Template Version Number: 01-2022

U.S. Department of Commerce
FirstNet Authority

Privacy Impact Assessment
for the
NTIA035 FirstNet Authority General Support System (FNA GSS)

Reviewed by: JEROME NASH Digitally signed by JEROME NASH Date: 2025.09.03 13:03:50 -04'00', Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

BRIAN ANDERSON Digitally signed by BRIAN ANDERSON Date: 2025.09.04 10:24:35 -04'00'

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

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

Unique Project Identifier: 2487

Introduction: System Description

Provide a brief description of the information system.

NTIA035 FirstNet Authority is a General Support System (GSS) architecture which houses a hybrid of on-premises servers and cloud-based systems hosted by third-party vendors. The FirstNet Authority's framework spans multiple servers, and the physical environment is owned by the bureau, and located in the United States. Third-party vendors and cloud service providers (CSPs) are Federal Risk and Authorization Management Program (FedRAMP) authorized. CSPs are responsible for maintenance and accessibility of cloud service offerings which transmit and store user, organization, and application data.

The FirstNet Authority GSS consists of on-premises and cloud-based IT systems supporting the bureau's mission to provide an infrastructure for productivity of FirstNet Authority personnel who support the public-private AT&T partnership. The current FirstNet Authority enterprise catalog includes Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) offerings with an expanding scope of services planned for future deployment.

The FirstNet Authority cloud services host information systems for its customers that may collect, maintain, and disseminate Personally Identifiable Information (PII)/Business Identifiable Information (BII). Access to the data assets containing PII/BII by applications is documented in relevant system-level Privacy Impact Assessments that are evaluated against the GSS with relevant security controls and applicability and is not available to CSPs. Access to the data assets containing PII/BII is specifically identified and restricted to those with need-to-know. For example, FirstNet Authority Human Resources (HR) access human resource systems for personnel onboarding, maintenance including personnel updates and clearance information, and pay. These assets and connections are available only to specified HR staff.

Address the following elements:

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

(b) System location
Local Area Network, Wide Area Network and wireless network services are provided at FirstNet Authority headquarters in Reston, Virginia as well as its regional offices in Boulder, Colorado, and Washington, DC.
FirstNet Authority assets are hosted in the Microsoft Azure cloud environment.

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

FNA-GSS interconnects with Department of Commerce Herbert C. Hoover Building (DOC HCHB) data center to streamline operations, improve collaboration, and for IT management providing FirstNet Authority employee consistent access to applications and resources in addition to leveraging DOC HCHB for Internet via the Trusted Internet Connection Access Provider (TICAP). Cloud Services connect with/receive/maintains data from FirstNet Authority's IT systems that are hosted on IaaS and PaaS cloud service offerings. Additionally, FirstNet Authority connects to Human Resource (HR) systems via dedicated connections or via connection to HCHB from a specified access control list (ACL) on FirstNet Authority firewalls. ACLs explicitly define who can access the resources, and accessible systems are accessed by specific users via username and password or multifactor authentication. Additionally, some cloud service offerings may have collateral PII, such as:

i. Microsoft Azure Government (IaaS)
ii. Accellion USA, LLC (SaaS)
iii. DocuSign (SaaS)
iv. ServiceNow (PaaS)
v. Microsoft (Office 365 Multi-tenant & Supporting Services) (SaaS)

(d) *The way the system operates to achieve the purpose(s) identified in Section 4*

FirstNet Authority is comprised of networked servers and storage systems, both owned on-premises and by-subscription cloud, designed to meet individual FirstNet Authority mission objectives. Servers are accessible via local area network, or via General Services Administration’s (GSA) Managed Trusted Internet Protocol Service (MTIPS) to transmit, process, and/or store user, organization, and application data. The technology or components in this system span multiple servers, and the physical environment is owned and managed by third-party FedRAMP authorized vendors at offsite facilities located in the United States. These third-party providers are responsible for keeping data/information available and accessible, and the physical environment protected and running.

FirstNet Authority primarily employs three service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)

The following are contained within the service models offered and are authorized to operate within the FirstNet Authority Boundary:

i. Microsoft Azure Government (IaaS/PaaS/SaaS)
ii. Microsoft Azure Commercial Cloud (IaaS/PaaS/SaaS)
iii. Accellion USA, LLC (SaaS)
iv. ArcGIS Online (AGO) (PaaS/SaaS)
v. Box, Inc. (SaaS)
vi. Cloudflare (SaaS)

vii. Cornerstone OnDemand (SaaS)
viii. Diligent, Inc. (SaaS)
ix. DocuSign (SaaS)
x. Granicus (SaaS)
xi. Keeper Security (SaaS)
xii. Microsoft (Office 365 Multi-tenant & Supporting Services) (SaaS)
xiii. Okta Identity as a Service (IDaaS) (SaaS)
xiv. OneStream Software (SaaS) (SaaS)
xv. Palantir Technologies Inc. (SaaS)
xvi. Palo Alto Networks, Inc. (SaaS)
xvii. Qualtrics (SaaS)
xviii. Sentinel Labs, Inc. (SaaS)
xix. ServiceNow (SaaS)
xx. Smartsheet (SaaS)
xxi. Splunk (SaaS)
xxii. Tenable Public Sector (TPS) (SaaS)
xxiii. VBrick Systems, Inc. (SaaS)
xxiv. Zimperium (SaaS)
xxv. Zscaler, Inc. (SaaS)

Microsoft Azure Commercial Cloud – Azure provides FirstNet Authority with a high impact level platform as a service which facilitates application and service management. FirstNet Authority personnel do not manage or control the Azure Cloud environment but use its services in the form of operating systems and storage. Both Microsoft environments have Microsoft Defender configured for data loss prevention, with policies preventing transmission of sensitive information including PII.

