Limited Access Death Master File Certification Program (Publication 100)

Information Security Guidelines for Use and Protection of Limited Access DMF Information

Table of Contents

This publication, "**Limited Access Death Master File Certification Program (Publication 100): Information Security Guidelines for Use and Protection of Limited Access DMF Information**," has been developed by the National Technical Information Service (NTIS) in conjunction with statutory responsibilities delegated to NTIS by the Secretary of Commerce under **Section 203 of the Bipartisan Budget Act of 2013, Pub. L. 113-67**.

This publication is not subject to copyright in the United States. Attribution would, however be appreciated by NTIS.
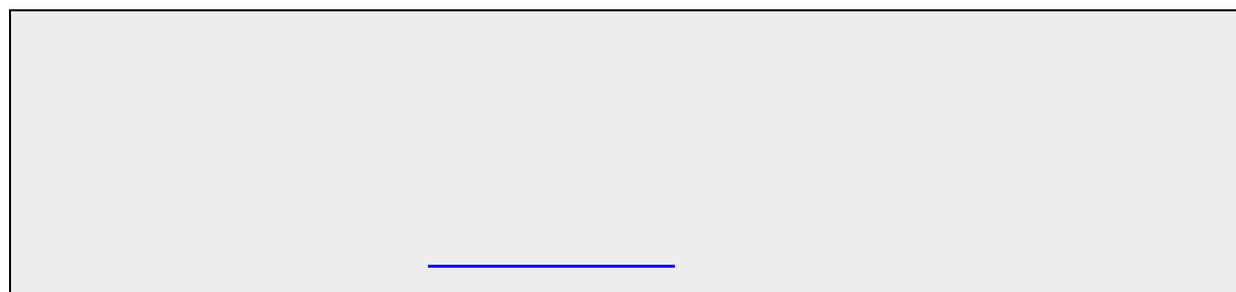
1   Introduction

1.1   General

The Death Master File (DMF) is an official Government dataset of deceased citizens maintained by the Social Security Administration (SSA). This dataset contains over eighty- five (85) million death records, from 1936 to present. The DMF includes key identifying data points on deceased individuals including first name, last name, social security number, date of birth, and date of death. Although SSA maintains the contents of the dataset, it is distributed by the Department of Commerce (DOC) National Technical Information Service (NTIS). Section 203 of the Bipartisan Budget Act of 2013 prohibits disclosure of DMF information during the three-calendar-year period following an individual's death (the "Limited Access DMF"), unless the person requesting access to the information has been certified to receive that information under a program established by the Secretary of Commerce and delegated by the Secretary to NTIS. In addition, the Limited Access DMF program requires a Certified Person to have a legitimate fraud prevention interest or a legitimate business purpose as a basis for certifying to receive and access Limited Access DMF information, as well as systems, facilities, and procedures in place to safeguard the information. This publication has been prepared by NTIS as a guide to safeguarding Limited Access DMF.

1.2   Overview of NTIS Limited Access DMF Information Security Guidelines

This publication provides guidance to assist Certified Persons in ensuring that their policies, practices, controls, and safeguards adequately protect Limited Access DMF information. The guidelines outlined herein apply to all Limited Access DMF information, no matter the amount or the media in which it is recorded. Certified Persons may be NTIS subscribers or licensees that have access to DMF information. Conforming to these guidelines is intended to assist Certified Persons in meeting the requirement that a Certified Person have systems, facilities, and procedures in place to safeguard Limited Access DMF information, and experience in maintaining the confidentiality, integrity, security, and appropriate use of such information, pursuant to requirements similar to the requirements of section 6103(p)(4) of the Internal Revenue Code of 1986.

Guidance throughout this document applies to all organizational segments of a Certified Person, whether a Licensee or Subscriber receiving Limited Access DMF information. It is the Certified Person's responsibility to ensure its own personnel and any others to whom it may permit access to Limited Access DMF information, understand and implement the guidance in this publication.

This publication provides the preliminary steps to consider before submitting a request to receive Limited Access DMF information, guidance for proper protection, and expectations of NTIS, and considerations that may be helpful in establishing a program to protect Limited Access DMF information.

NTIS is responsible for all interpretations of safeguarding guidance. This publication's guidance may be supplemented or modified between editions via guidance issued by NTIS and posted on the NTIS Limited Access DMF website.

To assist Certified Persons in selecting and implementing appropriate protective measures and practices, NTIS has developed this guidance document. This document reflects NTIS's current views on controls and does not itself establish legally enforceable requirements or impose any burdens on Certified Persons. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for safeguarding Limited Access DMF. Rather, they are examples of measures and practices that a Certified Person may choose to consider as part of its overall strategy. Certified Persons have the ability to choose and implement other measures based on their circumstances, including their security issues and risks, physical and operating environments, and other appropriate factors.

1.3   Access Safeguards Resources Online

NTIS maintains NTIS DMF Publication 100, templates, guidance, and frequently asked questions online at: https://dmf.ntis.gov/. Certified Persons are highly encouraged to periodically visit the website for new updates. The website is maintained with resources to assist with meeting the NTIS DMF Publication 100 guidance.

1.4   Key Definitions

This section establishes a baseline of key terms used throughout this publication. For additional definitions of terms and phrases, refer to Exhibit 1 Glossary and Key Terms. In the event that a term's definition in this publication differs from the definition of the same term in the NTIS regulation, found at Part 1110 of Title 15 of the Code of Federal Regulations, the regulation is controlling.

1.4.1   DMF Information

DMF information is the name, social security account number, date of birth, and date of death of deceased individuals maintained by the Commissioner of Social Security, other than information that was provided to such Commissioner under section 205(r) of the Social Security Act (42 U.S.C. 405(r)). DMF information does not include information provided directly by a Certified Person or third parties. If a Certified Person obtains, or a third party subsequently provides to a Certified Person, death information (i.e., the name, social security account number, date of birth, or date of death) independently, the information is not considered DMF information as long as the NTIS source information is replaced with the newly provided information.

1.4.2   Limited Access DMF Information

The Limited Access DMF information is the DMF product made available by NTIS which includes DMF with respect to any deceased individual at any time during the three- calendar-year period beginning on the date of the individual's death.

Safeguarding Limited Access DMF information is critically important to continuously protect DMF Limited Access information as required by Section 203 of the Bipartisan Budget Act of 2013 (Act).

1.4.3 Unauthorized Access

Unauthorized access occurs when an entity or individual receives or has access to Limited Access DMF information without authority. An unauthorized access is willful when it is a voluntary, intentional violation of a known legal duty.

Access to Limited Access DMF information should only be provided to individuals who require the data to perform their duties and as specified under the Act. DMF information must never be indiscriminately disseminated, even by a Certified Person. Certified Persons should evaluate the need for DMF information before the data is requested or disseminated.

An unauthorized disclosure has occurred when Limited Access DMF information is provided to an individual who does not have the statutory right to have access to it under the Act.

1.4.4 Unauthorized Disclosure

An unauthorized disclosure occurs when a Certified Person or an entity with authorization to receive Limited Access DMF information discloses it to another entity or individual who does not have authority, as defined in the Act.

