Template Version Number: 01-2020

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

Privacy Impact Assessment
for the
NTIA013 Institute for Telecommunication Sciences (ITS) General Support System (GSS)

Reviewed by: Dr. Catrina Purvis, 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

Jennifer Goode 10/14/2021

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

U.S. Department of Commerce Privacy Impact Assessment
NTIA/NTIA013 ITS GSS

Unique Project Identifier: NTIA013

Introduction: System Description

National Telecommunications and Information Administration (NTIA) 013 (NTIA013) is the Institute for Telecommunication Sciences (ITS) general support system (GSS) providing the information technology (IT) infrastructure to support mission and business processes of ITS telecommunications research and engineering through network services, collaboration services, internet/intranet connectivity, security services, web applications, office automation, and research tools. The technical support staff to the GSS is the NTIA ITS GSS IT team.

(a) *Whether it is a general support system, major application, or other type of system*
The NTIA013 ITS GSS is a general support system.

(b) *System location*
The ITS GSS is located within the DOC Boulder Laboratories, 325 Broadway, Boulder, CO 80305 with IT infrastructure primarily hosted in the Boulder Computing Facility (BCF).

(c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
The ITS GSS has an interconnection through the National Oceanic and Atmospheric Administration (NOAA) Enterprise Network (N-Wave) for internet connectivity and interconnects with the NTIA005 NTIA headquarters (HQ) GSS to provide network connectivity with the other NTIA sites for business and mission purposes.

(d) *The way the system operates to achieve the purpose(s) identified in Section 4*
Authorized users access the ITS GSS with commercial off the shelf (COTS) software loaded onto their Windows or macOS workstation to process business information for administrative and human resources (HR) purposes such as employee onboarding, personnel management, and access to the Table Mountain field site.

Documentation is collected which contains personally identifiable information (PII) to support HR, personnel administration, and access to the Table Mountain field site. Table Mountain access requests and HR information is collected from individuals and any documentation containing sensitive PII is stored on an access-controlled file share limited to staff with a need to know, with auditing and malware scanning in place. Table Mountain access requests are submitted by the requestor through the approved and encrypted DOC solution, kiteworks by Accellion, then forwarded through kiteworks to the Seattle DOC security office for approval.

Per organizational procedure, PII is retained and used for business purposes only and is minimized as much as possible, with Table Mountain access requests deleted after the approval process and HR onboarding documentation containing PII deleted after receipt of the information from the DOC HR Operations Center (HROC), ensuring that all requirements for it have been met.

Users are directed to report any incidents involving PII immediately, and any sensitive PII located outside of the authorized file share is securely deleted through data sanitization. Users are instructed to not complete fields on standard forms which contain PII that are not necessary for processing.

Web servers under the GSS that support NTIA enterprise applications maintain non-sensitive PII, such as usernames, office phone numbers, and office email addresses for application and authentication purposes.

The NTIA013 ITS GSS protects the confidentiality and integrity of organizational sensitive information. NTIA has implemented encryption on mobile devices and removable media to restrict and protect sensitive data at rest. In addition, other protection mechanisms are deployed such as security configuration settings, permission restrictions, anti-malware, system logging, and data monitoring tools.

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

General information in the ITS GSS is retrieved by users through various means:

- Printed Form: Users print and retrieve data either to a local printer or to a network printer.
- E-mail: Messages are retrieved via an email system hosted by NTIA HQ.
- Digital Collaboration Platforms: Information is exchanged through approved workplace chat, web conferencing, and file storage applications.
- Intranet/Internet:
    - Data is posted on internal web pages, for users to be informed about various topics. Users access the web pages with their web browsers.
    - Data is posted on a public internet site for the purpose of communicating the work of the institute, which is a part of its mission.
    - Data is posted on secure, restricted internet sites for the use of ITS government sponsors, a service that is a part of its mission.
- Network Storage: Data is saved to network drives for retrieval by users internally.

The GSS maintains information access to government agency enterprise service providers' web sites such as United States Department of the Treasury HRConnect and United States Department of Agriculture (USDA) National Finance Center (NFC) in support of HR and business functions.

Documentation containing sensitive PII is only transmitted to the Seattle DOC security office and the DOC HROC through the approved and encrypted DOC solution, kiteworks by Accellion. Sensitive PII is not electronically transmitted using any other method.

