Version Number: 01-2018

U.S. Department of Commerce
National Technical Information Service

Privacy Threshold Analysis
for the
NTIS IT Infrastructure System (NTIS001)

U.S. Department of Commerce Privacy Threshold Analysis

NTIS/NTIS001

Unique Project Identifier: 207500

Description of the information system and its purpose:

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 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. 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.

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 for 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.

Questionnaire:

1. 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.*

_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.*

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.

- The system includes a building entry and access control system that is used to process, maintain, and manage access to NTIS facilities and systems.
- The system includes a CCTV system that is used to monitor and keep record of access to NTIS facilities and systems.
- The system also includes network systems which are utilized for the storage of PII information such as financial information, personal data, work-related data, distinguishing features, and system administrative/audit data.

____ 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 about: (*Check all that apply.)*

_X_ Companies
_X_ Other business entities

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

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

_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
___ 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 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.

4c. 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, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the 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 the NTIS IT Infrastructure System (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 the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Leigh Anne Levesque

Signature of ISSO or SO: _____ Date: 7-31-19

Name of Information Technology Security Officer (ITSO): Bilal Baisa

Signature of ITSO: _____ Date: 07/31/19

Name of Authorizing Official (AO): Allison McCall

Signature of AO: Allison McCall _____ Date: 8/1/19

Name of Bureau Chief Privacy Officer (BCPO): Todd McKeever

Signature of BCPO: _____ Date: 8/5/19