1.4.5 Need to Know

Even if an entity or an individual has the authority to access Limited Access DMF information, a Certified Person should carefully consider whether that entity or individual should be given access to such information where such access is not necessary to perform his or her duties.

2   Limited Access DMF Information Authorized Use and Reviews

2.1   General

As a condition of receiving access to Limited Access DMF information from NTIS, a Certified Person must have shown, to the satisfaction of an Accredited Conformity Assessment Body (ACAB), the ability to protect the confidentiality of Limited Access DMF information. Safeguards must be implemented to prevent unauthorized access and use. A Certified Person must ensure its safeguards will be ready for implementation prior to receipt of Limited Access DMF information.

In any attestation or audit of a Person or Certified Person that will be submitted to NTIS under this part, an Accredited Conformity Assessment Body must attest that it is independent of that Person or Certified Person. The Accredited Conformity Assessment Body also must attest that it has read, understood, and agrees to the regulations in this part. The Accredited Conformity Assessment Body must also attest that it is accredited to a nationally or internationally recognized standard such as the ISO/IEC Standard 27006-2011 "Information technology—Security techniques—Requirements for bodies providing audit and certification of information security management systems," or any other similar nationally or internationally recognized standard for bodies providing audit and certification of information security management systems. The Accredited Conformity Assessment Body must also attest that the scope of its accreditation encompasses the safeguarding and security requirements as set forth in this part.

2.2   Authorized Use of Limited Access DMF information

In certifying Persons to have access to Limited Access DMF, NTIS considers whether the Certified Person's use is in conformance with the governing provisions allowing the access to Limited Access DMF information. The Certified Person must describe the purpose(s) for which the information is collected, used, maintained, and shared.

Any Certified Person that receives Limited Access DMF information for an authorized use may not use that information in any manner or for any purpose not consistent with that authorized use.

2.3   Obtaining Limited Access DMF information

NTIS has established a Secure Data Transfer (SDT) program to provide encrypted electronic transmission of Limited Access DMF information (referred to as "raw data DMF" information) between NTIS and a Certified Person. Information for establishing a raw data information feed is available on the NTIS Limited Access DMF website.

2.4   Coordinating Safeguards

Due to the diverse purposes for which authorized disclosures may be made to a Certified Person, Limited Access DMF information may be received and used by several quasi-independent units within the Certified Person's organizational structure. Where there is such a dispersal of Limited Access DMF information, the Certified Person should centralize safeguarding responsibilities to the greatest extent practical and establish and maintain uniform safeguard standards consistent with NTIS guidelines. The designee(s) assigned these responsibilities should hold a position high enough in the Certified Person's organizational structure to ensure compliance with the safeguard standards and procedures.

The selected designee(s) should also be responsible for ensuring that internal inspections are conducted, for submitting required safeguard information to independent third party auditors, and for properly reporting any data breach incidents to NTIS.

2.5   Periodic, Scheduled and Unscheduled Audits

As a condition of certification, a Certified Person agrees to be subject to periodic, scheduled and unscheduled audits of the systems, facilities, and procedures. The Limited Access DMF audit program is intended to ensure that a Certified Person has implemented security controls and procedures consistent with the guidelines provided in this publication.

2.5.1   Periodic Scheduled Audit Program

Limited Access DMF Certified Persons must have systems, facilities, and procedures in place to safeguard DMF information. Most Certified Persons will receive a periodic independent third party conformity assessment by an "Accredited Certification Body" to demonstrate mandatory or voluntary compliance with federal, industry or association information and systems security controls. NTIS will ordinarily accept audits conducted by an Accredited Certification Body. To ensure compliance with the controls to safeguard Limited Access DMF information, third party audits will generally meet the following requirements: (1) The auditor will submit a summary of the assessment results and an attestation that the results demonstrate that the Person has systems, facilities, and procedures in place to safeguard Limited Access information consistent, which may follow the guidelines provided in this publication; (2) The audit was performed within the preceding three years; (3) The auditor has been accredited by an appropriate third party accreditation organization to perform or attest to the audit results.

2.5.2   Unscheduled Audits

Unscheduled audits will generally be conducted by an Accredited Certification Body as described in the previous section. Several factors will be considered when determining the need for and the frequency of unscheduled audits.

Examples include reported system security breaches and attacks that indicate Limited Access DMF information has or may have been lost or stolen.

2.6   Conducting the Audit

Audits must be objective, impartial, and independent. Certified Persons are encouraged to discuss with NTIS their audit plan before initiating the audit to achieve compliance with the guidance in this publication. It is the responsibility of the Person seeking certification to identify and select an Accredited Certification Body that meets the qualifications as set forth in the applicable regulation, part 1110 of title 15 of the Code of Federal Regulations. NTIS does not maintain a list of approved third party auditors.

The auditor should conduct his/her assessment and attestation based on criteria such as the guidelines presented in the following sections of this document: (1) Information Secure Storage; (2) Restricting Access to Limited Access DMF Information; (3) Disposing of Limited Access DMF Information; and, (4) Information Security guidance, as described in sections four through seven of this document. After a third party auditor has completed the audit assessment, he/she will submit an audit attestation certificate that states whether or not a Person complies with an acceptable approach to safeguarding information, such as those set forth in this guideline

document. Additional sources to be considered include, but are not limited to, the Informative References of the "Framework for Improving Critical Infrastructure Cybersecurity" (Framework) published by the National Institute of Standards and Technology, and other approaches including Control Objectives for Information and Related Technology (COBIT), International Society of Automation (ISA), NIST's 800 series publications, and the Service Organization Controls (SOC) of the American Institute of CPAs (AICPA).

2.7   Violations, Fines and Revocation of Access

If the audit process determines that either a violation of Section 203, Limited Access DMF Final Rule, Non-Federal Subscriber Agreement, or Non-Federal Licensee Agreement for Use and Resale has occurred, the Certified Person may be subject to further audits, fines, and/or revocation of access to the Limited Access DMF. Section 1110.200 of title 15 of the Code of Federal Regulations sets out the penalties for unauthorized disclosures or uses of Limited Access DMF. Certified Persons can file an administrative appeal after receiving notice of denial, revocation, or imposition of penalties; additional information can be found in Section 1110.300 of title 15 of the Code of Federal Regulations.

3   Record Keeping Requirement

The Certified Person should consider retaining all information records and correspondence pertaining to Limited Access DMF applications, including all supporting documents and correspondence with the third party auditor, for a minimum of five (5) years.

Also, all information records and correspondence pertaining to Limited Access DMF audits, including internal, desk and field audits, should be maintained in the Certified Person's records management system for a minimum of five (5) years.

4   Limited Access DMF Information Secure Storage

4.1   General

Security for Limited Access DMF information may be provided for a document, an item, or an area in a number of ways. These include, but are not limited to, locked containers of various types, vaults, locked rooms, locked buildings, electronic security systems, identification systems, and control measures.

