Template Version Number: 01-2020

U.S. Department of Commerce
FirstNet Authority

Privacy Impact Assessment
for the
NTIA035 FirstNet Authority GSS

Reviewed by: Catrina Purvis, Bureau Chief Privacy Officer

[X] Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
[ ] Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 09/08/2021

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment FirstNet Authority/NTIA035

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

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system
The NTIA035 FirstNet Authority is a General Support System.

(b) System location
The NTIA035 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 way the system operates to achieve the purpose(s) identified in Section 4
Per organizational procedure, Personal Identifiable Information (PII) is maintained in the GSS in report format from the Department of Commerce Human Capital Client Services for personnel management reference. Human resource personnel access the HR Connect system through a web portal over the DOC HCHB MPLS (Multiprotocol Layer Switching) circuit.

The State Plan Portal is an online electronic system created 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 or business identifiable information (BII) is contained in the State Plan Portal and/or FirstNet Central system (AT&T account management system).

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 responder's 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.

(e) *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 and can be retrieved in spreadsheet. Data is retrieved using name as a unique identifier. Data is retrieved without sensitive PII.

Contact information is collected and managed by AT&T through AT&T FirstNet Central Portal for authorization and access to the State Planning portal.

COTS cloud-based survey tools, as authorized, collect non-PII/BII information via web link and consolidated as a report. Generally, the reports contain anonymized information.

(f) *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.

(g) *Any information sharing conducted by the system*

Information is collected and shared with other Agencies for personnel management purposes with Human Resources and investigation purposes.

AT&T manages accounts and access for the State Plan Portal to state government employees and their designees. No PII/BII is collected nor maintained.

Information collected via FirstNet Authority web portal and survey tools from external stakeholders, partners, and other key industry associations who voluntarily elect to provide their bureau information are used to conduct business and activities to fulfill FirstNet Authority missions. No PII/BII is collected nor maintained.

(h) *The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*

The legal authorities to maintain PII are 18 U.S.C 1030, Computer Fraud and Abuse Act; 44 U.S.C. 3554, Federal Information Security Management Act of 2002; 47 U.S.C. 1442(e), Middle Class Tax Relief and Job Creation Act of 2002 (State Network); 47 U.S.C. 1426; 5 U.S.C. 301; 44 U.S.C. 3101; Executive Order (E.O.) 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; Departmental Administrative Order (DAO) 202-957; E.O. 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, DAO 210-1, DAO 207-12; 5 U.S.C. 7531, 7532; 15 U.S.C. 1501 et. Seq.; 28 U.S.C. 533, 534, 535; Equal Employment Act of 1972; Section 208 of the E-government Act of 2002.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The Federal Information Processing Standards (FIPS) 199 Security impact category of this system is Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.

_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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.

____ 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).

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).

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport	X	k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: First Net Authority maintains human resources (HR) reports received from DOC HROC which include Social Security Number (SSN) and employee ID numbers. HR receives SSN as a part of onboarding or legal requests. Passport Number is collected for foreign personnel visit request as well as pre-PIV authorization.					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	

b. Maiden Name		i. Place of Birth	X	p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	X
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity		m. Education	X	t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address	X	g. Work History	X	k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs	X	j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	f. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email	X		
Other (specify): Accellion for encryption transfer. FirstNet Authority Onboarding requires for In Person as well as Hard Copy as sources; and data is stored encrypted in FirstNet Authority domain. Authorized FirstNet Authority personnel collects non-sensitive information via FirstNet Authority web portal 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 is collected from those such as government personnel, external stakeholders, partners, and other key industry associations who elect voluntarily to provide their contact information. Authorized FirstNet Authority personnel collects non-sensitive information via web link through COTS cloud-based survey tools directly from survey respondents, such as government personnel, external stakeholders, partners, and other key industry associations who elect voluntarily to provide their contact information.					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal	X	Foreign	X		
Other (specify): For State Plan Portal Access and/or FirstNet Central: Each State's Single Point of Contact (SPOC) provided FirstNet Authority with a list of individuals that are authorized to access the portal to review the Plan for the state or territory. The information collected to provide user access is submitted to FirstNet Authority in a Microsoft Excel spreadsheet by email which is secured within the FirstNet Authority domain.					

