Template Version Number: 01-2020

U.S. Department of Commerce

National Telecommunications and Information Administration (NTIA)

Privacy Impact Assessment
for the

NTIA-005 Headquarters NTIA Network General Support System

Reviewed by: Dr. Catrina D. 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 08/24/2021

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

U.S. Department of Commerce Privacy Impact Assessment
NTIA GSS-005

Unique Project Identifier: FISMA NTIA005

Introduction: System Description

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

(a) Whether it is a general support system, major application, or other type of system

NTIA005 is a general support system (GSS).

(b) System location

The GSS system location encompasses NTIA headquarters at 1401 Constitution Avenue in Washington, DC (HCHB), a remote field office in Gettysburg, PA (FFO), and a science and research facility located in Boulder CO (ITS).

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

The NTIA GSS system interconnects to the following FedRAMP cloud service providers: Microsoft 365, Microsoft Azure, Salesforce, and DocuSign.

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

The GSS operates to achieve the purpose of providing general support services such as: network services, e-mail services, file sharing, Internet/Intranet connectivity, client-server connectivity, web-enabled applications, and office automation tools to all users in an unclassified environment that ensures confidentiality, integrity, and availability. Additionally, the GSS is utilizing cloud-based systems to enable ubiquitous, on-demand access to configurable computing resources to enhance the user experience at NTIA while maintaining a secure environment.

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

Most users of the GSS work with commercial off the shelf (COTS) software loaded onto their user endpoint devices such as: laptops, desktops, tablets, and cell phones to process business information for administrative purposes and business information purposes in support of NTIA's various missions. As information is newly created and there is a need to share this data with other staff members; users exchange data in various means:

1) 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.
2) E-mail: Messages are created and sent to addresses requesting needed information.
3) Digital Collaboration Platforms: Information is exchanged through approved workplace chat, web conferencing, and file storage applications.

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

Information is transmitted and encrypted using FIPS 140-2 validated encryption modules for network communication

(g) Any information sharing conducted by the system

Information sharing is conducted by:

Intranet/Internet:

1) Data is posted on internal web pages, for users to be informed about various topics. Users access the web pages with their web browsers.
2) 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.
3) Data is posted on a secure, restricted internet site for the use of NTIA Government sponsors, a service that is a part of its mission.
4) Data is posted to NTIA-managed SaaS collaboration tools such as M365, SharePoint, Teams, etc.

(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, dated 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.

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

The NTIA-005 GSS protects the confidentiality and integrity of organizational sensitive information. NTIA has implemented encryption, using FIPS 140-2 validated encryption modules, 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, consistent and compliant with NIST SP 800-53, applicable DoD STIGs.

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

The FIPS Publication (PUB) 199 security impact category of this system has been assessed as 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.

__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 01-2015 or 01-2017).
____ 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	
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:					

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

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

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

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

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

Other Information (specify)

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

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	
Telephone		Email	x		
Other (specify): The non-sensitive PII (name, email address, phone number) are only collected thru email to NTIA Helpdesk on the SAAR (System Authorization Access Request).					

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 the HR onboarding, the information in the system is received directly from the subject/requestor, then is forwarded to the DOC's security department where they will perform security checks, requiring verification of the information.

The information stored in the HR systems is validated by DOC personnel and the employee; additionally, wherever possible, pre-formatted fields are used to ensure information accuracy.

Information not part of the HR onboarding process is obtained by other FISMA Major Applications (MAs) where the information is received directly from the subject, is limited to the information on a System Access Authorization Request (SAAR) form (i.e., name, email).

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: General personal data (GPD) and identifying numbers (IN) in section 2.1 are used for personnel management of NTIA 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: NTIA has removed sensitive PII (e.g., SSN) from the forms and processes for travel, transit subsidy program, acquisition, etc.
- IN, GPD, and work-related data (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 field sites, 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 NTIA 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 NTIA005 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 NTIA Division Chiefs, administrative personnel, and any other staff who are responsible for using it as part of official NTIA business and mission processes.
Privacy Training – NTIA has identified PII handling staff members and trained on PII protection (NTIA prepared training materials). NTIA managers with security roles have competed Privacy Act Training from OPOG. All ITD members are trained on Privacy multiple times at the ITD Monthly Power meetings.
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	NA	NA	Yes
DOC bureaus	NA	NA	NA
Federal agencies	NA	NA	NA
State, local, tribal gov't agencies	NA	NA	NA
Public	NA	NA	NA
Private sector	NA	NA	NA
Foreign governments	NA	NA	NA
Foreign entities	NA	NA	NA
Other (specify):	NA	NA	NA

	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.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	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: NTIA does not have a direct connection to other IT systems that contains PII; however, it has a web portal/application access (only who authorized with an account) to OPM HR system, DOC Enterprise Services, National Finance Center, etc. The security control responsibilities are on the system/application owners, and NTIA staff is just viewing and processing PII info, not be able to download.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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

Class of Users			
General Public		Government Employees	x
Contractors			
Other (specify):			

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: All NTIA public websites	
	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 NTIA access request form. Individuals may decline to provide PII information on the application or HR hiring documents but if required information is not provided, job application 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 HR Connect 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 with a "need to know" and can be tracked and recorded by system logs. DLP monitors the PII/BII misuse.
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): **08/26/2020** ☐ 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 accounts monitoring - Security baseline configuration - Data loss prevention (DLP) - Vulnerability and Baseline scans - Anti-Virus, Anti-spyware/malware/spam - Encryption on mobile devices and USB drives - Secure file sharing - Monitor and block PII data in transit or at rest - Malicious attack identification and analysis - Block and filter network traffic and malicious websites - Phishing/Spear-Phishing attack training - The NTIA005 GSS uses Personal Identity Verification (PIV) card for system access authentication, but does not collect or maintain the biometric data in the system

Section 9: Privacy Act

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

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

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

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

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

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. COMMERCE/DEPT-5, FOIA requests. COMMERCE/DEPT-9, Travel records. COMMERCE/DEPT-10, Executive Correspondence Files. COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Noticed 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. 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 (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 follows NARA Records Schedules updated in June 2020 at: https://www.archives.gov/files/about/records-schedule/nara-recordsschedule-list.pdf and specific General Records Schedule (GRS) at: https://www.archives.gov/records-mgmt/grs.html
	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.)

NTIA005 does not collect or maintain sensitive PII data directly but stores PII that is pulled out from other bureaus system/sources – e.g., NFC, Security Manager, DOC HR for Personnel management and Administration purposes. NTIA HR restricts the access to the PII file/folder
to only 'need to know' staff, and the files are under the capability of encryption of DAR (Data at Rest). During last several years NTIA has eliminated collecting SSN for Transit Subsidy and removed/marked as 'Leave Blank' the PII fields on Travel request and Training request forms. NTIA has trained staff members who have OSY Security Manager (PII) access and managers handle personnel info. NTIA has implemented Data Loss Prevention (DLP). 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.