4.2   Restricted Area Access

Care should be taken to deny unauthorized access to areas containing Limited Access DMF information during duty and non-duty hours. This can be accomplished by creating restricted areas, security rooms, or locked rooms. Additionally, Limited Access DMF information in any form (computer printout, photocopies, tapes, notes) should be protected during non-duty hours. This can be done through a combination of methods, including secured or locked perimeter, secured area, or containerization.

A restricted area is an area where entry is restricted to authorized personnel (individuals assigned to the area). All restricted areas either should meet secured area criteria or provisions should be made to store Limited Access DMF information in appropriate containers during non-duty hours. Using restricted areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized access or disclosure or theft of Limited Access DMF information. All of the following procedures should be implemented to qualify as a restricted area.

Restricted areas will be prominently posted and separated from non-restricted areas by physical barriers that control access. The number of entrances should be kept to a minimum and should have controlled access (e.g., electronic access control, key access, door monitor) to prevent unauthorized entry. The main entrance should be controlled by locating the desk of a responsible employee at the entrance to ensure that only authorized personnel with an official need may enter.

A restricted area visitor log will be maintained at a designated entrance to the restricted area, and all visitors (persons not assigned to the area) entering the area should be directed to the designated entrance.

The visitor access log should require the visitor to provide the following information:

- Name and organization of the visitor
- Signature of the visitor
- Form of identification
- Date of access
- Time of entry and departure
- Purpose of visit
- Name and organization of person visited

The visitor should sign, either electronically or physically, into the visitor access log. The security personnel should validate the person's identify by examining government- issued identification (e.g., state driver's license or passport) and recording in the access log the type of identification validated. The security personnel should compare the name and signature entered in the access log with the name and signature of the government-issued identification. When leaving the area, the security personnel or escort should enter the visitor's time of departure.

Each restricted area access log should be closed out at the end of each month and reviewed by management.

Visitor Access Log							
Date	Name & Organization of Visitor	Form of Identification of Visitor	Purpose of Visit	Name & Organization of Person Visited	Time of Entry	Time of Departure	Signature of Visitor

Table 1 Sample Visitor Access Log

4.2.1 Use of Authorized Access List

To facilitate the entry of employees who have a frequent and continuing need to enter a restricted area, but who are not assigned to the area, an Authorized Access List (AAL) can be maintained so long as minimum protection standards are enforced.

Employees: The AAL should contain the following:

• Name of individual

• Certified Person name

• Name and phone number of Certified Person's POC

• Address of Certified Person POC

• Purpose for access

The AAL for employees should be updated at least annually or when employee access changes.

Vendors and Non-Certified Persons: The AAL should contain the following information:

• Name of contractor/subcontractor personnel or customer

• Name and phone number of Certified Person Point of Contact authorizing access

• Name and address of contractor/subcontractor/customer POC

• Address of contractor/subcontractor/customer

• Purpose and level of access Contractor/subcontractor/customer AAL should be updated monthly.

If there is any doubt of the identity of the individual, the security monitor should verify the identity of the individual against the AAL prior to allowing entry into the restricted area.

For additional guidance, see Section 7.3.11.1, Physical Access Authorizations (PE-2). Also, see Section 7.3.11.6, Delivery and Removal (PE-16), for guidance on controlling information system components entering and exiting the restricted area.

4.2.2 Controlling Access to Areas Containing Limited Access DMF information

Management or the designee should maintain an authorized list of all personnel who have access to information system areas, where these systems contain Limited Access DMF information. This shall not apply to those areas within the facility officially designated as publicly accessible.

The site should issue appropriate authorization credentials. The Certified Person can issue authorization credentials, including badges, identification cards, or smart cards. In addition, a list should be maintained that identifies those individuals who have authorized access to any systems where Limited Access DMF information is housed. Access authorizations and records maintained in electronic form are acceptable.

Allowing an individual to "piggyback" or "tailgate" into a restricted locations should be prohibited and documented in policy. The Certified Person should ensure that all individuals entering an area containing Limited Access DMF information do not bypass access controls or allow unauthorized entry of other individuals. Unauthorized access should be challenged by authorized individuals (e.g., those with access to Limited Access DMF information). Security personnel should be notified of unauthorized piggyback/tailgate attempts.

4.2.3 Control and Safeguarding Keys and Combinations

All containers, rooms, buildings, and facilities containing Limited Access DMF information should be locked when not in actual use.

Access to a locked area, room, or container can be controlled only if the key or combination is controlled. Compromising a combination or losing a key negates the security provided by that lock. Combinations to locks should be changed when an employee who knows the combination retires, terminates employment, and transfers to another position or at least annually.

Combinations and/or keys should be given only to those who have a need to have access to the area, room, or container and should never be written on a sticky-note, calendar pad, or any other item (even though it is carried on one's person or hidden from view). Inventory records should be maintained on keys and should account for the total keys available and keys issued. The inventory should account for master keys and key duplicates. Keys and combinations will be given only to those individuals who have a frequent need to access the area.

4.2.4 Locking Systems for Secured Areas

Access control systems (e.g., badge readers, smart cards, and biometrics) that provide the capability to audit access control attempts should maintain audit records with successful and failed access attempts to secure areas containing Limited Access DMF information or systems that process Limited Access DMF information. Certified Person personnel should review access control logs on a monthly basis. The access control log should contain the following elements:

•   Owner of the access control device requesting access

- Success/failure of the request

- Date and time of the request

4.3   Limited Access DMF Information in Transit

Handling Limited Access DMF information should be such that the documents do not become misplaced or available to unauthorized personnel. Any time Limited Access DMF information is transported from one location to another, care should be taken to provide appropriate safeguards. When Limited Access DMF information is hand-carried by an individual in connection with a trip or in the course of daily activities, it should be kept with that individual and protected from unauthorized disclosures.

All shipments of paper and electronic (including compact disk [CD], thumb drives, hard drives, tapes, and microfilm) Limited Access DMF information should be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. All Limited Access DMF information transported through the mail or courier/messenger service should be double-sealed; that is, one envelope within another envelope. The inner envelope should be marked "confidential" with some indication that only the designee or delegate is authorized to open it. Using sealed boxes serves the same purpose as double-sealing and prevents anyone from viewing the contents thereof.

4.4   Physical Security of Computers, Electronic, and Removable Media

Computers and electronic media that receive, process, store, or transmit Limited Access DMF information should be in a secure area with restricted access. In situations when requirements of a secure area with restricted access cannot be maintained, such as home work sites, remote terminals or other office work sites, the equipment should receive the highest level of protection practical, including full disk encryption. All computers and mobile devices that contain Limited Access DMF information and are resident in an alternate work site should employ encryption mechanisms to ensure that this data may not be accessed, if the computer is lost or stolen

Basic security requirements should be met, such as keeping Limited Access DMF information locked up when not in use. When removable media contains Limited Access DMF information, it should be labeled as Limited Access DMF information.

Inventory records of electronic media should be maintained and reviewed semi-annually for control and accountability; Section 3.0, Record Keeping Requirement contains additional information.

4.5   Media Off-Site Storage Requirements

If the Certified Person uses an off-site storage facility and the following conditions are met, the Certified Person is not subject to additional safeguard requirements:

• The media is encrypted.

