

**U.S. Department of Commerce  
National Technical Information Service**



**Privacy Threshold Analysis  
for the  
Death Master File Certification (DMF Cert)**

## **U.S. Department of Commerce Privacy Threshold Analysis**

### **NTIS/ Death Master File (DMF)**

**Unique Project Identifier: 25230**

**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:** *Provide a general description of the information system and its purpose in a way that a non-technical person can understand.*

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).

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.

**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. *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. *Please describe the activities which may raise privacy concerns.*

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.)."

Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

Companies

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..."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

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?

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.

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.***

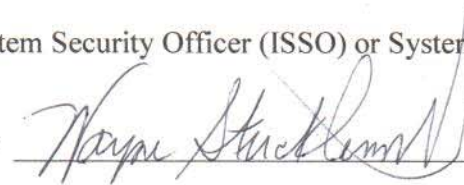
### CERTIFICATION

  X   I certify the criteria implied by one or more of the questions above **apply** to the DMF Cert 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): Wayne Strickland

Signature of ISSO or SO: \_\_\_\_\_



Date: 01/24/2018

Name of Information Technology Security Officer (ITSO): Heather Lynch

Signature of ITSO: \_\_\_\_\_



Date: 01/31/2018

Name of Authorizing Official (AO): Allison McCall

Signature of AO: \_\_\_\_\_



Date: 1/31/18

Name of Bureau Chief Privacy Officer (BCPO): Heather Lynch

Signature of BCPO: \_\_\_\_\_



Date: 01/31/18