Version Number: 01-2019

U.S. Department of Commerce
FirstNet Authority

Privacy Threshold Analysis
for the
NTIA-035 FirstNet GSS

U.S. Department of Commerce Privacy Threshold Analysis

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: *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).

The NTIA-035 FirstNet General Support System (GSS) is located within the operational spaces of FirstNet, which consists of office space in the U.S. Department of Commerce, Herbert C. Hoover Building, 1401 Constitution Avenue, NW, Washington, DC 20230 and an office and datacenter space in both the Department of the Interior (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 Department of the Interior and FirstNet as part of the NTIA-035 FirstNet GSS. MTIPS Internet connectivity, DNS functionality, intrusion detection, and incident response are services provided internal to FirstNet by Chief Information Office.

The purpose of the General Support System is to support FirstNet Authority's mission and activities by providing 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 work-related information is newly created, there is a need to share this data with other staff members. Users exchange data in various means including emails, file shares and websites. The GSS maintains photographs of employees and contractors email profile some voluntarily added which they voluntarily add onto their email profile. These photographs are displayed when a recipient opens the incoming email.

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

FirstNet web servers under the GSS that support FirstNet enterprise collect and maintain non-sensitive data, such as user's full name, title, name of employment, email address and phone number. Information will be collected via FirstNet web portal from external stakeholders, partners and other key industry associations who voluntarily elect to provide their contact information or to conduct business and activities to fulfill FirstNet missions. Activities may include, but are not limited to, public advocacy and first responders engagements, awards, speaker sessions or conferences. Data access is restricted to authorized users and shared for authorized business purposes.

GSS users work with COTS cloud-based survey tools, as authorized, to collect non-sensitive data, including general personal and work related PII (i.e., full name and contact information). Information will be collected via web link from government personnel, external stakeholders, partners and other key industry associations who voluntarily elect to provide their contact information or to conduct business activities such as conference registration to fulfill FirstNet's mission. Data access is restricted to authorized users and shared for authorized business purposes. The activities will not create or modify a system of records under the Privacy Act.

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. The system will be transitioned to FirstNet's domain under a new name of FirstNet Central. No PII is contained in the State Plan Portal and/or FirstNet Central system. FirstNet staff collects information via FirstNet email on the GSS, to provide user credentials for the State Plan Portal/FirstNet Central to state government employees and their designees. The information collected from state government employees consists 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):					

____ 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). *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 01-2017 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. *(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
____ National Institute of Standards and Technology Associates
__x__ Contractors working on behalf of DOC
____ Other Federal Government personnel
__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 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. FirstNet maintains human resources (HR) reports received through DOC HROC which include Social Security Number (SSN) and employee ID numbers. Passport number is collected for foreign personnel visit request as well as pre-PIV authorization.
Provide the legal authority which permits the collection of SSNs, including truncated form. 5 U.S.C. 301; 44 U.S.C. 3101; 47 U.S.C. § 1442(e), E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5370; 5 CFR Part 537; DAO 202-957; EO. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; E.O. 12564; Public Law 100-71, dated July 11, 1987 and E.O. 10450, E.O. 11478, E.O.12065, 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 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 FirstNet NTIA-035 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 [IT SYSTEM NAME] 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: 2020.04.29 11:40:48 -04'00' Date: _____

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

Signature of ITSO: SHINE KANG Digitally signed by SHINE KANG Date: 2020.05.08 18:10:38 -04'00' Date: _____

Name of Privacy Act Officer (PAO): J. Stephen Fletcher

Signature of PAO: Stephen Fletcher Digitally signed by Stephen Fletcher Date: 2020.05.11 12:02:51 -04'00' Date: _____

Name of Authorizing Official (AO): Jim Gwinn

Signature of AO: JAMES GWINN Digitally signed by JAMES GWINN Date: 2020.04.30 09:42:11 -04'00' Date: _____

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

Signature of Co-AO: Stephen Fletcher Digitally signed by Stephen Fletcher Date: 2020.05.11 12:03:29 -04'00' Date: _____

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

Signature of BCPO: Stephen Fletcher Digitally signed by Stephen Fletcher Date: 2020.05.11 12:04:07 -04'00' Date: _____