• The media is locked in a turtle case.

• The Certified Person retains the key to the turtle case.

If the media is not encrypted and locked in a turtle case (e.g., open-shelf storage) or storage contractor maintains the key, the facility is subject to all safeguarding requirements (e.g., visitor access logs, internal inspections, contractor access restrictions, training)

4.6   Telework Locations

If the confidentiality of Limited Access DMF information can be adequately protected, telework sites, such as employee's homes or other non-traditional work, sites can be used. Limited Access DMF information remains subject to the same safeguard requirements and the highest level of attainable security. All of the requirements of Section 4.4, Physical Security of Computers, Electronic, and Removable Media, apply to telework locations.

The Certified Person should conduct periodic inspections of alternative work sites during the year to ensure that safeguards are adequate. The results of each inspection should be fully documented. The Certified Person understands that third party auditors will have the right to visit alternative work sites while conducting safeguard reviews.

4.6.1 Equipment
The Certified Person should retain ownership and control, for all hardware, software, and end-point equipment connecting to public communication networks, where these are resident at all alternate work sites.

Employees should have a specific room or area in a room that has the appropriate space and facilities for the type of work done. The Certified Person should give employees locking file cabinets or desk drawers so that Limited Access DMF information may be properly secured when not in use. Therefore adequate means of storage should exist at the work site(s).

4.6.2 Storing Data
Limited Access DMF information may be stored on hard disks only if approved security access control devices (hardware/software) have been installed; are receiving regularly scheduled maintenance, including upgrades; and are being used. Access control should include password security, an audit trail, encryption, virus detection, and data overwriting capabilities.

4.6.3 Other Safeguards
Electronic media that is to be reused should have files overwritten or degaussed.

The Certified Person should maintain a policy for the security of alternative work sites. The Certified Person should test coordination with the managing host system(s) and any networks and

maintain documentation on the test. Before implementation, the Certified Person will certify that the security controls are adequate for security needs. Additionally, the Certified Person's will promulgate rules and procedures to ensure that employees do not leave computers unprotected at any time. These rules should address brief absences while employees are away from the computer.

Certified Person's should provide specialized training in security, disclosure awareness, and ethics for all participating employees and managers. This training should cover situations that could occur as the result of an interruption of work by family, friends, or other sources.

5   Restricting Access to Limited Access DMF Information

5.1   General

Limited Access DMF subscribers and licensees receiving Limited Access DMF should provide other safeguard measures, as appropriate, to ensure the confidentiality of the Limited Access DMF information. Limited Access DMF subscribers and licensees should provide a training program for their employees and contractors.

5.2   Training Requirements

Education and awareness are necessary to provide employees, contractors, subcontractors and other persons with the information to protect Limited Access DMF information. There are multiple components to a successful training program. In this section, training requirements are consolidated to ensure Limited Access DMF information users understand the guidance provided in this publication.

5.3   Disclosure Awareness Training

Prior to granting an Certified Person's employee or contractor access to Limited Access DMF information, each employee or contractor should certify his or her understanding of the security policy and procedures for safeguarding Limited Access DMF information.

Employees and contractors should maintain their authorization to access Limited Access DMF information through annual training and recertification.

Disclosure awareness training stipulates that:

• The training provided before the initial certification and annually thereafter should also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches (see Section 8.0, Reporting Improper Inspections or Disclosures).

• During this training, the Certified Person should make employees aware that disclosure restrictions and penalties under the regulation will apply even after employment with the Certified Person has ended.

- For both the initial certification and the annual renewal of certification, the employee or contractor should sign, either with ink or electronic signature, a confidentiality statement certifying his or her understanding of the security requirements. The initial certification and recertification should be documented and placed in the Certified Person's files for review and retained for at least five years.

5.4   Internal Inspections

NTIS recommends that internal inspections by subscribers and licensees of Limited Access DMF information take place. The purpose is to ensure that adequate safeguards and security measures for Limited Access DMF information have been maintained.

To provide reasonable assurance that Limited Access DMF information is adequately safeguarded, the self-inspection should address the safeguard guidelines reflected in this document. The Limited Access DMF subscriber and licensee should monitor and audit privacy controls and internal privacy policies to ensure effective implementation.

Below is a recommended review cycle for Limited Access DMF subscribers and licensees:

- Local offices receiving Limited Access DMF information: at least every two years

- Facilities housing Limited Access DMF information and the Certified Person's computer facility: at least every twelve (12) months

- All contractors and subcontractors with access to Limited Access information, including a consolidated data center or off-site storage facility: at least every twelve (12) months

If the inspection is conducted, then inspection reports, including a record of corrective actions, should be retained by the Certified Person for a minimum of five years from the date the inspection was completed. NTIS personnel and/or an independent third party auditor may review these reports, if available, in the course of a safeguard review.

6   Disposing of Limited Access DMF Information

6.1   General

Users of Limited Access DMF information are required to take archival and/or disposal actions after using Limited Access DMF information to protect its confidentiality.

6.2   Disposing of Limited Access DMF Information at End of Subscription

Certified Persons are NOT required to return Limited Access DMF information files to NTIS if the subscription is terminated. However, if the Certified Person continues to use the Limited Access DMF information file, it will agree to comply with all guidance set forth in this document and the subscription and license agreements for a minimum of three (3) years from the date of the

last subscription update. This requirement is to ensure that Limited Access DMF information is not released to non-DMF-certified persons within the three (3) years following the last update.

If the Certified Person will not continue use of Limited Access DMF information after ending its subscription, NTIS recommends that the Certified Person destroy or archive the Limited Access DMF information to ensure that it is not accessible for the three (3) year non-disclosure period.

It should be appreciated that a Certified Person's decision to end a subscription, or not to renew a certification, will not affect the obligations undertaken by the Certified Person under 15 CFR Part 1110 in accepting Limited Access DMF.

6.3   Destruction and Disposal

Limited Access DMF information furnished to the user and any paper material generated therefrom, such as copies, photographs, computer printouts, notes, and work papers, will be destroyed using a method that makes the Limited Access DMF information unreadable or unusable.

Limited Access DMF information furnished or stored in electronic format should be destroyed in the following manner:

•   Electronic media (e.g., hard drives, tapes, CDs, and flash media) will be destroyed according to guidance in Section 7.3.10.6, Media Sanitization (MP-6). Electronic media containing Limited Access DMF information will not be made available for reuse by other offices or released for destruction without first being subjected to electromagnetic erasing.

•   Whenever physical media leaves the physical or systemic control of the Certified Person for maintenance, exchange, or other servicing, any Limited Access DMF information on it should be destroyed, completely overwriting all data rendering it unrecoverable. If the information cannot be destroyed, the disk will be damaged in an obvious manner to prevent use in any disk drive unit and discarded.

7   Information Security

7.1   General

This section details the computer security requirements organizations should meet to adequately protect Limited Access DMF information under their administrative control. While NTIS has responsibility to ensure the protection of Limited Access DMF information, it is the responsibility of each Limited Access DMF certified organization to build in effective security controls into its own Information Systems to ensure that Limited Access DMF information is protected at all points where it is received, processed, stored, or transmitted. It will not be the intent of NTIS to monitor

each control identified, but to provide these to the organization, identifying those controls required for the protection of Limited Access DMF information.

