

**U.S. Department of Commerce  
FirstNet Authority**



**Privacy Threshold Analysis  
for the  
NTIA-035 FirstNet  
Authority GSS**

## U.S. Department of Commerce Privacy Threshold Analysis FirstNet

### Authority / 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 away 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*

The NTIA-035 FirstNet Authority is a General Support System.

b) *System location*

The NTIA-035 FirstNet Authority 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 (HCHB), 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. The FirstNet Authority GSS leverages FedRAMP Cloud storage solutions.

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

The NTIA-035 FirstNet Authority General Support System (GSS) interconnects with DOC HCHB for personnel management references.

d) *The purpose that the system is designed to serve*

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 Authority users in an unclassified environment that ensures confidentiality, integrity, and availability.

The portion that concerns with privacy are listed below:

- PII information from DOC Human Capital Client Services
- State Plan Portal / FirstNet Central on non-sensitive PII collection.
- FirstNet web portal within the GSS on non-sensitive PII collection.
- 3<sup>rd</sup> party software survey tools on non-sensitive PII collection.

e) *The way the system operates to achieve the purpose*

Per organizational procedure, PII data is maintained in the GSS in report format from the Department of Commerce Human Capital Client Services for personnel management reference.

The State Plan Portal is an online electronic system created and managed by AT&T on behalf of FirstNet Authority, maintained outside of the FirstNet Authority GSS domain, to deliver each state/territory's particular plan. No sensitive PII/BII is contained in the State Plan Portal and/or FirstNet Central system which is used to manage authorization and access to the State Plan Portal.

FirstNet Authority web servers under the GSS that support FirstNet Authority 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 Authority 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 Authority 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 Authority missions. 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.

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

Except for PII data in report format for the Department of Commerce Human Capital Client Services for personnel management reference, FirstNet Authority enterprise collects and maintain non-sensitive data, such as user's full name, title, name of employment, email address, and phone number.

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

FirstNet Authority Human Resources have access to the PII data for personnel management. Other data access is restricted to FirstNet authorized users and shared for authorized business purposes.

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

PII data for personnel management is obtained through the DOC Human Capital Client Services web portal from GSS is collected in internal database and can be retrieved in spreadsheet format. State Plan Portal/FirstNet Central data is collected in spreadsheet attachment sent via FirstNet Authority email.

COTS cloud-based survey tools, as authorized, are collected via web link and consolidated as reports in spreadsheet format.

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

Information is exchanged through secure, encrypted connections whether connecting through the web interface, email (including Kiteworks), and file repositories.

**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.*
- 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.
- 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.)

<b>Activities</b>			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

\_\_\_ 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.)."

\_\_\_ 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."

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

- \_\_\_ DOC employees
- \_\_\_ Contractors working on behalf of DOC
- \_\_\_ 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?

\_\_\_\_\_ 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.
Provide the legal authority which permits the collection of SSNs, including truncated form.

\_\_\_\_\_ 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?

\_\_\_\_\_ 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.

\_\_\_\_\_ 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 NTIA035-FirstNet Authority 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-035 FirstNet Authority GSS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

<p><b>(Acting) Chief Information Security Officer or System Owner</b>  Name:Saady Abd-Elfattaqh  Office: FirstNet Authority  Phone:571-665-6090  Email: saady.abd-elfattah@firstnet.gov</p> <p>Signature: <u>SAAD-ALDIN ABD-ELFATTAH</u>  <small>Digitally signed by SAAD-ALDIN ABD-ELFATTAH  Date: 2021.08.26 12:05:20 -04'00'</small></p> <p>Date signed: _____</p>	<p><b>Information Technology Security Officer</b>   Name: Shine Kang  Office: NTIA  Phone: 202-482-1752  Email: skang@ntia.gov</p> <p>Signature: <u>SHINE KANG</u>  <small>Digitally signed by SHINE KANG  Date: 2021.08.30 08:34:39 -04'00'</small></p> <p>Date signed: _____</p>
<p><b>Bureau Chief Privacy Officer and Privacy Act Officer</b>  Name: Catrina Purvis Office: NTIA  Phone: 202-482-6245  Email: cpurvis@ntia.gov</p> <p>Signature: <u>CATRINA PURVIS</u>  <small>Digitally signed by CATRINA PURVIS  Date: 2021.08.31 14:10:14 -04'00'</small></p> <p>Date signed: _____</p>	<p><b>Authorizing Official</b>  Name:Jim Gwinn  Office: FirstNet Authority  Phone: 571-665-6201  Email: jim.gwinn@firstnet.gov</p> <p>Signature: <u>JAMES GWINN</u>  <small>Digitally signed by JAMES GWINN  Date: 2021.08.26 12:26:38 -04'00'</small></p> <p>Date signed: _____</p>
<p><b>Co-Authorizing Official</b>  Name: Catrina Purvis  Office: NTIA  Phone: 202-482-6245  Email: cpurvis@ntia.gov</p> <p>Signature: <u>CATRINA PURVIS</u>  <small>Digitally signed by CATRINA PURVIS  Date: 2021.08.31 14:10:43 -04'00'</small></p> <p>Date signed: _____</p>	