Microsoft Office 365 – MSO365 provides FirstNet Authority with collaboration and productivity applications and services. FirstNet Authority personnel access MSO365 for day-to-day productivity, including SharePoint collaboration services, and Office file creation and management. Both Microsoft environments have Microsoft Defender configured for data loss prevention, with policies preventing transmission of sensitive information including PII.

Accellion Kiteworks – Kiteworks, a web-based system and not interconnected, allows FirstNet Authority personnel to share sensitive information that requires encryption. Users access Kiteworks through Okta Identity Management System.

Onboarding – Initially, FirstNet Authority onboards new employees via YRCI HR contract through DOC. FirstNet Authority HR personnel do not process PII. YRCI HR contractors onboard new employees via USA Staffing. USA Staffing personnel records feed into U.S

Department of the Treasury's HRConnect. HRConnect ultimately feeds into various other HR systems to which FirstNet Authority HR personnel access for personnel maintenance.

After onboarding, all employee actions are completed by FirstNet Authority personnel via DOC's Enterprise Services (ES) (myService Hub/Talent Management). Authorized HR personnel submit employee actions via ES tickets. HRConnect feeds into eOPF.

U.S. Department of the Treasury (USDT) HRConnect – FirstNet Authority accesses HRConnect via web. Only authorized HR personnel are granted access. HR personnel must be connected to the FirstNet Authority network to access HRConnect. HR personnel access employee information in HRConnect via employee name.

eOPF – FirstNet Authority employee information is populated to Office of Personnel Management's eOPF via HRConnect. HR personnel can query eOPF by employee name or social security number. Once an employee's record is made available, social security number (SSN) is obfuscated.

GSA USAccess – FirstNet Authority accesses this resource primarily through web-based access but processes individual personal identity verification (PIV) assignments via a dedicated router with one-way outgoing traffic from FirstNet Authority to GSA USAccess. Only authorized security personnel are granted access.

U.S. Department of Agriculture (USDA) National Finance Center (NFC) – FirstNet Authority accesses this resource via dedicated terminal emulator (TN3270+) through DOC and by ACLs. Only authorized HR personnel are granted access. HR personnel access financial information and can generate reports through NFC (via TN3270+, or Data Insight). Reports are redacted of personally identifiable information and saved to an access-restricted, Federal Information Processing Standard (FIPS) 140-2 encrypted, and impact level 4 (IL4) SharePoint site. These reports serve as alpha rosters or a complete employee list with necessary information to validate personnel actions.

Department of Commerce (DOC) GovTA – GovTA is provided by DOC for FirstNet Authority time keeping purposes. All federal employees have access to their own time and attendance, and supervisors and timekeepers can access records based on assignment. All access is gained by username and password and is web-based. GovTA information and records feed into the NFC.

(e) How information in the system is retrieved by the user

FirstNet Authority Human Resources (HR) staff access Office of Personnel Management (OPM) Department of Commerce (DOC), US Department of Agriculture (USDA), and Treasury Department information systems to conduct HR actions. FirstNet Authority uses its information systems and web servers (e.g., ServiceNow Information Technology Service

Management (ITSM), and SharePoint) within the GSS to support FirstNet Authority collection and maintenance of non-sensitive data, such as user's full name, title, name of employment, email address and phone number. FirstNet Authority also employs DocuSign to facilitate document signing for items such as telework agreements, that list home addresses, etc.. All applications are only accessible to authorized and designated users and have been granted authorizations at the Moderate or High level by FedRAMP. Data collected may be 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. These activities do not create or modify a system of records under the Privacy Act.

(f) How information is transmitted to and from the system

Information is transmitted to and from IaaS, PaaS, and SaaS cloud services only for authorized and lawful government purposes by employing secure communications (virtual private connections, dedicated terminal emulation, Trusted Internet Connection (TIC), and hypertext transfer protocol security (HTTPS).

(g) Any information sharing

Employee data is not collected through the FirstNet Authority GSS, but through DOC HR contractors who initiate onboarding via USA Staffing and then managed by FirstNet Authority HR personnel through myService Hub/Talent Management and HRConnect, which are web-based systems described d. above. Additional data collected may be 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. These activities do not create or modify a system of records under the Privacy Act.