The ITS GSS user base is comprised of NTIA and ITS staff, interns, guest researchers, and contractors. NTIA ITS federal staff and contractors who perform administrative or HR functions with a need to know are authorized for access to PII. Select NTIA ITS staff, interns, guest researchers, and contactors access business identifiable information (BII) for mission purposes. Only authorized users have access to the ITS GSS through a system access authorization request (SAAR) process.

Full name is used as a unique personal identifier to retrieve PII on the ITS GSS. Access is granted to the restricted file share storing PII on the ITS GSS file server through the SAAR process and is managed by active directory permissions. The ITS GSS contains no databases or applications which host PII, and simply uses an access controlled flat file structure to securely store HR documentation and forms, and site access requests. Data is retrieved by authorized users through file share access to view or modify the files they have stored.

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

General information in the ITS GSS is transmitted to and from the system through various means:

- Printed Form: Users print the data either to a local printer or to a network printer and physically give the data to other staff members.
- E-mail: Messages are created and sent via an email system hosted by NTIA HQ.
- Digital Collaboration Platforms: Information is exchanged through approved workplace chat, web conferencing, and file storage applications.
- Intranet/Internet:
  - Data is posted on internal web pages, for users to be informed about various topics. Users access the web pages with their web browsers.
  - Data is posted on a public internet site for the purpose of communicating the work of the institute, which is a part of its mission.
  - Data is posted on secure, restricted internet sites for the use of ITS government sponsors, a service that is a part of its mission.
- Network Storage: Data is saved to network drives for sharing with users internally.

Documentation containing sensitive PII is only transmitted to the Seattle DOC security office and the DOC HROC through the approved and encrypted DOC solution, kiteworks by Accellion. Sensitive PII is not electronically transmitted using any other method.

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

Documentation containing sensitive PII is only transmitted to the Seattle DOC security office and the DOC HROC through the approved and encrypted DOC solution, kiteworks by Accellion. The ITS GSS does not host or maintain any system capabilities for information sharing of PII.

(h) *The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*
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, Federal Information Security Management Act (FISMA) Section 3544, 5 U.S.C. 301; 44 U.S.C 3101; E.O. 12107, E.O. 13164, 41 U.S.C 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, July 11, 1987 and Executive Orders 10450, 11478, 12065, 5 U.S.C. 44, 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.

(i) *The Federal Information Processing Standards (FIPS) 199 security impact category for the system*
The FIPS 199 security impact category of the ITS GSS 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	X	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		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: Required for processing HR actions and the access approval process for the Table Mountain field site.					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X
b. Maiden Name	X	i. Place of Birth	X	p. Medical Information	X
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. Physical Characteristics	
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	
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	
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	
Telephone	X	Email	X		
Other (specify):					

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

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

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

As part of HR onboarding and Table Mountain access request processes, the information in the system is received directly from the subject/requestor, then is forwarded to the security department where they will perform security checks, requiring verification of the information.

PII is stored within a centralized file server that is encrypted with FIPS 140-2 cryptography to protect the integrity and confidentiality of the information. The ITS GSS does not contain any applications or databases that collect or process PII, information is only stored within files.

Information not part of the HR onboarding process and Table Mountain access request process is obtained by other FISMA Major Applications (MAs) where the information is received directly from the subject. This information is limited to the information on a SAAR form (i.e., name, email address, phone number, and affiliation) and is not processed by the NTIA013 ITS GSS, but only resides on it.

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.

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 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 HR programs: GPD and IN in section 2.1 are used for personnel management of NTIA ITS 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. PII is used in the security clearance process to determine if employees are eligible to handle NTIA sensitive materials.

- For administrative matters: PII may be used for travel processes, transit subsidy program, acquisition processes, etc.

- IN, GPD, and WRD for human resource management related purposes such as, hiring process, personnel management actions, government business travel, background check/security clearance, visit requests, access requests to the Table Mountain field site, etc.

- System administration/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.

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.)

Potential threats to the privacy of subjects from whom ITS collects PII could be an insider threat who intentionally leaks PII or a breach of the multiple levels of security controls that would allow a bad-actor to obtain the stored PII.

The ITS GSS has security controls and procedures in place that provide guidance and restrictions for the collection, storage, sharing, transmitting, faxing, printing, destruction of PII, and the reporting of security incidents involving PII.

Handling PII is restricted to ITS Division Chiefs, administrative personnel, and any other staff who are responsible for using it as part of official ITS business and mission processes.

