Version Number: 01-2018

U.S. Department of Commerce
National Technical Information Service

Privacy Impact Assessment
for the
National Technical Information Service
(NTIS) Electronic Subscription Service (NESS)
NextGen DMF

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: 2018.04.03 11:22:59 -04'00'

4/2/2018

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

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

Unique Project Identifier: 25200/21600
Introduction: System Description

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 owned facility in Alexandria, VA.

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 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..

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.

The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information is 15 U.S.C. 1151-57; 41 U.S.C. 104; 44 U.S.C. 3101; Section 203 of the Bipartisan Budget Act of 2013 (Pub. L. 113-67) (Act).

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

___X__ 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.

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*	x	e. File/Case ID		i. Credit Card	x
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	x
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth	x	m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	x	o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	
e. Age	x	k. Email Address	x	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): For DMF - Date of Birth, Date of Death.					

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		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	x
b. IP Address	x	d. Queries Run	x	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		Hard Copy: Mail/Fax	x	Online	x
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	x
State, Local, Tribal	x	Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application			x		
Other (specify):					

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

Information is received directly from SSA using SFTP method and is continuously updated insuring accuracy. System admins and staff are not able to modify or change information received. It also encrypted using TLS 1.2 when being transmitted.

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	
Video surveillance		Electronic purchase transactions	x
Other (specify): System administrators have access to the credit card information which is used in NESS			

	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	
For administrative matters	x	To promote information sharing initiatives	x
For litigation		For criminal law enforcement activities	
For civil enforcement activities	x	For intelligence activities	
To improve Federal services online	x	For employee or customer satisfaction	x
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).

- Social Security: The main purpose of this system is to allow users to access the death master file. Social security numbers of the deceased are stored and used in this system.
- Credit Card: The users must pay a subscription fee in order to obtain access to the system. The system collects the credit card information for these users and the credit card information is then manually deleted by the admin once the payment is processed. Only the last 4 digits are stored after.
- Financial Transaction: The transaction ID is stored for the purpose of completing the transaction along with having a reference for all transactions.
- Name: The names of the users and the deceased are stored by the system
- Age: The age of the peoples identified in the DMF can be determined based on their DOB and decease date.
- DOB: The DOB of the deceased is stored in DMF as well as the DOB of the users.
- Home Address: Home address is saved in the user profile and the peoples identified in the DMF
- Email Address: Email address is saved in the user profile
- Occupation: Occupation of the user is saved in their user profile.
- Job title: job title is saved for the user in the user profile
- Work Address: Work address is saved in the user profile
- Telephone Number: Telephone number is saved in the user profile for contact purposes.
- User ID: Unique user IDs are created in order to give access to subscribers.
- IP Address: The IP address is for the developers and admins to monitor who has accessed the system internally
- Contents: Contest that are used by the database admin is saved for audit purposes.

Persons seeking certification for access to the Limited Access Death Master File must submit the revised Certification Form, renewal of which is required annually. NTIS will use the information collected to determine whether the Person or Certified Person has established that it meets the requirements for certification under the final rule. Persons seeking DMF access must supply the data necessary to give them access to the information.

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.)

The National Technical Information Service (NTIS) Limited Access Death Master File Subscriber Certification Form, Form NTIS FM161 (Certification Form), is used to collect information related to the implementation of Section 203 of the Bipartisan Budget Act of 2013 (Pub. L. 113-67) (Act). Section 203 of the Act prohibits disclosure of Limited Access Death Master File (Limited Access DMF) information during the three-calendar-year period following the death of an individual unless the person requesting the information has been certified under a program established by the Secretary of Commerce. The Act directs the Secretary of Commerce to establish a certification program for such access to the Limited Access DMF. The Secretary of Commerce has delegated the authority to carry out the DMF certification program to the Director, NTIS.
Initially, on March 26, 2014, NTIS promulgated an interim final rule, establishing a temporary certification program (79 FR 16668) for persons who seek access to the Limited Access DMF. Subsequently, on December 30, 2014, NTIS issued a notice of proposed rulemaking (79 FR 78314). NTIS adjudicated the comments received and, on June 1, 2016, published a final rule (81 FR 34822). The interim final rule required that Persons and Certified Persons use the Certification Form to provide information necessary to establish whether they should be certified to access the Limited Access DMF (79 FR 16668 at 16671), and OMB approved the initial version of the Certification Form in March 2015. In the notice of proposed rulemaking, NTIS set forth initial revisions to the Certification Form (79 FR 78314 at 78320-21). The final rule requires that Persons and

Certified Persons provide additional information intended to improve NTIS's ability to determine whether a Person or Certified Person meets the requirements of the Act. Once the applicant is Certified and the Subscription order is fulfilled, and access is granted, the request is marked Complete on the tool and can no longer be edited by anyone. The DMFCERT review team can view the history of a request at any time. All uploaded files, including Form PDFs, attachments and even email communications are stored on a Secure File Server.

