Spring, MD, with much smaller facilities <10 employees in: Norfolk, VA, Woodford, VA, Boulder CO, Longmont, CO.

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

NOAA6001 NOS for Enterprise Level Services United States Coast Guard (USCG) Differential Global Positioning System (NDGPS) for GPS data (incoming only) will stop at end of FY20 Federal Aviation Administration (FAA) for GPS data (incoming only)

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

The mission of the National Geodetic Survey (NGS) is to define, maintain and provide access to the National Spatial Reference System (NSRS) to meet our nation's economic, social, and environmental needs. Using NOAA6401, NGS provides the framework for all positioning activities in the Nation. The foundational elements—latitude, longitude, elevation and shoreline information—contribute to informed decision making and impact a wide range of important activities including mapping and charting, flood risk determination, transportation, land use, and ecosystem management. NGS' authoritative spatial data, models and tools are vital for the protection and management of natural and man-made resources and support the economic prosperity and environmental health of the Nation.

The major NGS products and services are: Aeronautical Surveys Program (ASP), Antenna Calibration, Acquisitions, Continuous Operating Reference Stations (CORS) Data Ingestion and Distribution, Continuous Operating Reference Stations (CORS) Data Coordinate and Velocity Computation, Emergency Response Imagery (ERI), General Passive Control Tools, Geoid, Gravity for the Redefinition of the Vertical Datum (GRAV-D), Office Automation and Collaboration, Online Positioning User Service (OPUS), Orbit Processing, Shoreline Mapping Program, VDatum.

(e) How information in the system is retrieved by the user

Outside non-authenticated users connect to a public web server. Internal authenticated users can retrieve data based on their assigned Roles and Responsibilities.

(f) How information is transmitted to and from the system

National Geodetic Survey General Support System (NOAA6401) collects and stores limited Personally Identifiable Information (PII); specifically, names, telephone numbers, and email addresses (voluntarily submitted by staff, partners, volunteers, and government and non-government collaborators) to facilitate internal and external communications to facilitate business and collaborative functions (e.g. training and webinars). For training and webinars registration necessary to allow coordinating the activity and sharing URLs, only name and email address are required, agency name is optional. This is not a central collection, but rather separated by function or individual project or persons.

NOAA6401 stores information about individuals during the application and hiring (electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase), as well as standard Human Resources (HR) information (such as Travel authorization and vouchers, passports and international travel forms (completed by the employee through the travel portal), information for security badging processes (contact information only – the employee completes the badge application on paper forms, which are taken to the NOAA Office of Security), and performance appraisal ranking. NGS employee data is collected, stored, and maintained for internal COOP, Human Resources, and workforce planning purposes (federal employee/contractor).

NGS collects Business Identifiable Information (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 word processing/spreadsheet documents. There is no application or database used to collect or store BII or PII. NGS does not have a separate HR division and instead relies on the NOAA Office of Human Capital Services. All information is stored on supervisors' and acquisition managers' restricted access file storage available only to the specific employee(s). Access is restricted to those on a need to know basis, by permissions settings and/or passwords. The data is access controlled when on a supervisor's desktop machine or file share; if stored on a supervisor's laptop, the data is encrypted since all mobile devices have full encryption per DOC policy.

Grants Online Application Review (Grants Online) – Information in identifying form is made available by NOAA Grants Online (FISMA system ID, NOAA1101, PIA signed 5/25/2016) to NGS to accomplish Independent Individual Merit Reviews supporting the NOAA Grants Online system Version Number: 01-20153 and process. Information about the NOAA Grants Program (non-public system) may be found at:

http://www.corporateservices.noaa.gov/~grantsonline/index.html.

Information extracted from NOAA Grants Online to support the Independent Individual Merit Reviews is

stored temporarily to facilitate the review process lifecycle. This information can include any general personal information and work related information. Although it is not the intent to extract sensitive PII from the NOAA Grants Online system, it is possible the information could contain the Employer Identification Number (EIN). The EIN is a non-mandatory field, which may be populated on the grants information made available by federal forms not managed by NGS. The NGS General Support System (NOAA6401) does not collect this identifying information directly. Limited use of Microsoft Azure Cloud and Amazon Web Services for storage and distribution of select products.

