Version Number: 01-2015

U.S. Department of Commerce
National Telecommunication and Information Administration
FirstNet

Privacy Threshold Analysis
for
NTIA-035 FirstNet GSS

U.S. Department of Commerce Privacy Threshold Analysis

NTIA/FirstNet /NTIA-035

Unique Project Identifier: 006-000232600 00-60-03-00-02-00

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 NTIA-035 FirstNet General Support System (GSS) is located within the operational spaces of FirstNet, which consists of data center space in the U.S. Department of Commerce, Herbert C. Hoover Building, 1401 Constitution Avenue, NW, Washington, DC 20230 and in office space at the DOI USGS Building, 12201 Sunrise Valley Dr., Reston, VA 20192 and 3122 Sterling Circle, Boulder, CO 80310.

All controlling communication hardware such as servers and network devices for the GSS are located in areas certified as restricted by the Office of Security within the Department of Commerce, and are part of the NTIA-035 FirstNet GSS. Internet connectivity, DNS functionality, and intrusion detection and incident response are also provided by the Department of Commerce's system, and are outside the boundaries of this system.

The purpose of the General Support System is to provide network services, e-mail services, file sharing, Internet/Intranet connectivity, client-server connectivity, web-enabled applications, and office automation tools to all FirstNet users in an unclassified environment that ensures confidentiality, integrity, and availability. The technical support staff to the GSS is the Information Technology Division (ITD) within FirstNet Office of CIO (OCIO).

Most users of the GSS work with Commercial-Off-The-Shelf (COTS) software loaded onto their Windows workstation. As information is newly created, there is a need to share this data with other staff members. The GSS maintains some photographs of employees and contractors which they voluntarily add onto their email profile. These photographs are displayed when a recipient opens the incoming email. Users exchange data in various means:

PII is maintained in the GSS is in report format from the Department of Commerce Human Resources Operations Center (DOCHHROC) for personnel management reference.

The State Plan Portal is an online electronic system created by AT&T on behalf of FirstNet, maintained outside the FirstNet GSS domain, to deliver each state/territory's particular plan. No PII is contained on that system. FirstNet staff collected information via FirstNet email on the

GSS, for the purpose of providing user credentials for the State Plan Portal to state government employees and their designees. The information collected from state government employees consisted of portal users' full name, title, name of the employing agency, email address and mobile phone number.

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):					

__x__ This is an existing information system in which changes do not create new privacy risks. *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
__x__ 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
__X__ 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 - PTA

__X__I certify the criteria implied by one or more of the questions above **apply** to the NTIA-035 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-035 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)~~: Ronny Chan

Signature of ISSO or SO: RONNY CHAN Digitally signed by RONNY CHAN Date: 2019.03.28 11:36:57 -04'00' Date: _____

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

Signature of ITSO: SHINE KANG Digitally signed by SHINE KANG Date: 2019.04.29 17:06:20 -04'00' Date: _____

Name of Authorizing Official (AO): Jim Gwinn

Signature of AO: JAMES GWINN Digitally signed by JAMES GWINN Date: 2019.03.28 15:53:45 -04'00' Date: _____

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

Signature of Co-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: 2019.04.01 07:47:29 -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: 2019.04.01 07:48:13 -04'00' Date: _____