Non-government Sources					
Public Organizations	X	Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): Public Organizations comprised of State, Local, and Tribal government staff may bring contact information into FirstNet Authority domain.					

2.3 Describe how the accuracy of the information in the system is ensured.

For HR related information, accuracy of the data is a shared responsibility of authorized users which include FirstNet Authority HR specialists. Likewise, for the state plan portal, information is input and maintained by authorized users. For non-sensitive information collected on a voluntary basis as part of authorized business activities such as conference registration, FirstNet Authority relies on the information provided by the individuals/entities directly.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act. Exempt: see 47 U.S.C. 1426(d)(1).

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

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

X	There is not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): As required by statue for management of Grants programs. For State Plan Portal and/or FirstNet Central: FirstNet Authority provided the spreadsheet received from the SPOCs to AT&T by email which was used to create portal access credentials for the individuals identified as authorized reviewers for each state. This information was not used for any other purpose. Authorized FirstNet Authority personnel collect non-sensitive information via FirstNet Authority web portal 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. Authorized FirstNet Authority personnel collect non-sensitive information via web link through COTS cloud-based survey tools directly from survey respondents to fulfill FirstNet Authority Missions through research and other authorized business activities such as conferences or speaker sessions.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

For administering human resources programs: Information in Section 2.1 is used for personnel management of FirstNet Authority employees. Sensitive PII is used to assist with the HR process for personnel actions such as hiring, promotion, retirement, and employee in/out processing.

Business Processes/Operations: Sensitive PII may be used for travel processes, visitor access, etc. WRD and DFB are provided voluntarily by contractors and employees and used in their e-mail profile. SAAD, admin or service account ID of employees or contractors and system log or audit data, is used to support system access and network/system administration purposes.

Information from non-federal employees and contractors, such as state, local, and tribal sources, is used for the purposes of providing user credentials for FirstNet's State Plans Portal.

Non-sensitive information from non-federal employees, contractors, such as state, local, and tribal sources, industry stakeholders, partners, or other key industry associations and/or foreign nationals is used to conduct official business activities. Activities include, but are not limited to first responders' engagements, awards, speaker sessions, conferences, or surveys to fulfill FirstNet Authority missions.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed

appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

FirstNet Authority prevents any potential threats to privacy, such as insider threat, by leveraging our Microsoft Data Loss Prevention, Advanced Threat Protection modules in our environment. In addition, FirstNet Authority also requires our users to complete an annual Cybersecurity Awareness Training as well as review and sign the IT Rules of Behavior. Data Access is also restricted to authorized FirstNet Authority personnel users with a "need to know."

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
x	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	x
Contractors			
Other (specify): Authorized FirstNet Authority staff (HR/Finance federal employee) have access to general personal and work related PII (i.e., full name and contact information) to conduct business and activities to fulfill FirstNet Authority missions.			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
x	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: A Privacy Policy for FirstNet's publicly available website can be found at (https://www.firstnet.gov). In addition, an email notification is sent to confirm receipt of submission. However, FirstNet Authority is exempt from the Privacy Act Under 47 U.S.C. 1426(d)(2). COTs web tools implement their own Privacy Act statement and/or privacy policy, which can be found at the web link of each individual COTs tool. A webform notification would be shown after submission. Portal users are provided "State Plan Portal Terms of Use" when they login to the website at https://state-territory.firstnet.att.com/privacy-policy/. Users must agree to the terms of use before gaining access to the portal._____.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

x	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: For the PII data collected by DOC Human Capital Client Services, individuals may decline to provide PII by providing a written request to their servicing HR Specialist in DOC Human Capital Client Services. FirstNet Authority GSS and COTs tools web links are optional form of non-sensitive data collection.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: For the PII data collected by DOC Human Capital Client Services, written consent to only particular uses of PII must be submitted to the servicing HR specialist in DOC Human Capital Client Services. However, failure to consent to all uses may affect their employment status. For other information, employees, contractors, and other associates (to include non-employee students, guest researchers, etc.) sign an IT Rules of Behavior that specifies that data they choose to provide in FirstNet systems are non-private. Written notice is provided at FirstNet GSS and COTs tools web links to inform user how non-sensitive information would be used.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

