Version Number: 01-2017

U.S. Department of Commerce
National Technical Information Service

Privacy Impact Assessment
for the
NTIS001

Reviewed by: Allison McCall, 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: 2018.09.28 19:01:46 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NTIS/NTIS001

Unique Project Identifier: 207500

Introduction: System Description

The NTIS Information Technology Infrastructure System (NTIS001) is located in the NTIS data center at 5301 Shawnee Rd., Alexandria, VA 22312. NTIS001 is a General Support System (GSS) provides infrastructure and general support for all NTIS Data Center hosted systems. This includes network infrastructure such as servers, databases, user workstations virtual machines, network devices to include routers, switches, and firewalls, storage, telecommunications, information security tools, administrative utilities, general use printers, and access control systems. The system has been categorized, in accordance with Federal Information Processing Standard (FIPS) 199, as being a Moderate security impact system.

System data includes data to fulfill NTIS mission and business objectives. The data consists of NTIS system information stored within the NTIS infrastructure, Human Resources Management, Accounting and Finance, Building control and access control system, and CCTV system. CCTV access is restricted to key personnel, i.e. CISO, and CISO designees.

Authorized NTIS staff and contractors use their badges in order to gain access to the NTIS areas of the building and the NTIS data center. PIV badges are also used for authenticating to user workstations and laptops. Users are then able to retrieve, modify, and disseminate files from their workstations. Information sharing in regards to Human Resource documents (Employee on duty documents) occurs, on a case-by-case basis, between departments within NTIS, and between NTIS and other DOC Bureaus. Information sharing that occurs utilizes Accellion.

This information is collected, maintained, used, and disseminated in accordance with 5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12, IRS Publication-1075, Federal Information Security Management Act (Pub. L. 107-296, Sec. 3544); E-Government Act (Pub. L. 107-347, Sec. 203); Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et al.) and Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504); Federal Property and Administrative Services Act of 1949, as amended.

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 later). *Skip questions and complete certification.*

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*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID	X	f. Driver's License		j. Financial Account	X
c. Employer ID	X	g. Passport		k. Financial Transaction	X
d. Employee ID	X	h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*NTIS collects social security numbers while doing onboarding for all employees and contractors for HR related activities such as background investigations and PIV card processes. Although NTIS utilizes NIST for such HR related activities, soft copies of these files are scanned with SSNs redacted. Hard copies are secured in locked cabinets. For accounting services that require SSNs, these are purged (removed) immediately upon completion of processing which typically takes 24 hours. These hardcopies are also stored in locked cabinets.					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name		h. Place of Birth	X	n. Financial Information	X
c. Alias	X	i. Home Address	X	o. Medical Information	X
d. Gender	X	j. Telephone Number	X	p. Military Service	
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):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
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	
b. IP Address	X	d. Queries Run		f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)

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

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	
Telephone		Email			
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	x	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

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

All data stored in the NTIS001 system is encrypted when in transit as well as data at rest. All NTIS employees and contractors only have accesses and privileges to complete their job function and role. All accounts are recertified on an ongoing basis. All PII data is handled in person by specific personnel. All hard copies of the forms used to collect any of the PII data are locked away in a secure file cabinet and access is only allowed to specific personnel. Any data that is stored on the NTIS file share is only accessible by the personnel authorized to view the file. All NTIS personnel are required to complete an annual security awareness training. Local drives that store PII have Full Disk Encryption.

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	X
Video surveillance	X	Electronic purchase transactions	
Other (specify):			

	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).

PII collected, maintained, or disseminated by NTIS is used for two business functions: Human Resources and Accounting Services. NTIS collects PII for Human Resources to perform functions such as new hire onboarding. An example of this would be the completion of government required onboarding forms such as I-9 forms. Although, NTIS collects such data, human resource functions are tasked to The National Institute of Standards and Technology (NIST). NTIS collects hard copies of the information that is secured in locked cabinets. NTIS also retains soft copies of these forms with SSNs redacted.

