Version Number: 01-2015

U.S. Department of Commerce
National Technical Information Service

Privacy Impact Assessment
for the
Death Master File (DMF) Cert

Reviewed by: Heather Lynch, 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: 2018.02.08 13:13:38 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NTIS/Death Master File (DMF) Cert

Unique Project Identifier:

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) a general description of the information in the system

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.

The revised Certification Form collects the following information in addition to the information collected in the previously-approved form:

- First-time Certification or Renewal of Certification: All Persons and Certified Persons seeking to obtain or renew their certification for access to the Limited Access DMF must submit the Certification Form. A certification is effective for a period of one year from the date of the approval email from NTIS. As such, a Certified Person seeking to renew its certification must file a new Certification Form once each year. Section 1110.105(a) of the final rule specifies that the Certified Person must indicate on the Certification Form that it is a renewal. To implement this requirement of the final rule, the revised Certification Form requires the applicant to indicate whether this is a "First-Time Certification" or "Renewal of

Certification." The collection of this information will facilitate the Certified Person's satisfaction of the requirement of Section 1110.105(a).

- URL: Section 1110.102(a)(1) of the final rule requires that a Person seeking access to the Limited Access DMF establish that it has a legitimate fraud prevention interest or legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty. NTIS will use the URL, if any, for each Person or Certified Person to ascertain that the organization seeking certification or recertification is a legitimate business performing the functions that it claims to be performing. The collection of this information is necessary to evaluate whether a Person or Certified Person meets the requirements of Section 1110.102(a)(1).
- NTIS Customer Number: The collection of each Person or Certified Person's NTIS Customer Number provides a unique identifier which will allow NTIS to identify existing customers without requiring any personal identifying information.
- State Incorporation/Registration Number: Section 1110.102(a)(1) of the final rule requires that a Person seeking access to the Limited Access DMF establish that it has a legitimate fraud prevention interest or legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty. NTIS will use the State of Incorporation/Registration Number, if any, for each Person or Certified Person to ascertain that the organization seeking certification is a legitimate business performing the functions that it claims to be performing. The collection of this information is necessary to evaluate whether a Person or Certified Person meets the requirements of Section 1110.102(a)(1). Please note that NTIS had originally planned to include the Person or Certified Person's Dun and Bradstreet Number in the revised Certification Form (79 FR 78314 at 78320). However, NTIS has chosen to replace the collection of the Person or Certified Person's Dun and Bradstreet Number with the State Incorporation/Registration Number in the revised Certification because it is a more specific indicator that a person is engaged in business activity.
- Employer Identification Number (EIN): Section 1110.102(a)(1) of the final rule requires that a Person seeking access to the Limited Access DMF establish that it has a legitimate fraud prevention interest or legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty. NTIS will use the EIN for each Person or Certified Person to ascertain that the organization seeking certification is a legitimate business performing the functions that it claims to be performing. The collection of this information is necessary to evaluate whether a Person or Certified Person meets the requirements of Section 1110.102(a)(1).
- Authorized Contact Person: Collection of each Person or Certified Person's authorized contact person will expedite the certification process by permitting NTIS to contact the identified contact person without having to spend time identifying the correct person during the certification process.
- Email and Phone Number for Authorized Contact Person: Collection of the email and phone number of the authorized contact person will expedite the certification process by permitting NTIS to contact the identified contact person without having to spend time identifying the correct person during the certification process.
- State or Local Governmental Department or Agency: All Persons and Certified Persons, are required, under the final rule, to provide a written attestation from an independent Accredited Conformity Assessment Body (ACAB) (unless the ACAB qualifies for "firewalled status" under § 1110.502). If the Person or Certified Person, however, is a state or local government agency seeking or renewing certification, and a state or local government office of Inspector General (IG) or Auditor General (AG) is a department of the same state or local government, the two are not considered owned by a common "parent," and therefore, the office of IG or AG is considered independent under § 1110.501(2). The Certification Form requires the Person or Certified Person to indicate if it is a state or local government department or

agency. In these circumstances, the state or local IG or AG may provide the attestation in lieu of an independent ACAB, using the State and Local AG or IG Systems Safeguards Attestation Form (AG/IG Safeguards Attestation Form). NTIS will use the information to determine whether the associated written attestation should be submitted by an ACAB or a state or local government office of an AG or IG, using the applicable version of that form, and to determine the Person or Certified Person's eligibility for certification.

