Template Version Number: 01-2020

U.S. Department of Commerce

National Telecommunications and Information Administration (NTIA)

Privacy Threshold Analysis
for the

NTIA-005 Headquarters NTIA Network General Support System

U.S. Department of Commerce Privacy Threshold Analysis

NTIA GSS-005

Unique Project Identifier: FISMA NTIA005

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

NTIA005 is a general support system (GSS).

(b) System location

The GSS system location encompasses NTIA headquarters at 1401 Constitution Avenue in Washington, DC (HCHB), a remote field office in Gettysburg, PA (FFO), and a science and research facility located in Boulder CO (ITS).

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

The NTIA GSS system interconnects to the following FedRAMP cloud service providers: Microsoft 365, Microsoft Azure, Salesforce, and DocuSign.

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

The GSS operates to achieve the purpose of providing general support services such as: network services, e-mail services, file sharing, Internet/Intranet connectivity, client-server connectivity, web-enabled applications, and office automation tools to all users in an unclassified environment that ensures confidentiality, integrity, and availability. Additionally, the GSS is utilizing cloud-based systems to enable ubiquitous, on-demand access to configurable computing resources to enhance the user experience at NTIA while maintaining a secure environment.

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

Most users of the GSS work with commercial off the shelf (COTS) software loaded onto their user endpoint devices such as: laptops, desktops, tablets, and cell phones to process business information for administrative purposes and business information purposes in support of NTIA's various missions. As information is newly created and there is a need to share this data with other staff members; users exchange data in various means:

1) Printed Form: Users print the data either to a local printer or to a network printer and physically give the data to other staff members.
2) E-mail: Messages are created and sent to addresses requesting needed information.
3) Digital Collaboration Platforms: Information is exchanged through approved workplace chat, web conferencing, and file storage applications.

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

Information is transmitted and encrypted using FIPS 140-2 validated encryption modules for network communication

(g) Any information sharing conducted by the system

Information sharing is conducted by:

Intranet/Internet:

1) Data is posted on internal web pages, for users to be informed about various topics. Users access the web pages with their web browsers.
2) Data is posted on a public internet site for the purpose of communicating the work of the institute, which is a part of its mission.
3) Data is posted on a secure, restricted internet site for the use of NTIA Government sponsors, a service that is a part of its mission.
4) Data is posted to NTIA-managed SaaS collaboration tools such as M365, SharePoint, Teams, etc.

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

The legal authorities to collect and maintain PII are U.S. Code 1030, Computer Fraud and Abuse Act and Public Law 99-474, Counterfeit Access Device, Computer Fraud and Abuse Act of 1984, Federal Information Security Management Act (FISMA) Section 3544, 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 and Executive Orders 10450, 11478, 12065, 5 U.S.C. 44, 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.

Web servers under the GSS that support NTIA enterprise applications collect and maintain non-sensitive PII, such as usernames, office phone numbers, and office email addresses for application, authentication, and authorization purposes.

The NTIA-005 GSS protects the confidentiality and integrity of organizational sensitive information. NTIA has implemented encryption, using FIPS 140-2 validated encryption modules, on mobile devices and removable media to restrict and protect sensitive data at rest. In addition, other protection mechanisms

are deployed such as security configuration settings, permission restrictions, anti-malware, system logging, and data monitoring tools, consistent and compliant with NIST SP 800-53, applicable DoD STIGs.

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

The FIPS Publication (PUB) 199 security impact category of this system has been assessed as moderate.

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.*

__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 (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.

__X_ 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		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

__X_ 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.)."

_X__ 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."

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

__X_ DOC employees
__X_ Contractors working on behalf of DOC
__X_ 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?

__X_ 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. The collection of SSNs is part of the HR onboarding process; the information in the system is received directly from the subject/requestor, then is forwarded to the DOC's security department where they will perform security checks, requiring verification of the information.
Provide the legal authority which permits the collection of SSNs, including truncated form. U.S. Code 1030, Computer Fraud and Abuse Act and Public Law 99-474, Counterfeit Access Device, Computer Fraud and Abuse Act of 1984, Federal Information Security Management Act (FISMA) Section 3544, 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 and Executive Orders 10450, 11478, 12065, 5 U.S.C. 44, 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.

____ 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?

__X_ 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.

__X_ 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 NTIA005 HQ's NTIA 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 NTIA005 HQ's NTIA GSS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Barton Gibbon Office: DOC/NTIA/OPCM/ITD Phone: 717-549-4555 Email: bgibbon@ntia.gov Signature: BARTON GIBBON Digitally signed by BARTON GIBBON Date: 2021.08.09 17:02:24-04'00' Date signed:	**Information Technology Security Officer** Name: Shine Kang Office: DOC/NTIA/OPCM/ITD Phone: 202-482-1752 Email: skang@ntia.gov Signature: SHINE KANG Digitally signed by SHINE KANG Date: 2021.08.10 17:23:15 -04'00' Date signed:
Privacy Act Officer Name: Dr. Catrina D. Purvis Office: DOC/NTIA/OPCM/ITD Phone: 202-482-3463 Email: cpurvis@ntia.gov Signature: CATRINA PURVIS Digitally signed by CATRINA PURVIS Date: 2021.08.24 18:00:01 -04'00' Date signed:	**Authorizing Official** Name: Dr. Catrina D. Purvis Office: DOC/NTIA/OPCM/ITD Phone: 202-482-3463 Email: cpurvis@ntia.gov Signature: CATRINA PURVIS Digitally signed by CATRINA PURVIS Date: 2021.08.24 18:00:32 -04'00' Date signed:
Bureau Chief Privacy Officer Name: Dr. Catrina D. Purvis Office: DOC/NTIA/OPCM/ITD Phone: 202-482-3463 Email: cpurvis@ntia.gov Signature: SHINE KANG Digitally signed by SHINE KANG Date: 2021.08.10 17:24:51 -04'00' Date signed:	