Aerial imagery from fixed wing aircraft are collected as part of NGS' Aeronautical Survey Program, Coastal Mapping Program, and Emergency Response Imagery with a resolution of approximately 15cm. An Unmanned Aerial System (UAS) collecting imagery with a resolution of ~6 cm are being used for research evaluation associated with the Coastal Mapping Program; and it only operates over public lands, not over private property. In addition, UAS aerial gravity data are collected as part of NGS' GRAV-D program. **None of these data sets are aimed or have the ability to uniquely identify individuals. However, DEPT-29 is referenced in this document.**

(g) Any information sharing conducted by the system

As stated in Sections 5.1 and 6.1, information is shared periodically within the bureau on a case-by-case basis. Additionally, non-sensitive POC information for certain subject matter experts is made available via the NGS web presence. In case of a privacy breach, information will also be shared with the Department and other federal agencies, e.g., Department of Justice (see Section 6.1).

For verification of foreign visitor identity, information may be shared with NOAA Office of Security.

Access to NGS' Norfolk, Virginia, facility is subject to external video surveillance.

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

-5 U.S.C. § 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

-15 U.S.C. § 1512 is an Organic Law which confers general powers and duties authority to executive agencies, vesting jurisdiction and control of departments, bureaus, offices and branches.

Authorities from DEPT-2: 28 U.S.C. 3101-3105, Debt Collection Act of 1982 (Pub. L. 97-365); 26 U.S.C. 6402(d); and 31 U.S.C. 3711.

Authorities from DEPT-6, 5 U.S.C. 301; 44 U.S.C. 3101.

Authorities from DEPT-9: Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966.

Authorities from DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.

Authorities from DEPT-18: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

Authorities from GSA-GOVT-9: For the Entity Management functional area of SAM, the authorities for collecting the information and maintaining the system are the Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204 and 2 CFR, Subtitle A, Chapter I, and Part 25, as well as 40 U.S.C. 121(c). For the exclusions portion of the Performance Information functional area, the authorities are FAR Subparts 9.4 and 28.2, Executive Order 12549 (February 18, 1986), Executive Order 12689 (August 16, 1989).

Authorities from 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.

Authorities from DEPT-29: Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (Feb. 15, 2015); National Marine Sanctuaries Act, 16 U.S.C. 1431 *et seq.*; Marine Debris Act, 33 U.S.C. 1951 *et seq.;* Coast and Geodetic Survey Act, 33 U.S.C. 883a *et seq.*; Coastal Zone Management Act, 16 U.S.C. 1451 *et seq.*; Coral Reef Conservation Act, 16 U.S.C. 6401 *et seq.*; National Historic Preservation Act, 16 U.S.C. 470 *et seq.*; Ocean Pollution Act, 33 U.S.C. 2701 *et seq.*; Comprehensive Environmental Response, Compensation and Liability Act, 42 U.S.C. 9601 *et seq.*; Clean Water Act, 33 U.S.C. 1251; 47 CFR parts 80, 87, and 95. The system is also authorized by the U.S. Office of Management & Budget (OMB) Circular A–130; the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 *et seq.* (Magnuson-Stevens Act); High Seas Fishing Compliance Act of 1995, 16 U.S.C. 5501 *et seq.*; International Fisheries Regulations: Vessels of the United States Fishing in Colombian Treaty Waters: 50 CFR 300.120; the FAA Modernization and Reform Act of 2012 (Pub. L. 112–95); the American Fisheries Act, Title II, Public Law 105–277; the Atlantic Coastal Fisheries Cooperative Management Act of 1993, 16 U.S.C. 5101–5108, as amended 1996; the Tuna Conventions Act of 1950, 16 U.S.C. 951–961; the Atlantic Tunas Convention Authorization Act, 16 U.S.C. Chapter 16A; the Northern Pacific Halibut Act of 1982, 16 U.S.C. 773 *et seq.* (Halibut Act), the Antarctic Marine Living Resources Convention Act of 1984, 16 U.S.C. 2431–2444; the Marine Mammal Protection Act, 16 U.S.C. 1361; and the Debt Collection Improvement Act, 31 U.S.C. 7701.

