U.S. Department of Commerce
NTIS

Privacy Threshold Analysis
for the
National Technical Information Service
(NTIS) Electronic Subscription Service (NESS)
NextGen DMF

U.S. Department of Commerce Privacy Threshold Analysis
NTIS/NESS

Unique Project Identifier: 25200/21600

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:

The NTIS Electronic Subscription Service (NESS) is a Major Application (MA) with a Federal Information Processing Standard (FIPS) 199 security impact category of moderate. NESS is housed in the NTIS Data Center on the 2nd floor of 5301 Shawnee Road Alexandria, VA 22312 within a business park. The first through third of four floors of the building are occupied by NTIS federal employee/contractor personnel and not accessible by the public except for the first-floor common lobby. The fourth-floor tenants can only access the fourth floor and the lobby. There are no distinguishing signs outside the building to indicate the presence of a Data Center. The building is freestanding and exterior walls are composed of brick.

The purpose of the NESS system is to provide a secure web interface for NTIS data product access for registered subscribers, including database search capability through an NTIS-owned and operated system. Traditionally, the service was being provided by a legacy Joint Venture Partner, Global Information Management (GIM), for such data products such as the Limited Access Death Master File (LADMF). The benefits of transitioning to NESS are:

- Reduction in costs (estimated at least 20%);
- Improvements in security;
- Improvements in database functionality
- A more streamlined set of product alternatives; and
- A system that is more agile and responsive to customer and NTIS needs.

The raw data files for the Limited Access Death Master File (LADMF) from the Social Security Administration (SSA) contains over 83 million records of deaths that have been reported to SSA. This file includes the social security number, name, date of birth, and date of death each decedent, if the data are available to the SSA. By methodically running financial, credit, and other applications against the LADMF, the financial community, insurance companies, security firms and state and local governments are better able to identify and prevent identity fraud. The SSA reports that the LADMF contains 85% of all deaths annually. Updates are available on a weekly, or monthly basis. Visit http://classic.ntis.gov/products/ssa-dmf/# for further information.
NESS receives files from the Social Security Administration using a secured file transfer protocol/program (SFTP) or through an encrypted internet communication protocol (HTTPS [https://dmf.ntis.gov]) daily, weekly, monthly and quarterly. NESS receives files from The Drug Enforcement Agency in a similar manner on a daily basis.

There are two typical types of system transactions conducted on the NESS system; financial and database query transactions. Customers use a system called ELAN which will collect user account information, order information, and credit card information to pay for the rights to conduct for database query transactions. A NESS subscription administrator will manually take the transaction ID from ELAN and manually enter it into the NESS system thus enabling subsequent database query transactions.

Database query transactions can be conducted using three prototypical methods once authenticating through a web interface. Customers can either download batch files, leverage an internal API service to view the files through a basic interface which allows for searching, sorting, and aggregation, or leverage external APIs which allow then use their own applications to query data from the NESS databases.

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.*

____ 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). *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 01-2017 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.

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

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

X 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.)*

____ DOC employees
____ National Institute of Standards and Technology Associates
____ Contractors working on behalf of DOC
____ Other Federal Government personnel
X 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.

NESS NextGen DMF system is used to host the subscription services NTIS provides to gain access to the Social Security Administration's (SSA) Death Master File (DMF). Customers must go through a certification process in which they are evaluated on their ability to keep the information secure once access has been approved.

SSA and NTIS have entered into an agreement in which NTIS will collect, host, and disseminate SSNs to approved customers.

____ 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 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 NESS 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 Information System Security Officer (ISSO) or System Owner (SO): Pad Hosmane

Signature of ISSO or SO: PAd Hosmane Digitally signed by PAd Hosmane Date: 2020.09.30 09:10:01 -04'00' Date: _____

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

Signature of ITSO: BILAL BAISA Digitally signed by BILAL BAISA Date: 2020.09.29 14:27:30 -04'00' Date: _____

Name of Privacy Act Officer (PAO): Allison McCall

Signature of PAO: Allison McCall Digitally signed by Allison McCall Date: 2020.09.30 09:24:59 -04'00' Date: _____

Name of Authorizing Official (AO): Allison McCall

Signature of AO: Allison McCall Digitally signed by Allison McCall Date: 2020.09.30 09:25:17 -04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Allison McCall

Signature of BCPO: Allison McCall Digitally signed by Allison McCall Date: 2020.09.30 09:25:40 -04'00' Date: _____