

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



**Privacy Impact Assessment
for
NTIA-013 NTIA ITS
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: 2019.08.14 17:04:22 -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: NTIA-013

Introduction: System Description

The National Telecommunications and Information Administration 013 (NTIA-013) general support system (GSS) is located in Boulder Labs, Building 1-3430, 325 Broadway, Boulder, CO. The NTIA site in Gettysburg is designated as the emergency relocation site in case of disaster or emergency.

The purpose of the GSS is to provide network services, collaboration services, internet/intranet connectivity, web-enabled applications, and office automation tools to users in an unclassified environment that ensures confidentiality, integrity, and availability. The technical support staff to the GSS is the Institute for Telecommunication Sciences (ITS) information technology (IT) team, henceforth in this document referred to as the GSS support staff.

Most users of the GSS work with commercial off the shelf (COTS) software loaded onto their Windows or macOS workstation. As information is newly created, there is a need to share this data with other staff members. Users exchange data in various means:

- Printed form
- Email
- Websites
- File shares

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

Documentation is collected which contains personally identifiable information (PII) to support HR and personnel administration. HR information is collected in person 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. Per organizational procedure, PII is retained and used for business purposes only and is minimized as much as possible, with HR onboarding documentation containing PII deleted after receipt of information from the DOC HR Operations Center (HROC) and ensuring that all requirements for it have been met. Documentation containing sensitive PII is only transmitted through the approved and encrypted DOC solution kiteworks by Accellion. 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 is not necessary for processing.

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 user names, office phone numbers, and office email addresses for application and authentication purposes.

The NTIA-013 GSS protects the confidentiality and integrity of organizational sensitive information. NTIA ITS 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-virus, system logging, and data monitoring tools.

The Federal Information Processing Standards (FIPS) Publication (PUB) 199 security impact category of this system is moderate.

Section 1: Status of the Information System

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

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

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify):			

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

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	x	j. Financial Account	x
c. Employer ID		g. Passport	x	k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify): The GSS collects as part of personnel actions and stores on an access controlled file share limited to staff with a need to know, with system auditing and malware scanning in place. Documentation is transmitted through DOC secure file transfer to DOC HROC for processing. HR on-boarding documentation containing PII is removed from the ITS GSS immediately after being sent to DOC and ensuring that all requirements for it have been met.					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: Required for processing HR actions.					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth	x	m. Religion	
b. Maiden Name	x	h. Place of Birth	x	n. Financial Information	x
c. Alias	x	i. Home Address	x	o. Medical Information	x
d. Gender	x	j. Telephone Number	x	p. Military Service	x
e. Age	x	k. Email Address	x	q. Physical Characteristics	
f. Race/Ethnicity	x	l. Education	x	r. Mother's Maiden Name	
s. Other general personal data (specify): The GSS collects as part of personnel actions and stores on an access controlled file share limited to staff with a need to know, with system auditing and malware scanning in place. Documentation is transmitted through DOC secure file transfer to DOC HROC for processing. HR on-boarding documentation containing PII is removed from the ITS GSS immediately after being sent to DOC and ensuring that all requirements for it have been met.					

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	x
c. Work Address	x	f. Business Associates			
i. Other work-related data (specify): The GSS collects as part of personnel actions and stores on an access controlled file share limited to staff with a need to know, with system auditing and malware scanning in place. Documentation is transmitted through DOC secure file transfer to DOC HROC for processing. HR on-boarding documentation containing PII is removed from the ITS GSS immediately after being sent to DOC and ensuring that all requirements for it have been met.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	x	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): 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.					

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	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 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		x		Personal Identity Verification (PIV) Cards	x
Other (specify):					

	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			
To determine eligibility	x	For administering human resources programs	x
For administrative matters	x	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): As required by statue for management of Grants programs.			

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 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 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, 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.

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			
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 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: National Finance Center, Office of Personnel Management (OPM / E-QIP and eOPF), HR Connect, webTA, and Carlson Wagonlit Travel/SATO Travel. All access to these enterprise services are managed and approved by other Government agencies that are under the same FISMA compliance. Access to the secure websites are 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.

6.3 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			
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. 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.
	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 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>8/27/2018</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 FIPS PUB 199 security impact category for this system is a moderate or higher.
x	National Institute for Standards and Technology (NIST) Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 security and privacy 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.

<ul style="list-style-type: none"> - Access Control: access provisioning, access/privileged account monitoring - Security configuration - Vulnerability scans - Anti-malware, anti-spyware, and spam protection - Encryption on mobile devices and USB drives - Secure file sharing - Malicious attack identification and blocking - Block and filter network traffic and malicious websites - The GSS uses PIV cards 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	Yes, this system is covered by an existing System of Records Notice (SORN). Provide the SORN name and number (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. 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-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, 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:
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 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: 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 an access controlled central location.
	Obligation to Protect Confidentiality	Provide explanation:
x	Access to and Location of PII	Provide explanation: Documentation containing sensitive PII is stored in a centralized access controlled file share and is limited to only personnel with a need to know.
	Other:	Provide explanation:

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.