

**U.S. Department of Commerce
National Telecommunications and Information
Administration (NTIA)**



**Privacy Impact Assessment
for
NTIA-035 FirstNet
General Support System**

Reviewed by: J. Stephen Fletcher, 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

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
Date: 2019.08.15 17:51:17 -04'00'

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

Date

U.S. Department of Commerce Privacy Impact Assessment National Telecommunications and Information Administration

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

Introduction: System Description

The NTIA-035 FirstNet General Support System (GSS) is located within the operational spaces of FirstNet, which consists of data center space in the U.S. Department of Commerce, Herbert C. Hoover Building, 1401 Constitution Avenue, NW, Washington, DC 20230 and in office space at the 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 Office of Security within the Department of Commerce, and are part of the NTIA-035 FirstNet GSS. Internet connectivity, DNS functionality, and intrusion detection and incident response are also provided by the Department of Commerce's system, and are outside the boundaries of this system.

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

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

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

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

The legal authorities to maintain PII are 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; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987 and Executive Orders 10450, 11478, 12065, 5

U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. Seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.

FirstNet GSS protects the confidentiality and integrity of organizational sensitive information at rest. Several protection mechanisms are deployed, such as security baseline configurations, permissions restrictions, Anti-virus, and system logs and vulnerability scanning.

The legal authorities to collect and maintain PII are U.S. Code 1030, Computer Fraud and Abuse Act and Public Law 99-474, Counterfeit Access Device, Computer Fraud and Abuse Act of 1984, FISMA Section 3544, U.S.C 301 and 44, and U.S.C. 3101.

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	x
j. Other changes that create new privacy risks (specify): Initial PIA					

☒ This is an existing information system in which changes do not create new privacy risks

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	e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport	x	k. Financial Transaction	
d. Employee ID	x	h. Alien Registration		l. Vehicle Identifier	
* Explanation for the need to collect, maintain, or disseminate the Social Security number, 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.					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth	x	m. Religion	
b. Maiden Name		h. Place of Birth	x	n. Financial Information	
c. Alias		i. Home Address	x	o. Medical Information	

d. Gender		j. Telephone Number	x	p. Military Service	x
e. Age		k. Email Address	x	q. Physical Characteristics	
f. Race/Ethnicity		l. Education	x	r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	x	d. Telephone Number	x	g. Salary	x
b. Job Title	x	e. Email Address	x	h. Work History	
c. Work Address	x	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs	x	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. 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	d. 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	
Telephone		Email	x		
Other (specify): Accellion for encryption transfer. FirstNet Onboarding requires for In Person as well as Hard Copy as sources and data is stored encrypted in our FirstNet domain.					

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: Each State's Single Point of Contact (SPOC) provided FirstNet 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 in a Microsoft Excel spreadsheet by email which is secured within the FirstNet domain.					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 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	x	Biometrics	
Caller-ID	x	Personal Identity Verification (PIV) Cards	x
Other (specify): O365			

	All cipher suites supported by Office 365 use algorithms acceptable under FIPS 140-2.
--	---

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 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			
To determine eligibility		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 statute for management of Grants programs. For State Plan Portal: FirstNet 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.			

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: General Personal Data (GPD) and identifying numbers in Section 2.1 are used for personnel management of FirstNet employees and contractors. Sensitive PII is used to assist with the HR process for personnel actions such as hiring, promotion, retirement, and employee in/out processing.
- System Admin/Audit Data information, 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 collected 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.

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			x
Public			
Private sector			x
Foreign governments			
Foreign entities	x		
Other (specify): FirstNet provides the information submitted by SPOCs to AT&T for providing user credentials for the state portal.		x	

	The PII/BII in the system will not be shared. Foreign entities are handled case-by-case basis when personnel requests visit to FirstNet's offices.
--	--

6.2 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.
x	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 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):		

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.)*

x	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: _FirstNet website http://www.firstnet.gov Portal users are provided "State Plan Portal Terms of Use" when they login to the website at http://state-territory.firstnet.att.com/ . 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 DOCHROC, individuals may decline to provide PII by providing a written request to their servicing HR specialist in DOCHROC.
	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 DOCHROC, written consent to only particular uses of PII must be submitted to the servicing HR specialist in DOCHROC. However, failure to consent to all uses may affect their employment status.
	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 DOCHROC, PII is routinely updated as an employee's position changes by the servicing HR specialist in DOCHROC. Employees may request to review their information from and ask that it be updated through their supervisors. Updates are made by the servicing HR specialist or HRConnect manager.
	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: Access is restricted only for employees and contractors with a “need to know” and can be tracked and recorded by the system logs.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>9/11/2018</u> <input type="checkbox"/> 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 4 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 (POAM).
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 ownership rights 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.

- 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
- 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 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.”

x	<p>Yes, this system is covered by an existing System of Records Notice (SORN). Provide the SORN name and number (<i>list all that apply</i>):</p> <p>COMMERCE/Dept-1, Attendance, leave, payroll records COMMERCE/Dept-18, Employees Personnel Files Not Covered by Notices of Other Agencies OPM/GOVT – 1 General Personnel Records OPM/GOVT – 2 Employee Performance File System Records OPM/GOVT – 3 Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers OPM/GOVT – 5 Recruiting, Examining and Placement Records OPM/GOVT – 6 Personnel Research and Test Validation Records</p>
---	--

	OPM/GOVT – 7 Applicant Race, Sex, National Origin, and Disability Status Records. OPM/GOVT – 9 File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals, and Fair Labor Standard Act (FLSA) Claims and Complaints
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

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: NTIA Record Schedule, N1-417-10-1, approved by NARA on May 20, 2011.
	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: Under development
x	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation: Record control schedule is under development.

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):			

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

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.

	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 levels. *(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 Privacy Act of 1974.
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: No sensitive PII on state portal users is collected.

Section 12: Analysis

12.1 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.

12.2 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.