All information systems used for receiving, processing, storing, or transmitting Limited Access DMF information should be hardened in accordance with the requirements in this publication. These requirements apply to equipment, facilities, and people that collect, process, store, display, and disseminate Limited Access DMF information. This includes computers, hardware, software, and communications, as well as policies and procedures for their use.

These information security guidelines are derived from NIST SP800- 53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. Only NIST SP 800-53 controls believed to be essential to the protection of Limited Access DMF information are included in this publication as a baseline. Applicability was determined by selecting controls relevant to protecting the confidentiality of Limited Access DMF information. The NIST controls are intended by NTIS to be illustrative, not exclusive. Other controls that can be assessed and used as guidelines include the NIST Framework for Improving Critical Infrastructure Cybersecurity v1.0. The Framework Core provides a common set of activities for managing risks, and associated controls. The references provided in the Framework Core represent a diverse set of information security guidelines including: International Organization for Standardization ISO 27001; International Society for Automation ISA/IEC 62443; Control Objectives for Information and Related Technology COBIT; Council on Cybersecurity Critical Security Controls CCS CSC2; and NIST 800-53 rev. 4. Again, these references are illustrative.

7.2   Assessment Process

A Certified Person's compliance with the computer security requirements identified in this publication will be subject to periodic and unscheduled audits. To ensure a standardized assessment process, desk and/or field audit techniques may be used to evaluate the Certified Person's compliance with security requirements to protect Limited Access DMF information from unauthorized disclosure.

7.3   Information Security Control Requirements

7.3.1   Access Control

7.3.1.1   Access Control Policy and Procedures (AC-1)

    a.   The Certified Person will develop, document, and disseminate:
        1.   An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        2.   Procedures to facilitate the implementation of the access control policy and associated access controls; and
        3.   Review and update the current: 1. Access control policy every three years (or if there is a significant change); and 2. Access control procedures at least annually.

7.3.1.2 Account Management (AC-2)

The Certified Person will:

    a. Identify and select the accounts with access to Limited Access DMF information to support missions/business functions;
    b. Assign account managers for information system accounts;
    c. Establish conditions for group and role membership;
    d. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
    e. Require approval for requests to create information system accounts;
    f. Create, enable, modify, disable, and remove information system accounts in accordance with documented account management procedures;
    g. Monitor the use of information system accounts;
    h. Notify account managers when accounts are no longer required, when users are terminated or transferred, or when individual information system usage or need- to-know permission changes;
    i. Authorize access to information systems that receive, process, store, or transmit Limited Access DMF information based on a valid access authorization, need-to-know permission, and under the authority to re- disclosed Limited Access DMF information under the provisions of this publication;
    j. Review accounts for compliance with account management requirements at a minimum of annually for user accounts and semi-annually for privileged accounts; and
    k. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

7.3.1.3 Access Enforcement (AC-3)

The information system will enforce:

    a. Approved authorizations for logical access to information and system resources in accordance with applicable access control policies; and
    b. A role-based access control policy over defined subjects and objects and controls access to Limited Access DMF information based upon a valid access authorization, intended system usage, and the authority to be disclose Limited Access DMF information under the provisions of this publication.

7.3.1.4 Information Flow Enforcement (AC-4)

The information system will enforce approved authorizations for controlling the flow of Limited Access DMF information within the system and between interconnected systems based on the technical safeguards in place to protect the Limited Access DMF information.

7.3.1.5 Separation of Duties (AC-5)

The Certified Person will:

    a. Separate duties of individuals to prevent harmful activity without collusion;
    b. Document separation of duties of individuals; and

c.   Define information system access authorizations to support separation of duties.

7.3.1.6 Least Privilege (AC-6)

The Certified Person will:

a.   Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with mission and business functions;

b.   Explicitly authorize access to Limited Access DMF information

c.   Restrict privileged accounts on the information system to a limited number of individuals with a need to perform administrative duties

d.   Prevent non-privileged users from executing privileged functions; including disabling, circumventing, or altering implemented security safeguards/countermeasures.

7.3.1.7 Remote Access (AC-17)

Remote access is defined as access to an information system by a user communicating through an external network, for example, the Internet.

The Certified Person will:

a.   Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed;

b.   Authorize remote access to the information system prior to allowing such connections; and

The information system will:

a.   Monitor and control remote access methods

b.   Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions where Limited Access DMF information is transmitted over the remote connection; and

7.3.1.8 Wireless Access (AC-18)

The Certified Person will:

a.   Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and,

b.   Authorize wireless access to the information system prior to allowing such connections.

The information system will protect wireless access to the system using authentication and encryption.

7.3.1.9 Access Control for Mobile Devices (AC-19)

A mobile device is defined as a computing device that (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable, or removable data storage; and (iv) includes a self-contained power source.

The Certified Person will:

    a.   Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for mobile devices;

    b.   Authorize the connection of mobile devices to information systems; and,

    c.   Employ encryption to protect the Limited Access DMF information on mobile devices (e.g., smartphones and laptop computers).

7.3.1.10   Use of External Information Systems (AC-20)

External information systems include any technology used to receive, process, transmit, or store Limited Access DMF information that is not owned and managed by the Certified Person.

Unless approved by NTIS, in writing, the Certified Person will prohibit:

    a.   Access to Limited Access DMF information from unauthorized external information systems;

    b.   Portable storage devices (e.g., flash drives, external hard drives) containing Limited Access DMF information from being used with external information systems; and

    c.   Use of non-entity-owned information systems; system components; or devices to process, store, or transmit Limited Access DMF information.

7.3.1.11   Information Sharing (AC-21)

The Certified Person will restrict the sharing/re-disclosure of Limited Access DMF information in accordance with 15 CFR Part 1110.

7.3.1.12   Publicly Accessible Content (AC-22)

The Certified Person will:

    a.   Designate individuals authorized to post information onto a publicly accessible information system;

    b.   Train authorized individuals to ensure that publicly accessible information does not contain Limited Access DMF information;

    c.   Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that Limited Access DMF information is not included; and,

    d.   Review the content on the publicly accessible information system for Limited Access DMF information, at a minimum, quarterly and remove such information, if discovered.

7.3.2 Awareness and Training

7.3.2.1 Security Awareness and Training Policy and Procedures (AT-1)

The Certified Person will:

 a.   Develop, document, and disseminate:

1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and,
2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and

b.   Review and update the current:

1. Security awareness and training policy every three years (or when significant changes occur); and,
2. Security awareness and training procedures at least annually.

7.3.2.2 Security Awareness Training (AT-2)
The Certified Person will:

a. Provide basic security awareness training to information system users (including managers, senior executives, and contractors):
    1. As part of initial training for new users;
    2. When required by information system changes; and
    3. At least annually thereafter.
b. Include security awareness training on recognizing and reporting potential indicators of insider threat, which could include the unauthorized access or re-disclosure of Limited Access DMF information.

