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

Privacy Impact Assessment
for
NTIA-005 Headquarters NTIA Network General Support System

Reviewed by: J. Stephen Fletcher, NTIA 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
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.08.29 12:01:14 -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: 006-60-02-00-02-7313-00

Introduction: System Description

The General Support System (GSS) is located within the operational spaces of NTIA, which consists of office space in the U.S. Department of Commerce (DOC), Herbert C. Hoover Building, 1401 Constitution Avenue, NW, Washington, DC 20230 and in office space at the Federal Communications Commission (FCC) offices in Gettysburg, PA. The site located in Gettysburg is designated as the Emergency Relocation Site (ERS) in case of disaster or emergency.

All controlling communication hardware such as servers, workstations, and network printers for the GSS are located in areas certified as restricted by the Office of Security within the Department of Commerce, and is part of the Department of Commerce's NTIA Headquarter Network, NTIA-005. Internet connectivity, Domain Name Server (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 GSS 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 users (federal employees and contractors) in an unclassified environment that ensures confidentiality, integrity, and availability. The technical support staff to the GSS is the Information Technology Division (ITD) within the NTIA, Office of Policy, Coordination, and Management (OPCM). The ITD support staff and primarily the Information Technology Operations Branch support staff are referenced, henceforth in this document, as the GSS support staff.

The users of the GSS work with the NTIA CIO approved Commercial-Off-The-Shelf (COTS) software loaded onto their Windows workstation. As work related information is created and there is a need to share this data with other staff members in the NTIA, users exchange data in various means; data exchange network shares, emails, and websites. The GSS maintains some photographs of employees and contractors which they voluntarily add onto their email profile with consent in compliance with the NTIA rules of behavior, section 6.7 Privacy, personal photography. These photographs are displayed when a recipient opens the incoming email.

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

The legal authorities to maintain PII are 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. 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.

Also web servers under the GSS that support NTIA enterprise applications collect and maintain non-sensitive PII, such as user names, office phone number, and office email addresses for applications/web portal access/authentication purpose. The data collection is done through a formal request process using the NTIA System Authorization and Access Request (SAAR) form, and the access is annually validated. The sources of PII are other DOC Bureau (i.e., NOAA) and other government agencies (e.g., Department of Defense, Federal Communications Commission). The non-sensitive data collected for the NTIA application access is only used within the bureau for account creation and access permission process. It's not shared with outside the organization.

NTIA GSS protects the confidentiality and integrity of organizational sensitive information at rest. NTIA has implemented Data Loss Prevention (DLP) tools to identify, restrict, monitor, and protect sensitive data in use and at rest. In addition, other protection mechanisms are deployed, such as security baseline configurations, permission restrictions, Anti-virus, and system logs and data monitoring tools.

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

__X__ 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		k. Financial Transaction	
d. Employee ID	x	h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: NTIA maintains human resources (HR) reports received from DOCHROC which include Social Security Numbers (SSN) and employee ID numbers.					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth	x	m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	x	o. Medical Information	
d. Gender		j. Telephone Number	x	p. Military Service	
e. Age		k. Email Address	x	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		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		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) form.					

Government Sources					
Within the Bureau	x	Other DOC Bureaus	x	Other Federal Agencies	x
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	x	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		For administering human resources programs	x
For administrative matters	x	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

- For administering human resources programs: General Personal Data and Identifying numbers 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.

- 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.

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			
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.

	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:
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: On all NTIA public websites: http://www.ntia.doc.gov/ http://www.digitalliteracy.gov/ http://www2.ntia.doc.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: For the NTIA web portal access, individuals may decline (a statement included in the access request form: 'Disclosure of this information is voluntary') to provide PII by providing a written request on the NTIA access request form when they request an account. However, this action will affect NTIA application access permission. 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 NTIA web portal access, written consent to only particular uses of PII must be submitted as a part of the SAAR (System Authorization Access Request) form. However, failure to consent to the particular uses may affect NTIA application access. 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 particular 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 NTIA web portal access, PII is routinely updated as a part of annual account validation process. The account holder may submit a request to his/her NTIA sponsor point of contact to review and update their information anytime or at the annual account renewal time. 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. DLP monitors the PII/BII misuse.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 8/30/2017 ☐ 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 - 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 by Data Loss Prevention. - 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	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-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. 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: The information directly identifies a small number of individuals using SSN.
x	Quantity of PII	Provide explanation: Quantity of PII is minimal. Most NTIA web portals have between 50-100 accounts which are annually validated. In addition, the sensitive PII related to HR reports is minimal.
x	Data Field Sensitivity	Provide explanation: Sensitive PII data is in the GSS system.
	Context of Use	Provide explanation:
x	Obligation to Protect Confidentiality	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 access to PII information is limited to only the restricted staff members who create user accounts. The data is stored securely on the internal database. The PII in HR reports is stored in a designated data storage with limited access to managers and staff with HR responsibilities.

	Other:	Provide explanation:

Section 12: Analysis

12.1 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.