

**U.S. Department of Commerce  
NOAA**



**Privacy Threshold Analysis  
for the  
NOAA1101General Support System (GSS)**

## **U.S. Department of Commerce Privacy Threshold Analysis**

### **NOAA1101 General Support System (GSS)**

**Unique Project Identifier: 006-48-01-01-01-3801-00**

**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:**

The NOAA1101 General Support System (GSS) is an interconnected set of information resources under the management and control of Service Delivery Division (SDD) within the NOAA Office of the Chief Information Officer (CIO).

The NOAA1101 General Support System (GSS) includes facilities, hardware, software, communications, major and minor applications, and people.

NOAA1101 General Support System (GSS) provides Infrastructure As A Service (IAAS), Data Center colocation, and Application Support services that are instrumental to obtaining the objectives of the President's Management Agenda; achieving the goals of the Office of Management and Budget for effective and efficient Government; and NOAA's goal for excellence in the technical operational support of NOAA's financial, management, and administrative systems. Support activities of the GSS include direct, technical, and operational support of financial and administrative systems.

The NOAA1101 General Support System (GSS) boundary encompasses layer 2/layer 3 Cisco Switches, Fortinet Firewalls/IPS, Citrix Netscalers, F-5 Load Balancers, physical and virtual servers running Solaris 11, Red Hat 7 and Windows 2008/2012, Oracle Databases and a number of security devices.

NOAA1101 General Support System (GSS) hosts Two (2) major applications, Commerce Business System (CBS) and Grants Online (GOL) along with a number of minor applications. System descriptions for these applications can be found in Appendix D System Environment Description in CSAM.

**Questionnaire:**

1. 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 later). *Continue to answer questions and complete certification.*

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

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

- Yes. *Please describe the activities which may raise privacy concerns.*
- 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 about: (*Check all that apply.*)

Companies

Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

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

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

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

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

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

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

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

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

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

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

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

## CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the NOAA1101 General Support System (GSS) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

\_\_\_\_\_ I certify the criteria implied by the questions above **do not apply** to the NOAA1101 General Support System (GSS) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

LEEB.STEFAN.ANTON.1158781260 Digitally signed by LEEB.STEFAN.ANTON.1158781260  
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER,  
cn=LEEB.STEFAN.ANTON.1158781260  
Date: 2019.05.23 12:37:17 -04'00'

Stefan Leeb; System Owner

SHORE.JOHN.WILLIAM.1043300675 Digitally signed by SHORE.JOHN.WILLIAM.1043300675  
Date: 2019.05.21 14:30:20 -04'00'

John Shore: Information System Security Officer

OBENSCHAIN.CHARLES.THOMAS.1506347293 Digitally signed by OBENSCHAIN.CHARLES.THOMAS.1506347293  
Date: 2019.06.13 15:15:22 -04'00'

Charles Obenschain: Information Technology Security Officer

PERRY.DOUGLAS.A.1365847270 Digitally signed by PERRY.DOUGLAS.A.1365847270  
Date: 2019.06.14 10:48:14 -04'00'

Doug Perry: Authorizing Official

DARLING.KIMBERLY.A.1398604373 Digitally signed by DARLING.KIMBERLY.A.1398604373  
Date: 2019.07.02 15:21:26 -04'00'

Kim Darling: Co-Authorizing Official

GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892  
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER,  
cn=GRAFF.MARK.HYRUM.1514447892  
Date: 2019.07.18 19:41:10 -04'00'

Mark Graff: Bureau Chief Privacy Officer