Template Version Number: 01-2020

U.S. Department of Commerce
National Telecommunications and Information Administration

Privacy Threshold Analysis
for the
NTIA013 Institute for Telecommunication Sciences (ITS)
General Support System (GSS)

U.S. Department of Commerce Privacy Threshold Analysis

NTIA/NTIA013 ITS GSS

Unique Project Identifier: NTIA013

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).

National Telecommunications and Information Administration (NTIA) 013 (NTIA013) is the Institute for Telecommunication Sciences (ITS) general support system (GSS) providing the IT infrastructure to support mission and business processes of ITS telecommunications research and engineering through network services, collaboration services, internet/intranet connectivity, security services, web applications, office automation, and research tools.

a) *Whether it is a general support system, major application, or other type of system*
The NTIA013 ITS GSS is a general support system.

b) *System location*
The ITS GSS is located within the DOC Boulder Laboratories, 325 Broadway, Boulder, CO 80305 with IT infrastructure primarily hosted in the Boulder Computing Facility (BCF).

c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
The ITS GSS has an interconnection through the National Oceanic and Atmospheric Administration (NOAA) Enterprise Network (N-Wave) for internet connectivity and interconnects with the NTIA005 NTIA headquarters (HQ) GSS to provide network connectivity with the other NTIA sites for business and mission purposes.

d) *The purpose that the system is designed to serve*
The purpose of the ITS GSS is to provide the IT infrastructure to support mission processes for ITS telecommunications research and engineering, and business processes including human resources (HR) administration.

e) *The way the system operates to achieve the purpose*
Authorized users access the ITS GSS with commercial off the shelf (COTS) software loaded onto their Windows or macOS workstation to process scientific information for mission purposes, and business information for administrative and HR purposes such as employee onboarding, personnel management, and access to the Table Mountain field site.

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

The ITS GSS collects, maintains, and uses business information including, but not limited to, HR, personnel management, budget, facilities, fleet, IT, and system security information. Mission information includes, but is not limited to, research and development, spectrum, equipment, and radio frequency information.

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

The ITS GSS user base is comprised of NTIA and ITS staff, interns, guest researchers, and contractors. NTIA ITS federal staff and contractors who perform administrative or HR functions with a need to know are authorized for access to personally identifiable information (PII). Select NTIA ITS staff, interns, guest researchers, and contactors access business identifiable information (BII) for mission purposes. Only authorized users have access to the ITS GSS through a system access authorization request (SAAR) process.

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

Information in the ITS GSS is retrieved by users through various means:

- Printed Form: Users print and retrieve data either to a local printer or to a network printer.
- E-mail: Messages are retrieved via an email system hosted by NTIA HQ.
- Digital Collaboration Platforms: Information is exchanged through approved workplace chat, web conferencing, and file storage applications.
- Intranet/Internet:
    - Data is posted on internal web pages, for users to be informed about various topics. Users access the web pages with their web browsers.
    - 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.
    - Data is posted on secure, restricted internet sites for the use of ITS government sponsors, a service that is a part of its mission.
- Network Storage: Data is saved to network drives for retrieval by other users.

Full name is used as a unique personal identifier to retrieve PII on the ITS GSS. Access is granted to a restricted file share storing PII on the ITS GSS file server through a SAAR process and is managed by active directory permissions. The ITS GSS contains no databases or applications which host PII, and simply uses an access controlled flat file structure to securely store HR documentation and forms, and site access requests. Data is retrieved by authorized users through file share access to view or modify the files they have stored.

i) *How information is transmitted to and from the system*

Information in the ITS GSS is transmitted to and from the system through various means:

- 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.
- E-mail: Messages are created and sent via an email system hosted by NTIA HQ.
- Digital Collaboration Platforms: Information is exchanged through approved workplace chat, web conferencing, and file storage applications.

- Intranet/Internet:
  - Data is posted on internal web pages, for users to be informed about various topics. Users access the web pages with their web browsers.
  - 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.
  - Data is posted on secure, restricted internet sites for the use of ITS government sponsors, a service that is a part of its mission.
  - Network Storage: Data is saved to network drives for sharing with other users.

The ITS GSS is categorized as a Federal Information Security Modernization Act (FISMA) moderate system.

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 for the new employee onboarding HR process and the access approval process for the Table Mountain field site.
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 NTIA013 ITS 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 NTIA013 ITS 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: Jacob Neal Office: NTIA/OPCM/ITD Phone: 720-682-6262 Email: jneal@ntia.gov Signature: JACOB NEAL Digitally signed by JACOB NEAL Date: 2021.10.22 15:57:39 -04'00' Date signed: _____	**Information Technology Security Officer** Name: Shine Kang Office: NTIA/OPCM/ITD Phone: 202-482-1752 Email: skang@ntia.gov Signature: SHINE KANG Digitally signed by SHINE KANG Date: 2021.10.22 17:39:42 -04'00' Date signed: _____
Privacy Act Officer Name: Dr. Catrina D. Purvis Office: NTIA/OPCM Phone: 240-672-4974 Email: cpurvis@ntia.gov Signature: CATRINA PURVIS Digitally signed by CATRINA PURVIS Date: 2021.10.26 17:12:19 -04'00' Date signed: _____	**Authorizing Official** Name: Dr. Catrina D. Purvis Office: NTIA/OPCM Phone: 240-672-4974 Email: cpurvis@ntia.gov Signature: CATRINA PURVIS Digitally signed by CATRINA PURVIS Date: 2021.10.26 17:12:42 -04'00' Date signed: _____
Bureau Chief Privacy Officer Name: Dr. Catrina D. Purvis Office: NTIA/OPCM Phone: 240-672-4974 Email: cpurvis@ntia.gov Signature: SHINE KANG Digitally signed by SHINE KANG Date: 2021.10.22 17:41:09 -04'00' Date signed: _____	