(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.

☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015).

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

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	
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		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:					

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

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	
c. Work Address	X	g. Work History	X		
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		
k. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		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):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
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	
Telephone		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):					

BII is associated with Pre/Post Acquisition tasks only. Generally, PII is acquired as part of facilities safety and security and administrative tasks; and it is stored only for a temporary period of time in restricted networked drives.

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

Agency Products and Services Data:

All data collected related to producing the Agency's products and services is quality controlled using criteria established for the specific product or service it is destined for, and only distributed

if it meets the Agency's standards. Any contact information that is submitted by the public, e.g. email, telephone, is not validated and will be deleted if invalid. **Acquisition Data:**

All acquisitions are under the purview of the contracting officer. The contracting officer verifies not only all vendor contact information, but also validity of other information submitted by the vendor and may avail themselves of technical experts as needed.

Human Resource (HR) Data: All HR data is verified at the time of collection by the HR representative. This verification may involve verification of identification cards (Driver's License, Passport, etc) and other documents.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	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	X	Electronic purchase transactions	
Other (specify): Video surveillance of ingress/egress points at NGS Norfolk, VA, facility occurs. Warning signs are posted.			

	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	
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): PII concerning name, email address, and agency may be collected to coordinate training and webinars. BII may be collected to determine qualification and/or eligibility for open acquisitions. PII/BII: NOAA Grants Online – Grant Merit Reviews.			

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).

PII

The collection and storage of information is part of accomplishing the legislated mission of NGS, NOS, and NOAA. NOAA6401 stores PII on an ad hoc basis as part of the application and hiring of employees, including electronic copies of resumes, as well as processing of HR data about employees. This information is stored temporarily during the hiring phase, and the security badging process. Standard HR information such as travel authorization and vouchers, (name, work email address and work telephone number), and performance appraisal ranking are stored for a required period of time for auditing purposes generally 6 years.

In addition NGS stores limited PII and potentially an EIN (BII), for grant review only, on an ad hoc basis about individuals or entities that are providing information in support of a grant application submitted through NOAA Grants Online which is retained for the review process lifecycle only.

BII

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

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.)

All information stored within the NOAA6401 system in shared network drives are controlled by defined permissions based on the project and employee access rights. Least privilege is the default policy in NOAA6401 and is implemented through file share permissions and access control lists to ensure privacy and open only to those demonstrating a "need to know." Access to restricted files or folders must be requested through a change request ticket, which is reviewed and documented by the NOAA6401 Information System Security Officer and Information Technology Manager for authorization prior to implementation. Any electronically transmitted PII information must follow the federal government and NOAA standard procedure of secure packaging such as utilization of Department of Commerce (DOC) Kiteworks for encryption in transit.

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			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*In case of privacy breach.

	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.

	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:
X	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			
	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: https://geodesy.noaa.gov/privacy.html .	
X	Yes, notice is provided by other means.	Specify how: Notice is on the applicable 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: By providing data via email or online forms, the individual consents to its use for the purpose of follow-up contact on information provided as described in the NGS privacy policy. When NGS administrative PII is requested, individuals are verbally told by administrative appointed staff or supervisor that they can decline but that it may affect the overall processing of their employment. Privacy statements are embedded in forms. 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. PII provided within NOAA Grants Online, utilized within the Review Application, is managed through the NOAA Grants Online application only. Completion of the Grants Online application is needed for award consideration.
	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: Public submission of PII data associated with a job application is voluntary basis and is only used with regards to this purpose. Employment applications are submitted via OPM and NOAA WFM 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 regards to this purpose. NGS administrative PII may be collected with respect to ongoing business tasks e.g. Travel and is only used for that specific task. 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. BII provided within NOAA Grants Online, utilized within the CSCOR Review Application, is managed through the NOAA Grants Online application only.
	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: The public may contact NGS via email to request to review/update PII/BII as described in the NGS privacy policy. NGS 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.
	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 agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
	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: All logins and access to NOAA6401 IT systems is tracked and recorded. ACL rules control access to folders
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): March 31 2019 ☐ 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).
	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.
	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 stored within the NOAA6401 system in shared network drives is controlled by defined permissions based on the project and employee access rights. Least privilege is the default policy in NOAA6401 and is implemented through file share permissions and access control lists to ensure privacy and open only to those demonstrating a "need to know." Access to restricted files or folders must be requested through a change request ticket which is reviewed and documented by the NOAA6401 Information System Security Officer and Information Technology Manager for authorization prior to implementation. Any electronically transmitted PII information must follow the federal government and NOAA standard procedure of secure packaging such as utilization of Department of Commerce (DOC) Kiteworks for encryption in transit.