For accounting services, NTIS collects and maintains PII to perform functions such as payment of vendor invoices, reimbursement to employees for any payments, as well as checking the Do Not Pay service to ensure the parties that are receiving payment are authorized to do so. However, SSNs are purged (removed) immediately upon completion of processing. Forms containing social security numbers are collected in person and not electronically.

5.2 Describe any potential threats to privacy 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 privacy as a result of the use of this PII data by NTIS would include risks such as unauthorized access, manipulation, and disclosure of any of the PII data stored/used by NTIS. To ensure that the information is secure all PII data is only handled by authorized personnel. All physical (hard copy) PII data is kept securely in locked file cabinets which only allow access to a maximum combination of 2 people. Any electronic copies of the files with PII are stored with Full Disk Encryption. Locally stored PII data is kept for historical reference, and only available and accessible by authenticating to a full-drive encrypted workstation. Specifically, for accounting services, electronically captured SSNs are purged (removed) immediately upon completion of processing. For HR services, any document will have SSNs redacted prior to scanning.

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.

	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.	
	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: _____.	
X	Yes, notice is provided by other means.	Specify how: Notice is provided at the time of employment and when changes to required access (data and physical) are made. Notice is posted regarding video surveillance, both outside and inside of the building.

	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: Individuals may decline to provide PII at the time of employment effectively not allowing it to be used at all. Declining to provide PII effectively declines employment.
	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.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Individuals are not presented with an opportunity to provide consent upon initial employment for particular uses of PII. However, PII is typically not utilized after initial HR processing.

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: Users may review their PII in person with NTIS onboarding staff and security personnel.
	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 to any PII/BII that is stored on any workstations or servers are monitored via OS and Network level auditing.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): _12/21/2017_____ ☐ 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 (POA&M).
X	A security assessment report has been reviewed for the supporting 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.
	Contracts with customers establish ownership rights over data including PII/BII.
	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).*

As required by FIPS 199, the NTIS001 system and all its components are reviewed for the sensitivity of the information in them and were determined to require protection appropriate for Moderate Impact systems. All relevant policies, procedures and guidelines, including NIST Special Publication 800-53, have been followed to ensure the security of the systems and the information in them. All PII is stored in a secure file cabinet for hard copies and all electronic copies are stored with Full Disk Encryption. No PII data is transmitted via email or by any other means.

Specifically, for accounting services, electronically captured SSNs are purged (removed) immediately upon completion of processing. For HR services, any document will have SSNs redacted prior to scanning.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a.

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-25, Access Control and Identity Management System, http://osec.doc.gov/opog/PrivacyAct/SORNs/dept-25.html, GSA/GOVT-7, Federal Personal Identity Verification Identity Management System (PIV IDMS), DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons, DEPT-13, Investigative and Security Records, and DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
	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: GRS 3.1 General Technology Management. User data is deleted as part of the user employment termination process.
	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		Deleting	X
Other (specify): All hard drives that store PII, when they need to be disposed are destroyed completely.			

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 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 levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Photographs, social security numbers, name, address, date of birth.
X	Quantity of PII	Provide explanation: Approximately 165 users are currently in the database.
	Data Field Sensitivity	Provide explanation:

X	Context of Use	Provide explanation: PII is only used for Human Resources and Accounting services.
X	Obligation to Protect Confidentiality	Provide explanation: NTIS has an obligation to protect the privacy and confidentiality of all of its customers, employees, contractors, and vendors.
X	Access to and Location of PII	Provide explanation: Very limited access to PII by approved and authorized personnel only.
	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.)

Potential threats to privacy as a result of the use of this PII data by NTIS would include risks such as unauthorized access, manipulation, and disclosure of any of the PII data stored/used by NTIS. The PII data collected by NTIS was determined to be required for the processing of personnel and services needed to fulfill the NTIS business mission. Any PII data that is collected is required to be sourced directly from the individuals being staffed to maintain accuracy and compliance with government onboarding and access requirements. The PII data is limited only to NTIS affiliated entities. BII data collected from Private Sector sources is required for funding and payment of contract related expenses and profits. This information is required to sustain the business model and mission of NTIS. NTIS collects PII information in regards to human resources to comply with NIST as NIST is the service provider to NTIS for all PIV badging and background investigation activities.

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.