7.3.2.3 Role-Based Security Training (AT-3)
The Certified Person will provide role-based security training to personnel with assigned security roles and responsibilities:

a.   Before authorizing access to the information system or performing assigned duties that require access to Limited Access DMF information;
b.   When required by information system changes; and,
c.   At least annually thereafter.

7.3.2.4 Security Training Records (AT-4)
The Certified Person will:

a.   Document and monitor individual information system security training activities, including basic security awareness training and specific information system security training; and,
b.   Retain individual training records for a period of five years.

7.3.3 Audit and Accountability
7.3.3.1 Audit Review, Analysis, and Reporting (AU-6)
The Certified Person will:

a.   Review and analyze information system audit records for indications of unusual activity related to potential unauthorized Limited Access DMF information access; and,

b.   Report findings according to the Certified Person's incident response policy. If the finding involves a potential unauthorized disclosure of Limited Access DMF information, the incident will be reported to NTIS as described in Section 8.0, Reporting Improper Inspections or Disclosures.

7.3.3.2 Audit Record Retention (AU-11)

The Certified Person retains audit records for five years to provide support for after-the-fact investigations of security incidents.

7.3.3.3 Monitoring For Information Disclosure (AU-13)

The Certified Person monitors for evidence of unauthorized disclosure of Limited Access DMF information and reports such incidents to NTIS as described in Section 8.0, Reporting Improper Inspections or Disclosures.

7.3.4   Security Assessment and Authorization

7.3.4.1 System Interconnections (CA-3)

The Certified Person will:

a.   Authorize connections through the use of Interconnection Security Agreements; between external information systems and internal information system that receive, process, store, or transmit Limited Access DMF information; and

b.   Review and update system interconnection agreements on an annual basis or when changes occur.

7.3.4.2 Penetration Testing (CA-8)

The Certified Person conducts penetration testing periodically on systems or system components that contain Limited Access DMF information to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills).

7.3.5   Configuration Management

7.3.5.1 Configuration Change Control (CM-3)

The Certified Person will:

a.   Determine the types of changes to the information system that are configuration-controlled;

b.   Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses;

c.   Test, validate, and document changes to the information system before implementing the changes on the operational system.

7.3.5.2 Access Restrictions for Change (CM-5)

The Certified Person will define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

7.3.5.3 Configuration Settings (CM-6)

The Certified Person will:

    a.   Establish, implement, and document configuration settings for IT products that receive, process, store, or transmit Limited Access DMF information;

    b.   Identify, document, and approve any deviations from established configuration settings for information systems that receive, process, store, or transmit Limited Access DMF information; and,

    c.   Monitor and control changes to the configuration settings in accordance with policies and procedures.

7.3.5.4 Information System Component Inventory (CM-8)

The Certified Person will:

    a.   Develop and document an inventory of information system components that:
   1. Accurately reflects the current information system;
   2. Includes all components that store, process, or transmit Limited Access DMF information;
   3. Is at the level of granularity deemed necessary for tracking and reporting; and,
   4. Includes information deemed necessary to achieve effective information system component accountability; and,

    b.   Review and update the information system component inventory through periodic manual inventory checks or a network monitoring tool that automatically
   1. maintains the inventory; and,
   2. Update the inventory of information system components as an integral part of component installations, removals, and information system updates.

7.3.5.5 User-Installed Software (CM-11)

The Certified Person will:

    a.   Establish policies governing the installation of software by users;

    b.   Enforce software installation policies; and,

    c.   Monitor policy compliance on a continual basis.

7.3.6 Identification and Authentication

7.3.6.1 Identification and Authentication (Users) (IA-2)

The information system will:

    a.   Uniquely identify and authenticate authorized users (or processes acting on behalf of authorized users); and

b. Implement authentication for all remote network access to privileged and non-privileged accounts for information systems that receive, process, store, or transmit Limited Access DMF information.

7.3.6.2 Device Identification and Authentication (IA-3)

The information system will uniquely identify and authenticate devices before establishing a connection.

7.3.6.3 Identifier Management (IA-4)

The Certified Person will manage information system identifiers by:

a. Receiving authorization from designated Certified Person officials to assign an individual, group, role, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, or device; and,
c. Assigning the identifier to the intended individual, group, role, or device;

7.3.6.4 Authenticator Management (Passwords) (IA-5)

The Certified Person will manage information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e. Changing default content of authenticators prior to information system installation;
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
g. Changing/refreshing authenticators;
h. Protecting authenticator content from unauthorized disclosure and modification;
i. Requiring individuals to take specific security safeguards to protect authenticators; and,
j. Changing authenticators for group/role accounts when membership to those accounts changes.

7.3.6.5 Identification and Authentication (Non-Organizational Users) (IA- 8)

The information system will uniquely identify and authenticate non- Certified Person users (or processes acting on behalf of non- Certified Person users).

7.3.7 Incident Response

Incident response controls apply to both physical and information system security relative to the protection of Limited Access DMF information.

7.3.7.1 Incident Response Policy and Procedures (IR-1)

a. The Certified Person will develop, document, and disseminate to designated Certified Person officials:

      1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Certified Person entities, and compliance; and,

      2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls.

   b. Review and update the current:

      1. Incident response policy every three years; and,

      2. Incident response procedures at least annually.

7.3.7.2 Incident Monitoring (IR-5)

The Certified Person will track and document all physical and information system security incidents potentially affecting the confidentiality of Limited Access DMF information.

7.3.7.3 Incident Reporting (IR-6)

Refer to Section 8.0, Reporting Improper Inspections or Disclosures, for more information on incident reporting.

7.3.8 Maintenance

7.3.8.1 Controlled Maintenance (MA-2)

The Certified Person will:

a. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

b. Require that designated Certified Person officials explicitly approve the removal of the information system or system components from Certified Person facilities for off-site maintenance or repairs;

c. Sanitize equipment to remove all Limited Access DMF information from associated media prior to removal from Certified Person's facilities for off-site maintenance or repairs; and,

d. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions and update maintenance records accordingly.

7.3.8.2 Non-Local Maintenance (remote maintenance) (MA-4)

The Certified Person will:

a. Approve and monitor non-local maintenance and diagnostic activities;

b. Allow the use of non-local maintenance and diagnostic tools and documented in the security plan for the information system;

c. Maintain records for non-local maintenance and diagnostic activities;

d. Terminate session and network connections when non- local maintenance is completed; and,

e. Document policies and procedures for the establishment and use of non-local maintenance and diagnostic connections.

7.3.8.3 Maintenance Personnel (MA-5)

The Certified Person will:

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

b. Ensure that non-escorted personnel performing maintenance on the information system have required access authorizations; and,

c. Designate personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

7.3.9 Media Protection

Information system media is defined to include both digital and non- digital media.

7.3.9.1 Media Protection Policy and Procedures (MP-1)

The Certified Person will:

a. Develop, document, and disseminate to designated Certified Person officials:
    1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among entities, and compliance; and,
    2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls.

b. Review and update the current:
    1. Media protection policy every three years; and,
    2. Media protection procedures at least annually.