NGS/NOAA6401 is categorized as a Moderate IT System using the FIPS-199 standards and implements the associated security controls listed in NIST Special Publication 800-53 Revision 4. To comply with NIST Special Publication 800-53 Revision 4 controls NGS has an IT security program that completes continuous monitoring activities including: security control reviews, vulnerability scanning and patching, review of security access control lists, review of audit logs, handling of access change requests and change control board activities. Risk assessments include the possible threats and vulnerability to the confidentiality, integrity, and availability of mission and sensitive PII/BII data along with associated countermeasures. Every year as part of the

required Assessment and Authorization (A&A) process, an external auditor is hired and evaluates the security plan, the selected security controls of NOAA6401 to ensure that they meet Department of Commerce and NOAA 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)?

☒ 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)*: DEPT-2, Accounts Receivable, DEPT-6, Visitor Logs and Permits for Facilities Under Department Control, DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons, DEPT-13, Investigative and Security Records, DEPT-18, Employees Personnel Files not covered by Notices of Other Agencies, 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. DEPT-29, Unmanned Aviation Systems
	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. Provide the name of the record control schedule: Retention records are indicated in each of the aforementioned SORN's see Section 9 and are further covered under General Records Schedules (GRS) issued by the National Archives and Records Administration (NARA) see https://www.archives.gov/records-mgmt/grs.html All electronic versions of records scheduled for disposal may be deleted at the expiration of the retention period Any administrative PII data, the records would be retained under the following NARA General Records Schedules (GRS): 2.4 Employee Compensation and Benefits Records 2.5 Employee Separation Records 3.1 General Technology Management Records 3.2 Information Systems Security Records 4.1 Records Management Records 4.2 Information Access and Protection Records 5.1 Common Office Records 5.2 Transitory and Intermediary 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	X	Deleting	
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 levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Contact information (email, telephone) could identify an individual.
X	Quantity of PII	Provide explanation: 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 kept for auditing purposes.
X	Data Field Sensitivity	Provide explanation: PII data fields are only used when absolutely necessary and SSN is never filled out. In the NOAA Grants Online EIN number is not required and not used but may be retained temporarily.
X	Context of Use	Provide explanation: PII is only stored for a limited time-period and for a specific purpose.
	Obligation to Protect Confidentiality	Provide explanation:.
X	Access to and Location of PII	Provide explanation: The storage of PII is mostly temporary and is the data is kept only in access control restricted locations and minimizing the number of authorized users. Some Travel documents and Acquisition documents are kept longer in restricted folders for auditing requirements.
	Other:	Provide explanation:

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.)

NGS minimizes both its collection and retention of PII/BII data and does not store any sensitive PII. The limited data that is collected is restricted by policy to be stored in access controlled folders consistent with assigned employee roles and responsibilities. This reduces the risk of privacy related information being stored in other locations. NGS has an assigned employee in charge of Records Management who ensures that reviews and retention times are maintained. In addition all items both paper and electronic that are slated for excess comply with NIST/DOC/NOAA requirements, including, but not limited to shredding, degaussing, wiping, etc.

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.