- Whether the Certified Person is Submitting a Written Attestation with the Certification Form: Under the final rule, all Certified Persons must be audited with respect to the requirements of Section 1110.102(a)(2) at least once every three years under the program. Section 1110.105(b) specifies that either the submission of a written attestation of an ACAB or completion of a satisfactory unscheduled or scheduled audit under § 1110.201 by NTIS or by an ACAB acting on behalf of NTIS within three years of the date of the present application will satisfy this requirement. To implement this requirement of the final rule, the revised Certification Form requires an applicant not submitting a new written attestation to indicate why it is not submitting a written attestation of an ACAB or an AG or IG. The collection of this information will also prompt Persons and Certified Persons to remember to include the written attestation with the Certification Form, thus minimizing potential delays in the processing of their applications if NTIS had to contact them to provide a copy of the attestation or audit, and possibly even preventing denials of their applications for incompleteness. This information also will allow NTIS to ensure that it has been provided with the written attestation or audit, and that the written attestation or audit was completed within the three-year timeframe.

(b) a description of a typical transaction conducted on the system

The customer logs into the system using a username or password. If they don't already have one, they can register themselves and create username and password. Once logged in, they create a request with all the forms on it. For Certification and Agreement, there is a web version of the form that they fill online on the tool. Once done, they have to download the filled PDF, print, sign, scan and upload it back to the tool. They then submit the form and can no longer edit it. For Attestation and Firewall forms, they directly download a fillable PDF, fill, print, sign, scan and then upload back to the system and submit. They can then log out and wait for further notice via email from the NTIS personnel.

NTIS personnel (Customer Support team, Subscriptions, Security, IT etc) will receive system generated emails for when a request is in their queue for review. Each role user has their own username and password for login. When they login, they have queues with different customer requests on them, waiting for their review. They review and fill out verification forms on the tool itself. Every approval from stage one, moves the request further along for final Certification. Once Certifier approves, the customer is certified and then Subscriptions work on their actual subscription order. The order is manually placed in ELAN by Subscriptions team, and then order number and subscription start date are updated on the tool. At any step, if some correction is needed by the customers, the NTIS personnel enter comments and mark the request for correction. Auto generated system emails notify the customer of the same and then they can log back in and work on the correction.

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.

(c) any information sharing conducted by the system

N/A

(d) a citation of the legal authority to collect PII and/or BII

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)

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system

Moderate

Section 1: Status of the Information System

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

____ This is a new information system.
_X_ This is an existing information system that has not undergone any changes that create new privacy risks.
____ 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):					

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*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	

c. Employer ID	X	g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify): NTIS Customer Number, State Incorporation/Registration Number					
*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		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	
b. Job Title		e. Email Address	X	h. Work History	
c. Work Address		f. Business Associates			
i. Other work-related data (specify): URL & Company Name					

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		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify): Application exceptions.					

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		Online	X
Telephone		Email			
Other (specify):					

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

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

2.3 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	
Other (specify):			

X	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			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	

For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
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).

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.

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			
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

X	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.

	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:
X	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	X
Contractors	X		
Other (specify):			

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.

X	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.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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 review/update PII/BII pertaining to them.	Specify how: Individuals may request to review/update their 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
	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.
	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.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 02/08/2017 ☐ 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 (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	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.

System users access the application via an HTTPS connection. DMF Cert is located within a secure government data center with restricted access. NIST SP 800-53 Rev 4 Moderate controls are in place for the system. Data at rest is encrypted using FIPS 140-2 approved measures.

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."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: COMMERCE/NTIS-1 has been updated.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

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 Levels

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.

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

	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: NTIS expects 560 users annually.
X	Data Field Sensitivity	Provide explanation: Not storying any sensitive PII.
	Context of Use	Provide explanation:
X	Obligation to Protect Confidentiality	Provide explanation: Privacy Act of 1974
X	Access to and Location of PII	Provide explanation: Data is stored in the NTIS data center which has multiple layers of physical security controls present.
	Other:	Provide explanation:

Section 12: Analysis

12.1 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.

12.2 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.