7.3.9.2 Media Access (MP-2)

The Certified Person will restrict access to digital and non- digital media containing Limited Access DMF information to authorized individuals.

7.3.9.3 Media Marking (MP-3)

The Certified Person will label information system media containing Limited Access DMF information to indicate the distribution limitations and handling caveats.

7.3.9.4 Media Storage (MP-4)

The Certified Person will:

a. Physically control and securely store media containing Limited Access DMF information; and,

b. Protect information system media until the media is destroyed or sanitized using approved equipment, techniques, and procedures.

7.3.9.5 Media Transport (MP-5)

The Certified Person will:

a. Protect and control digital (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, DVDs) and non-digital (e.g., paper) media during transport outside of controlled areas;

b. Maintain accountability for information system media during transport outside of controlled areas;

c. Restrict the activities associated with the transport of information system media to authorized personnel; and,

d. Implement cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

7.3.9.6 Media Sanitization (MP-6)

The Certified Person will:

a. Sanitize media containing Limited Access DMF information prior to disposal, release out of Certified Person's control, or release for reuse in accordance with applicable regulations, standards and policies; and,

b. Review, approve, track, document, and verify media sanitization and disposal actions.

7.3.10 Physical and Environmental Protection

7.3.10.1   Physical Access Authorizations (PE-2)

The Certified Person will:

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the information system resides;

b. Review the access list detailing authorized facility access by individuals, at least annually;

c. Remove individuals from the facility access list when access is no longer required; and,

d. Enforce physical access authorizations to the information system in addition to the physical access controls for the facility at spaces where Limited Access DMF information is received, processed, stored, or transmitted.

7.3.10.2   Physical Access Control (PE-3)

The Certified Person will:

a. Enforce physical access authorizations at entry/exit points to facilities where the information systems that receive, process, store, or transmit Limited Access DMF information reside by:
   1. Verifying individual access authorizations before granting access to the facility; and,
   2. Controlling ingress/egress to the facility using physical access control systems/devices or guards.

b. Escort visitors and monitor visitor activity;

c. Secure keys, combinations, and other physical access devices;

d. Inventory physical access devices; and,

e. Change combinations and keys when an employee who knows the combination retires, terminates employment, or transfers to another position or at least annually.

7.3.10.3 Access Control for Transmission Medium (cabling & network hardware) (PE-4)

The Certified Person will control physical access within Certified Person's facilities.

7.3.10.4 Access Control for Output Devices (PE-5)

The Certified Person will control physical access to information system output devices (e.g., monitors, printers, copiers, scanners, fax machines, and audio devices) to prevent unauthorized individuals from obtaining the output.

7.3.10.5 Monitoring Physical Access (PE-6)

The Certified Person will:

a. Monitor physical access to the facility where the information system resides to detect and respond to physical security incidents;
b. Coordinate results of reviews and investigations; and
c. Monitor physical intrusion alarms and surveillance equipment.

7.3.10.6 Delivery and Removal (PE-16)

The Certified Person will authorize, monitor, and control information system components entering and exiting the facility and maintain records of those items.

7.3.11 Planning

7.3.11.1 Rules of Behavior (PL-4)

The Certified Person will:

a. Establish and make readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
b. Receive a signed acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
c. Review and update the rules of behavior;
d. Require individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated; and,
e. Include in the rules of behavior, explicit restrictions for posting Limited Access DMF information on public websites.

7.3.12 Personnel Security

7.3.12.1 Personnel Screening (PS-3)

The Certified Person will:

a. Screen individuals prior to authorizing access to the information system; and,
b. Rescreen individuals according to defined conditions requiring rescreening.

7.3.12.2   Termination (PS-4)

The Certified Person, upon termination of individual employment will disable the individual's access to Limited Access DMF information.

7.3.12.3   Personnel Transfer (PS-5)

The Certified Person will:

a. Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
b. Initiate transfer or reassignment actions following the formal transfer action;
c. Modify access authorizations as needed to correspond with any changes in operational need due to reassignment or transfer; and,
d. Notify designated personnel, as required.

7.3.12.4   Third-Party Personnel Security (PS-7)

The Certified Person will:

a. Establish personnel security requirements, including security roles and responsibilities for third-party providers;
b. Require third-party providers to comply with established personnel security policies and procedures;
c. Document personnel security requirements;
d. Require third-party providers to notify the Certified Person of any personnel transfers or terminations of third-party personnel who possess credentials or badges or who have information system privileges; and,
e. Monitor provider compliance.

7.3.13 Risk Assessment

7.3.13.1   Risk Assessment (RA-3)

The Certified Person will:

a. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Document risk assessment results in a risk assessment report;
c. Review risk assessment results at least annually;
d. Disseminate risk assessment results to designated Certified Person officials; and
e. Review the risk assessment report at least every three years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities) or other conditions that may impact the security state of the system.

7.3.13.2   Vulnerability Scanning (RA-5)

The Certified Person will:

a. Scan for vulnerabilities in the information system and hosted applications at a minimum of monthly for all systems and when new vulnerabilities potentially affecting the system/applications are identified and reported;
b. Analyze vulnerability scan reports and results from security control assessments; and,
c. Remediate legitimate vulnerabilities in accordance with an assessment of risk.

7.3.14 System and Services Acquisition

7.3.14.1   External Information System Services (SA-9)

The Certified Person requires that providers of external information system services comply with organizational information security requirements and employ security controls in accordance with applicable federal laws, policies, regulations, standards, and guidance.

External service providers that are processing, storing, or transmitting Limited Access DMF information or operating information systems on behalf of the organization ensure that such providers meet the same security requirements that the Certified Person is required to meet.

7.3.14.2   Developer Security Testing and Evaluation (SA-11)

The Certified Person will require the developer of the information system, system component, or information system service to comply with the same security requirements that the organization is required to meet

a. Create and implement a security assessment plan;
b. Perform security testing/evaluation;
c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
d. Implement a verifiable flaw remediation process; and,
e. Correct flaws identified during security testing/evaluation.

7.3.15 System and Communications Protection

7.3.15.1   Boundary Protection (SC-7)

The information system will:

a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; and,
b. Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with your security architecture requirements.

The Certified Person will limit the number of external network connections to the information system.

a. Establish a traffic flow policy for each external connection;
b. Protect the confidentiality of the information being transmitted across each external connection.

7.3.15.2   Transmission Confidentiality and Integrity (SC-8)

Information systems that receive, process, store, or transmit Limited Access DMF information, will:

a. Protect the confidentiality of transmitted information.
b. Implement cryptographic mechanisms to prevent unauthorized disclosure of Limited Access DMF information during transmission between external systems.

7.3.15.3   Protection of Information at Rest (SC-28)

The information system will protect the confidentiality of Limited Access DMF information at rest. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems.

7.3.16 System and Information Integrity

7.3.16.1   Flaw Remediation (SI-2)

The Certified Person will:

a. Identify and correct information system security flaws; and,
b. Install security-relevant software and firmware updates based on severity and associated risk to the confidentiality of Limited Access DMF information.

