Version Number: 01-2017

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

Privacy Threshold Analysis
for the
NTIA-013 ITS GSS

U.S. Department of Commerce Privacy Threshold Analysis

NTIA/NTIA-013 ITS GSS

Unique Project Identifier: NTIA-013

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this information technology (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 Institute for Telecommunication Sciences (ITS) general support system (GSS) is the GSS used by the National Telecommunications & Information Administration (NTIA) to manage daily operations for ITS users. The GSS is located within the operational spaces of ITS which consists of office space on the second and third floors of the DOC Boulder Laboratories at 325 Broadway, Boulder, CO 80305. NTIA-013 has an interconnection through the National Oceanic and Atmospheric Administration (NOAA) Boulder Network Operations Center (BNOC) for internet connectivity. The purpose of NTIA-013 is to support the mission and business processes of ITS telecommunications research and engineering by providing network services, collaboration services, internet/intranet connectivity, linkages to web-enabled applications, and office automation tools to users in an unclassified environment that ensures confidentiality, integrity, and availability. The technical support staff to the GSS is ITS Division D.

Most users of the GSS work with commercial off the shelf (COTS) software loaded onto their Windows or macOS workstation to process business information for administrative purposes and scientific information for mission purposes. As information is newly created, there is a need to share this data with other staff members. Users exchange data in various means:

a) 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.
b) E-mail: Messages are created and sent to addresses requesting needed information.
c) Intranet/Internet:
    i. Data is posted on the internal web pages, including NTIA headquarters intranet pages, for users to be informed about various topics. Users access the web pages with their web browsers.
    ii. 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.
    iii. Data is posted on a secure, restricted internet site for the use of ITS Government sponsors, a service that is a part of its mission.
d) Network Backup: Data is saved to tape backup device and drives for data restoration.

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.*

__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 01-2015 or later). *Skip 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.*

__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 about: *(Check all that apply.)*

__X__ 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..."

__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
____ 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?

__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.

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.

__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, 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 NTIA-013 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 NTIA-013 ITS GSS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Jacob Neal

Signature of ISSO or SO: JACOB NEAL Digitally signed by JACOB NEAL Date: 2018.07.05 14:02:57 -04'00' Date: 7/5/18

Name of Information Technology Security Officer (ITSO): Shine Kang

Signature of ITSO: SHINE KANG Digitally signed by SHINE KANG Date: 2018.08.02 14:24:54 -04'00' Date: 8/2/18

Name of Authorizing Official (AO): J. Stephen Fletcher

Signature of AO: JAMES FLETCHER Digitally signed by JAMES FLETCHER DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=National Telecommunication and Information Administration, cn=JAMES FLETCHER, 0.9.2342.19200300.100.1.1=13001003509495 Date: 2018.08.02 14:36:49 -04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): J. Stephen Fletcher

Signature of BCPO: JAMES FLETCHER Digitally signed by JAMES FLETCHER DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=National Telecommunication and Information Administration, cn=JAMES FLETCHER, 0.9.2342.19200300.100.1.1=13001003509495 Date: 2018.08.02 14:47:55 -04'00' Date: _____