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			
Federal agencies	x	x	
State, local, tribal gov't agencies	x		
Public	x		
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.

x	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: NESS receives information from the SSA system referred to as "LADMF". • User account: This consists of purchase order and profile using TLS 1.2 and AES 256 encryption mechanisms to protect the confidentiality of the PII. • Product and service related information: Using AES 256 compliant encryption
	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	
Contractors			
Other (specify): Individuals and organizations who have been certified to access information by demonstrating a need to know. This can include the financial community, insurance companies, security firms, and state and local governments to identify and prevent identity fraud.			

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.	
x	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: https://classic.ntis.gov/about/policies/	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: If individuals wish to decline to provide PII/BII they must opt out of using the system. Orders cannot be processed if information is not provided.
x	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: The user will be given the opportunity to acknowledge/accept the terms of use. However if they do not agree they can leave the page. There is not a button for declining.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: If individuals wish to decline to provide PII/BII they must opt out of using the system. Orders cannot be processed if information is not provided.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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	Specify how: Individuals may request to review/update their

	review/update PII/BII pertaining to them.	PII/BII via mail to the FOIA and Privacy Act officer, phone call, or directly within the DMF Cert website. National Technical Information Service Freedom of Information Act and Privacy Act Officer 5301 Shawnee Rd Alexandria, VA 22312 1-800-553-6847 https://dmfcert.ntis.gov The users can also view their user profile and make changes as necessary. However the user cannot update their transaction number or credit card number after an order has been completed.
	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: transaction process is tracked
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): _____ ☒ 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).
	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.
x	Contracts with customers establish ownership rights over data including PII/BII.
x	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).*

SSL and TLS 1.2 is used for security in transmission. Also use SFTP server for data at rest and sending files. AES 256 encrypted.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

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."

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*:
	Yes, a SORN has been submitted to the Department for approval on (date).
x	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: NC1-422-82-1 National Technical Information Service
	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		Overwriting	x
Degaussing		Deleting	x
Other (specify):			

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.)*

	Identifiability	Provide explanation:
x	Quantity of PII	Provide explanation: DMF currently has over 83 million Social security numbers. These are numbers for the deceased however there are discrepancies at times with people who are not deceased. The NESS system has an ongoing subscriber count which can change over time however at the time being is roughly 2000 users. Initially NESS expects this number to decrease and then increase over time due to retirement and users being given access later on. The credit card information used for transactions is on a case by case basis, only users who want a subscription have this information stored.
x	Data Field Sensitivity	Provide explanation: The information collected by NESS is sensitive PII as for users it consists of credit card number, DOB, Name, user ID, etc. For DMF the information is also sensitive but the information is for the deceased.
	Context of Use	Provide explanation:
x	Obligation to Protect Confidentiality	Provide explanation: NTIS is responsible for ensuring that the information that is collected is stored and maintained in accordance with DOC policy, FISMA, and NIST.

x	Access to and Location of PII	Provide explanation: The PII that is stored for NESS is located on an encrypted database. Only the system administrators can access this information. All transactions are performed using SSL, TLS 1.2, and on an AES 256 compliant encryption mechanism for information at rest.
	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.)

Specifically with the DMF, upon receiving updates from the SSA, occasionally, records will be withdrawn from the DMF due to the fact that the record is based on an individual who is not actually deceased. Due to the nature of these updates, it would be possible for a malicious actor to track which records are being withdrawn and therefore exposing PII of living individuals.

Additionally, there is a risk that customers may mishandle information potentially causing a data leakage. This is risk minimized by the mandatory certification process to emphasize the proper handling of potentially sensitive information and help assure individuals and organizations provide proper due diligence.

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.