

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



**Privacy Threshold Analysis
for the
NOAA6401
National Geodetic Survey General Support System**

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/National Geodetic Survey General

Support System

Unique Project Identifier: NOAA6401 (006-48-02-00-01-0511-00)

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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

General Support System

b) *System location*

NGS's primary facility is in the Silver Spring Metro Campus, Silver Spring, MD, with much smaller facilities in: Norfolk Field Office, Norfolk, VA, Testing and Training Center, Woodford, VA, David Skaggs Research Center, Boulder, CO, Table Mountain Field Site and Radio Quiet Zone, Longmont, CO, and, an unstaffed, NOAA Enterprise Data Center, Ashburn, VA. Cloud-based services located in Amazon Web Services and Microsoft Azure.

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
Federal Aviation Administration (FAA) for GPS data (incoming only)

d) The purpose that the system is designed to serve

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. 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 manmade resources and support the economic prosperity and environmental health of the Nation. NGS makes available to the public and other federal, state and local agencies its authoritative spatial data, models and tools. To explain its data, model and tools, the system also stores images, audio/video recordings of webinars, and training. To support NGS’s mission tasks the system also provides administrative support for Human Resource tasks including, but not limited to processing of incoming employees, security badging, performance reviews, and travel documentation. The system also supports acquisition of hardware, software and contract support, along with grant reviews/processing.

e) The way the system operates to achieve the purpose

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.

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

The principal products and services created by NGS involve collection, computation and distribution of: geodetic data (GNSS, terrestrial levelling, gravity etc.) and associated metadata, coordinates of points/benchmarks, imagery of coastlines using a variety of sensors. The geodetic data used to create NGS products and services is primarily collected by NGS employees (federal and contractors), but may also be collected by other federal, state, local agencies, educational institutions, private companies, and the public and given to NGS. In addition, select/adhoc images, audio and video recordings of training/informational webinars, meetings and fieldwork done by NGS employees (federal and contractors) are available for the public to view/download. National Geodetic Survey General Support System (NOAA6401) collects (federal and contractors), 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). This data is not shared with any external group.

NGS federal employees collect 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 by federal employees, stored, and maintained for internal COOP, Human Resources, and workforce planning purposes (federal employee/contractor).

NGS federal employees collect 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' (both categories are federal employees) restricted access file storage available only to the specific federal employee(s).

g) Identify individuals who have access to information on the system

Authenticated Users – Federal and Contractors (On-site) – Access to all data is based on assigned Roles and Responsibilities. Access to PII/BII data is only authorized to Federal Employees based on assigned Roles and Responsibilities.

Supervisors – Federal (On-site) - Access to all data is based on assigned Roles and Responsibilities

IT Services Staff (Administrators) – Federal and Contractors (On-site) - Access to all data is based on assigned Roles and Responsibilities

Developers – Federal and Contractors (On-Site)- Access to specific development, staging, and production data is based on assigned Roles and Responsibilities

Web Visitors – Public – Access to mission data published on public websites

h) How information in the system is retrieved by the user

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

i) How information is transmitted to and from the system

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.

Access to any PII/BII 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 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 4/15/2020) 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 is 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 is 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 is 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.

Select/adhoc images, audio and video recordings of training/informational webinars, meetings and fieldwork are available for the public to view/download.

Outside users can choose to share Global Navigation Satellite System (GNSS) data with NGS to obtain National Spatial Reference System aligned coordinates from their data, and support future improvements to the NSRS.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

- This is a new information system. *Continue to answer questions and complete certification.*
- This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non- Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

- This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*
- This is an existing information system in which changes do not create new privacy

risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017). *Continue to answer questions and complete certification.*

This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

Yes. This is a new information system.

Yes. This is an existing information system for which an amended contract is needed.

No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *(Check all that apply.)*

Activities			
Audio recordings	X	Building entry readers	
Video surveillance	X	Electronic purchase transactions	
Other (specify): NGS collects aerial imagery to support its mission, using both aircraft and sUASs. We have video a surveillance system for physical security purposes at our Norfolk Field Office, Norfolk, VA, with posted signs. In addition, select/adhoc images, audio and video recordings of training/informational webinars, meetings and fieldwork are available for the public to view/download.			

No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the submitter has a commercial interest” and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)”

Yes, the IT system collects, maintains, or disseminates BII.

No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

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

- DOC employees
- Contractors working on behalf of DOC
- Other Federal Government personnel
- Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact

level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the National Geodetic Survey General Support System and as a consequence of this applicability, I will perform and document a PTA for this IT system.

 I certify the criteria implied by the questions above **do not apply** to the National Geodetic Survey General Support System and as a consequence of this non-applicability, a PTA for this IT system is not necessary.

<p>Information System Security Officer or System Owner Name: Giovanni Sella Office: NOAA NGS Phone: 240-533-9479 Email: Giovanni.Sella@noaa.gov</p> <p>I certify that this PTA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u>SELLA.GIOVANNI.FEDERICO.1365835140</u> Digitally signed by SELLA.GIOVANNI.FEDERICO.1365835140 Date: 2021.01.26 08:23:34 -05'00'</p> <p>Date signed: <u>2020-jan-26</u></p>	<p>Information Technology Security Officer Name: John D. Parker Office: NOAA NOS Phone: 240-533-0832 Email: John.D.Parker@noaa.gov</p> <p>I certify that this PTA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u>PARKER.JOHN.D.136583</u> Digitally signed by PARKER.JOHN.D.1365835914 Date: 2021.01.28 10:46:22 -05'00'</p> <p>Date signed: <u>1/28/2021</u></p>
<p>Privacy Act Officer Name: Adrienne Thomas Office: NOAA OCIO Phone: 828-257-3148 Email: Adrienne.Thomas@noaa.gov</p> <p>I certify that the appropriate authorities and SORNs (if applicable) are cited in this PTA.</p> <p>Signature: <u>THOMAS.ADRIENNE.M.1365859600</u> Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2021.02.02 16:48:43 -06'00'</p> <p>Date signed: <u>2/2/21</u></p>	<p>Authorizing Official Name: Juliana Blackwell Office: NOAA NGS Phone: 240-533-9658 Email: Juliana.Blackwell@noaa.gov</p> <p>I certify that this PTA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u>BLACKWELL.JULIANA.P.1043590622</u> Digitally signed by BLACKWELL.JULIANA.P.1043590622 Date: 2021.02.01 16:59:19 -05'00'</p> <p>Date signed: <u>2/1/2021</u></p>
<p>Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary and this PTA ensures compliance with DOC policy to protect privacy.</p> <p>Signature: <u>GRAFF.MARK.HYRUM.151447892</u> Digitally signed by GRAFF.MARK.HYRUM.151447892 Date: 2021.02.03 09:30:35 -05'00'</p> <p>Date signed: <u>2/3/2021</u></p>	