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

Privacy Threshold Analysis
for the
NTIS Electronic Subscription Service (NESS)

U.S. Department of Commerce Privacy Threshold Analysis

NTIS/NESS

Unique Project Identifier: CSAM ID – 2651

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 on 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

The NTIS Electronic Subscription Service (NESS) is a Major Application (MA)

(b) System Location

The National Technical Information Service Electronic Subscription Service (NESS) is hosted by the cloud service provider (CSP) Amazon Web Services (AWS). AWS is responsible for providing all facility related physical security, access control measures, environmental controls, data center layout diagrams, etc. for NTIS websites/applications that AWS hosts.

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

The NTIS Electronic Subscription Service (NESS) system consists of an interconnected group of applications, services, business processes, and organizations with the mission to provide access to search the Social Security Administration’s (SSA) Death Master File (DMF).

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

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
- A system that is more agile and responsive to customer and NTIS needs.

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

NESS is comprised of an independent database system. The Death Master File (DMF) from the Social Security Administration (SSA) contains over 86 million records created from SSA payment records. This file includes the following information on each decedent, if the data are available to the SSA: social security number, name, date of birth, and date of death. This database was created to streamline their perspective verification processes and provide singular resource connectivity.

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

NESS collects sensitive PII information from users such as credit card number, DOB, Name, user ID, etc. For DMF, the information is also sensitive, but the information is for the deceased. The PII within the system is collected, stored, used, processed, disclosed, or disseminated to support business certification and subscription. Additionally, to advise businesses/agencies of deceased Social Security Numbers. The PII that is stored for NESS is located on an encrypted database.

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

Only the system administrators can access this information.

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

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 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.

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

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.

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.*

_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. *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.

____ 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
____ 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 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 SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

_X__ The criteria implied by one or more of the questions above **apply** to the NESS and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_____ 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.

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: 2023.05.08 09:19:03 -04'00' Date signed: ______________________	**Information Technology 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: 2023.04.12 11:40:44 -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: 2023.04.12 11:41:38 -04'00' Date signed: ______________________	**Authorizing Official** Name: Wayne Strickland Office: NTIS/OPM Phone: 703-943-6543 Email: wstrickland@ntis.gov Signature: Wayne Strickland Digitally signed by Wayne Strickland Date: 2023.05.18 15:06:30 -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: 2023.04.12 11:42:03 -04'00' Date signed: ______________________	

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PTA.