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

It has been determined that the FirstNet Authority General Support System (GSS) is not a system of records. As a result, information systems containing PII/BII that are hosted on the FirstNet Authority GSS are governed by the system of records notices(s) (SORN(s)) specific to the record types stored within the information system and must be used in accordance with the purpose(s) enumerated in the SORN. The legal authorities for each information system, containing PII/BII hosted on the FirstNet Authority GSS, can be located in its respective SORN. SORN(s) for information systems hosted on the FirstNet Authority GSS are referenced in their applicable system-level PIA.

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

NTIA035 – FNA GSS Security Categorization (Information System Impact) is **Moderate**. The high-watermark impact rating of the FNA GSS (NTIA035) for each security objective is

as follows: Confidentiality = Moderate, Integrity = Moderate, and Availability = 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.
X 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): There is no previously approved PIA on file. Previously submitted PTA/PIA have expired. Listed all CSOs, and changed authorities to reflect 47 USC1426(d)(2). No additional changes creating privacy risks.					

____ 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.

____ This is an existing information system that is eligible for an annual certification, in which security and privacy controls are properly implemented, changes do not create new privacy risks and there is a SAOP approved Privacy Impact Assessment.

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	X
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: FirstNet Authority maintains human resources (HR) reports received from appropriate HR servicing systems, which include social security numbers (SSN), and employee ID numbers. HR receives SSNs as part of onboarding or legal requests. Passport number is collected for foreign personnel visit requests as well as pre-PIV authorization.					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	
b. Maiden Name	X	i. Place of Birth	X	p. Medical Information	
c. Alias	X	j. Home Address	X	q. Military Service	X
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Marital Status	
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	
g. Citizenship	X	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	X
c. Work Address	X	g. Work History	X	k. Procurement/contracting records	X
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	X	f. Scars, Marks, Tattoos		k. Signatures	X
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording	X	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):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal	X	Foreign	X		
Other (specify):					

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 brig contact information into FirstNet					

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. 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. 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	X	Building entry readers	X
Video surveillance		Electronic purchase transactions	
Other (specify): All users are granted opportunity to not participate in recorded sessions. Explicit consent for participating in recorded sessions are presented prior to start of recording.			
	There are 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):			

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.. Data may be provided voluntarily by contractors and employees and used in their e-mail profile. System Authorization Access Requests (SAAR), admin or service account identification 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 Authority GSS. 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 (DLP), Advanced Threat Protection modules in our environment.
In addition, FirstNet Authority also requires our users to complete the annual Cybersecurity Awareness Training (CSAT), 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" basis. FNA GSS provides secure, role-based access and use encryption to protect data.

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.

X	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: FNA-GSS interconnects with Department of Commerce Herbert C. Hoover Building data center to streamline operations, improve collaboration, and for IT management providing FirstNet Authority employee consistent access to applications and resources in addition to leveraging DOC HCHB for Internet via the Trusted Internet Connection Access Provider (TICAP). Cloud Services connect with/receive/maintains data from FirstNet Authority's IT systems that are hosted on IaaS and PaaS cloud service offerings. Additionally, FirstNet Authority connects to Human Resource (HR) systems via dedicated connections or via connection to HCHB from a specified access control list (ACL) on FirstNet Authority firewalls. ACLs explicitly define who can access the resources, and accessible systems are accessed by specific users via username and password or multifactor authentication. FirstNet Authority employs data loss prevention tools, configured with policies for preventing data exfiltration, including PCI and PII data. Users cannot copy and paste data included in DLP policies. CSOs in use which may contain collateral PII. i.Microsoft Azure Government (IaaS)ii.Accellion USA, LLC (SaaS)iii.DocuSign (SaaS)iv.ServiceNow (PaaS)v.Microsoft (Office 365 Multi-tenant & Supporting Services) (SaaS)
	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	X		
Other (specify): Authorized FirstNet Authority staff (HR federal employees and cleared contractors) have access to 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: _https://firstnet.gov/privacy-policy_____.	
	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: Individuals may decline to provide PII by providing a written request to their servicing HR specialist.
	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: Individuals are notified that failure to consent may affect 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 commercial off the shelf (COTS) tools web links to inform users 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: 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: FNA-GSS employs multiple data loss prevention tools, including Microsoft Defender for Cloud, Microsoft Purview, Endpoint DLP, etc.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): _6 March 2025_____ ☐ This is a new system. The A&A date will 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 **5** Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks. No POA&Ms for the system.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish DOC ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
X	Other (specify): FNA-GSS employs multiple data loss prevention tools, including Microsoft Defender for Cloud, Microsoft Purview, Endpoint DLP, etc.

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
- Microsoft Office (O365) & Zscaler Data Loss Prevention: Monitor and block PII/BII data transfer
- Encryption on hard drives, mobile devices and universal serial bus (USB) drives
- Secure file sharing (Accellion Kiteworks) - 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)?

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

_X__ 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.

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.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: National Archives Office of the Chief Records Officer: The General Records Schedules Transmittal 35; FirstNet Authority NARA Re
	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:
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 a 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: 250 billets; ~230 personnel listed on alpha. Sensitive PII data related to HR reports is minimal. Alpha rosters are obtained from HR systems, redacted, and saved
X	Data Field Sensitivity	Provide explanation: Sensitive PII data is in the GSS. Controlled Unclassified Information (CUI) marking
	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.