All NTIA ITS users must complete annual cyber security awareness training which includes sensitive information handling guidance.

Sensitive PII must be stored in a specific file share which has restricted access and security measures in place.

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	N/A	N/A	Yes
DOC bureaus	Yes	N/A	N/A
Federal agencies	N/A	N/A	N/A
State, local, tribal gov't agencies	N/A	N/A	N/A
Public	N/A	N/A	N/A
Private sector	N/A	N/A	N/A
Foreign governments	N/A	N/A	N/A
Foreign entities	N/A	N/A	N/A
Other (specify):	N/A	N/A	N/A

	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: A system interconnection is maintained with the NTIA005 Headquarters NTIA Network for connectivity with the other NTIA sites for business and mission purposes. NTIA ITS administrative staff connect to the National Finance Center, Office of Personnel Management (OPM) e-QIP and eOPF, HRConnect, webTA, and CWTSatoTravel portals. All access to these enterprise services is managed and approved by other Government agencies that are under the same FISMA compliance. Access to the secure websites is restricted by permissions and systems under the GSS are all covered with the technical controls described in section 8.2 in this PIA.
	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):			

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: the NTIA public website https://www.ntia.gov.	
	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: This is done by the DOC HROC hiring process and the Table Mountain access request process. Individuals may decline to provide PII information on the application or HR hiring documents but if required information is not provided, the job application could be declined. On access request forms for the Table Mountain field site, requestors can decline to provide PII information, but if required information is not provided, access to the site could be declined.
	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: This is done by the DOC HROC hiring process for the sensitive PII, written consent to only particular uses of PII must be submitted to the servicing HR specialist in DOC HROC. For non-sensitive PII, individuals are given an explanation as to why the required information is needed on the system access request form and in the instructions. They consent by signing the form. Declining may affect eligibilities or services. Consent is received from individuals for the use of photographs through Form I-9, Employment Eligibility Verification, as required by the Immigration Reform and Control Act of 1986.
	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 HROC, PII is routinely updated as an employee's position changes by the servicing HR specialist in DOC HROC. 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 the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 10/15/2021 ☐ 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 (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.
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.
	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 account monitoring - Security configuration - Vulnerability scanning and remediation - Anti-malware, anti-spyware, and spam protection - Encryption on mobile devices and external drives - Secure file sharing - Malicious attack identification and blocking - Block and filter network traffic and malicious websites - The ITS GSS uses PIV cards for multifactor system access authentication, but does not collect or maintain the biometric data in the system

<u>Section 9</u>: 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."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/DEPT-1, Attendance, Leave, Payroll Records of Employees and Certain Other Persons COMMERCE/DEPT-5, Freedom of Information Act and Privacy Act Request Records COMMERCE/DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons COMMERCE/DEPT-10, Executive Correspondence Files COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies COMMERCE/DEPT-22, Small Purchase Records 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 OPM/GOVT-7 Applicant Race, Sex, National Origin, and Disability Status Records OPM/GOVT-10: Employee Medical File System Records
	Yes, a SORN has been submitted to the Department for approval on (date).
	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: 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:
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):			

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: Documentation contains unique identifiers such as SSNs that could directly identify individuals.
X	Quantity of PII	Provide explanation: The number of affected records is sufficiently low to reduce risk.
	Data Field Sensitivity	Provide explanation:
X	Context of Use	Provide explanation: PII collected is for human resources and personnel administration use only and is stored in access controlled central locations.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Documentation containing sensitive PII is stored in centralized access-controlled locations and is limited to only personnel with a need to know.
	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.)

The very minimal type and quantity of PII included on the access request form for access to the Table Mountain field site is provided by the requestor. It is only transmitted via the DOC approved and encrypted kiteworks by Accellion. Table Mountain access requests reside on the GSS for the minimum length of time possible. For the onboarding HR process, only the minimum type and quantity of PII required is obtained from the onboarding individual and resides on the GSS for the minimum length of time possible. Other PII that resides on the GSS is acquired by other FISMA MAs to comply with their access control requirements, and only resides on the GSS for the minimum amount of time required for use of the FISMA MA that acquired it and by law. The only threats to the privacy of the subjects for whom the PII was collected is a potential insider threat that could intentionally leak the information or a breach of the many security layers and controls allowing access to the stored PII. Neither of the potential threats to the privacy of the subjects is likely.

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.