Template Version Number: 01-2020

U.S. Department of Commerce
National Technical Information Service
(NTIS)

Privacy Threshold Analysis
for the
NTIS001

U.S. Department of Commerce Privacy Threshold Analysis

NTIS/NTIS001

Unique Project Identifier:

CSAM ID: 1810

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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

NTIS 001 Infrastructure & Networking System is a General Support System (GSS)

(b) System Location

NTIS001 is located at NTIS HQ Data Center5301 Shawnee Road, Alexandria, VA 22313

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

NTIS001 is a General Support System (GSS) provides infrastructure and general support for all NTIS Data Center hosted systems. This includes network infrastructure elements such as servers, databases, user workstations virtual machines, and network devices to include routers, switches, and firewalls, storage, telecommunications, administrative utilities, general use printers, and access control systems.

(d) The purpose that the system is designed to serve

The purpose of the system is to provide infrastructure and general support for all NTIS Data Center hosted systems. Additionally, the NTIS001 provides two business functions which collect, maintain, or disseminate PII by NTIS. Human Resources and Accounting Services. The PII is stored in the NTIS001 system and is encrypted when in transit as well as data at rest. NTIS collects PII of employees and contractors 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 purges soft copies upon the transfer to NIST.

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.

(e) The way the system operates to achieve the purpose

NTIS collects PII of employees and contractors 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. 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.

(f) A general description of the type of information collected, maintained, used, or disseminated by the system

NTIS collects PII of employees and contractors 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 purges soft copies upon the transfer to NIST.

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.

Some of the information collected would be social security number, taxpayer ID, employer ID, employee ID, financial account, financial transaction, name, gender, age, race/ethnicity, date of birth, place of birth, home address, telephone number, email address, and medical information.

(g) Identify individuals who have access to information on the system

The individuals who have access to the PII information on the system would be the HR staff, accounting staff and the system administration team. Logical access, role-based access, and least privilege controls are implemented for all administrators and users.

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

NTIS collects PII of employees and contractors 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. 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.

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

As 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 purges soft copies upon the transfer to NIST.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*

____ 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). *Continue to answer questions and complete certification.*

_X___ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

__X__ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

__X__ Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	X
Video surveillance	X	Electronic purchase transactions	
Other (specify):			

____ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

__X__ Yes, the IT system collects, maintains, or disseminates BII.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: (*Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
____ Other Federal Government personnel

____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

__X__ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form. 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 and sent to NIST for processing. Once NTIS has completed sending information to NIST for processing, soft copies are destroyed and/or purged. 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.
Provide the legal authority which permits the collection of SSNs, including truncated form. National Institute of Standards and Technology Authorization Act of 2010 (Public Law 111-358, Title IV); 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107; and 5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 3309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397.

____ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to NTIS001 and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to NTIS001 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Leigh Anne Levesque Office: NTIS/OCIO Phone: 703-605-6097 Email: LLevesque@ntis.gov Signature: Leigh Anne Levesque Digitally signed by Leigh Anne Levesque Date: 2022.09.22 11:42:53 -04'00' Date signed: _____	**Chief Information Security Officer** Name: Bilal Baisa Office: NTIS/OCIO Phone: 703-605-6172 Email: BBaisa@ntis.gov Signature: Bilal Baisa Digitally signed by Bilal Baisa Date: 2022.09.22 11:14:52 -04'00' Date signed: _____
Privacy Act Officer Name: Bilal Baisa Office: NTIS/OCIO Phone: 703-605-6172 Email: BBaisa@ntis.gov Signature: Bilal Baisa Digitally signed by Bilal Baisa Date: 2022.09.22 11:15:11 -04'00' Date signed: _____	**Authorizing Official** Name: Gregory Capella Office: NTIS/OCIO Phone: 703-605-6710 Email: GCapella@ntis.gov Signature: Gregory Capella Digitally signed by Gregory Capella Date: 2022.09.23 21:09:36 -04'00' Date signed: _____
Bureau Chief Privacy Officer Name: Bilal Baisa Office: NTIS/OCIO Phone: 703-605-6172 Email: BBaisa@ntis.gov Signature: Bilal Baisa Digitally signed by Bilal Baisa Date: 2022.09.22 11:15:44 -04'00' Date signed: _____	