x	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: For the PII data collected by DOC Human Capital Client Services, PII is routinely updated as an employee's position changes by the servicing HR specialist in DOC Human Capital Client Services. Individuals may use Employee Personal Page (EPP) to review and update their information throughout employment. After survey participants submit their non-sensitive information through FirstNet Authority GSS and COTS tools web links, FirstNet Authority personnel may verify, or participants may resubmit their data in some instances. Otherwise, data will be as current as the last date of contact with the survey participant.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

x	All users signed a confidentiality agreement or non-disclosure agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to the PII/BII is restricted to authorized personnel only.
x	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: The FirstNet Authority General Support System has implemented Data Loss Prevention (DLP) for monitoring, tracking, and recording of PII/BII.

x	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide dateof most recent Assessment and Authorization (A&A): **09/08/2020** ☐ This is a new system. The A&A datewill be provided when the A&A package is approved.
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place andfunctioning asintended; or haveanapproved Plan of Action and Milestones (POA&M).

x	A security assessment report has been reviewedfor the information system and it hasbeendetermined that therea re no additionalprivacyrisks.
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
x	Contractswith customers establish DOC ownershiprights over data including PII/BII.
x	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable)*

- Access Control: access provisioning, access/privileged accounts monitoring
- Security baseline configuration
- Passive vulnerability scans
- O365 Data Loss Prevention: Monitor and block PII/BII data transfer
- Encryption on hard drives, mobile devices and USB drives
- Secure file sharing (Acellion) - Malicious attack identification and analysis
- Block and filter network traffic and malicious websites
- Phishing/Spear-Phishing attack training

-The GSS uses Personal Identity Verification (PIV) card for system access authentication, but does not collect or maintain the biometric data in the system.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

x Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*:
	Yes, a SORN has been submitted to the Department for approval on (date).
x	No, this system is not a system of records and a SORN is not applicable. FirstNet Authority is exempt from the Privacy Act pursuant to 47 U.S.C. 1426(d)(2).

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

	There is an approved record control schedule. Provide the name of the record control schedule:
x	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule: FirstNet Authority is currently following the General Records Schedule (GRS) for the disposition of records. A record schedule was submitted by FirstNet Authority for approval with NARA in November 2018. The record schedule is currently with an Appraiser from NARA under review. Until FirstNet Authority receives approval, no unique agency program records, if not duplicated elsewhere, will be deleted from the system.
x	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	x	Overwriting	x
Degaussing	x	Deleting	x
Other (specify): Records are destroyed in accordance with the General Records Schedule in the manner indicated above, as appropriate. Records pending NARA approval are not currently destroyed.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
x	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.*

x	Identifiability	Provide explanation: The information directly identifies a small number of individuals using SSN.
x	Quantity of PII	Provide explanation: Sensitive PII data related to HR reports is minimal.

x	Data Field Sensitivity	Provide explanation: Sensitive PII data is in the GSS.
	Context of Use	Provide explanation:
x	Obligation to Protect Confidentiality	Provide explanation: The protection of sensitive PII that the GSS maintains is governed by the E-Government Act of 2002.
x	Access to and Location of PII	Provide explanation: The PII in HR reports is stored in a designated data storage with limited access to managers and staff with HR responsibilities.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

FirstNet Authority follows the rules and regulations from Section 208 of the E-Government Act of 2002 and Department of Commerce policy when identifying and evaluating any potential threats to privacy. FirstNet maintains human resources (HR) reports received through DOC HROC which include Social Security Number (SSN) and employee ID numbers. Passport numbers are collected for foreign personnel who request to visit as well as for pre-PIV authorization. Non-sensitive personal and work related PII (i.e., full name and contact information) are voluntarily collected to conduct FirstNet Authority missions. Data access is restricted to authorized FirstNet Authority personnel and shared for authorized business purposes only.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.