Security-relevant software updates include, for example, patches, service packs, hot fixes, and antivirus signatures.

7.3.16.2   Malicious Code Protection (SI-3)

The Certified Person will:

a. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
b. Update malicious code protection mechanisms whenever new releases are available in accordance with the Certified Person's configuration management policy and procedures; and,
c. Configure malicious code protection mechanisms to:
    1 Perform periodic scans and real-time scans of files from external sources at endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with security policy; and,
    2 Either block or quarantine malicious code and send an alert to the administrator in response to malicious code detection; and

7.3.16.3   Information System Monitoring (SI-4)

The Certified Person will:

a. Monitor the information system to detect:
    1. Attacks and indicators of potential attacks; and
    2. Unauthorized local, network, and remote connections.
b. Identify unauthorized use of the information system; and,

c. Heighten the level of information system monitoring activity whenever there is an indication of increased risk based on credible sources of information;

The information system will:

a. Monitor inbound and outbound communications for unusual or unauthorized activities or conditions.
b. Alert designated Certified Person officials of detected suspicious events occur.

7.3.16.4   Security Alerts, Advisories, and Directives (SI-5)
The Certified Person will:

a. Receive information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;
b. Generate internal security alerts, advisories, and directives as deemed necessary;
c. Disseminate security alerts, advisories, and directives to designated Certified Person officials; and,
d. Implement security directives in accordance with established time frames or notify NTIS of the degree of noncompliance.

7.3.16.5   Software, Firmware, and Information Integrity (SI-7)
The Certified Person will employ integrity verification tools to detect unauthorized changes to software, firmware, and information.

7.3.17 Program Management
7.3.17.1   Information Security Program Plan (PM-1)
The Certified Person will develop and disseminate an organization- wide information security program plan that:

a. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
b. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
c. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and,
d. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations.

The Certified Person will:

a. Review the organization-wide information security program plan periodically; and,
b. Update the plan to address organizational changes and problems identified during plan implementation or security control assessments.

7.3.17.2   Senior Information Security Officer (PM-2)

The Certified Person will appoint an individual with the mission and resources to coordinate, develop, implement, and maintain the organizations information security program.

8   Reporting Improper Use or Disclosures

8.1   General

Upon discovering a possible improper use or disclosure of Limited Access DMF information, including breaches and security incidents, the Certified Person is required to notify NTIS within 3 hours after discovery. This notification will occur even if it is outside normal NTIS business hours.

8.2   Office of Safeguards Notification Process

To notify NTIS, the Certified Person will document the specifics of the incident known at that time into a data incident report, including but not limited to:

- Name of Certified Person and Certified Person Point of Contact for resolving data incident with contact information;
- Date and time of the incident;
- Date and time the incident was discovered;
- How the incident was discovered;
- Description of the incident and the data involved, including specific data elements, if known;
- Potential number of Limited Access DMF information records involved; if unknown, provide a range if possible;
- Address where the incident occurred; and,
- Information Technology involved (e.g., laptop, server, mainframe).
- Do not include any Limited Access DMF information in the data Incident report.
- Reports should be sent electronically and encrypted via NTIS-approved encryption techniques. Use the term data incident report in the subject line of the email.

The Certified Person will cooperate with NTIS, providing data and access as needed to determine the facts and circumstances of the incident.

8.3   Incident Response Procedures

The Certified Person should not wait to conduct an internal investigation to determine if Limited Access DMF information was involved in an unauthorized use, disclosure or data breach. If Limited Access DMF information may have been involved, the Certified Person should contact NTIS immediately. The Certified Person will cooperate with NTIS and, as appropriate, federal

investigators, providing data and access as needed to determine the facts and circumstances of the incident.

NTIS will coordinate with the Certified Person regarding appropriate follow- up actions required to be taken by the Certified Person to ensure continued protection of Limited Access DMF information. Once the incident has been addressed, the Certified Person will conduct a post-incident review to ensure the incident response policies and procedures provide adequate guidance.

9   Glossary and Key Terms

> **A**

Accountability. A process of holding users responsible for actions performed on an information system.

Accredited Conformity Assessment Body. A third party conformity assessment body that is accredited by an accreditation body under nationally or internationally recognized criteria such as, but not limited to, ISO/IEC 27006-2011, "Information technology—Security techniques—Requirements for bodies providing audit and certification of information security management systems," to attest that a Person or Certified Person has systems, facilities and procedures in place to safeguard Limited Access DMF.

Adequate security. Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, unauthorized access to, or modification of information.

Alternative work site. Any working area that is attached to the wide area network either through a public switched data network or through the Internet.

Assurance. A measure of confidence that management, operational and technical controls are operating as intended and achieving the security requirements for the system.

Assurance testing. A process used to determine if security features of a system are implemented as designed, and are adequate for the proposed operating environment. This process may include hands-on functional testing, penetration testing, and/or verification.

Audit. An independent examination of security controls associated with a representative subset of organizational information systems to determine the operating effectiveness of system controls; to ensure compliance with established policy and operational procedures; and to recommend changes in controls, policy, or procedures where needed.

Audit trail. A chronological record of system activities sufficient to enable the reconstruction, review, and examination of security events related to an operation, procedure, or event in a transaction from its inception to final results.

Authentication. Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system; see Identification.

Authorization. Access privileges granted to a user, program, or process.

Availability. Timely, reliable access to information and information services for authorized users.

B

Baseline security requirements. A description of the minimum security requirements necessary for an information system to enforce the security policy and maintain an acceptable risk level.

Blurring. The act of obscuring data so that it cannot be read or reconstructed.

C

Classified. National security information classified pursuant to Executive Order 12958.

Compromise. The disclosure of sensitive information to persons not authorized to receive such information.

Comingling. The presence of Limited Access DMF information and non-Limited Access DMF information data together on the same paper or electronic media.

Confidentiality. The preservation of authorized restrictions on information access and disclosure.

Configuration management. A structured process of managing and controlling changes to hardware, software, firmware, communications, and documentation throughout the system development life cycle.

Container. An object that can be used to hold or transport something. Containerize. To package (freight) in uniform, sealed containers for shipment. Control number. A code that identifies a unique document or record.

Control schedule. A record retention and disposal schedule established by the Certified Person.

Corrective Action Plan (CAP). A report required to be filed semi-annually, detailing the Certified Person's planned and completed actions to resolve findings identified during an NTIS safeguard review.

Countermeasure. Action, device, procedure, mechanism, technique, or other measure that reduces the vulnerability of an information system.

Cryptography. The process of rendering plain text information unreadable and restoring such unreadable information to a readable form.

D

Data. A representation of facts, concepts, information, or instruction suitable for communication, processing, or interpretation by people or information systems.

Decryption. The process of converting encrypted information into a readable form. This term is also referred to as deciphering.

Degauss. To erase information electromagnetically from a magnetic disk or other storage device.

Digital subscription line. A public telecommunications technology that delivers high bandwidth over conventional copper wire that covers limited distances.

Discretionary access control. A method of restricting logical access to information system objects (e.g., files, directories, devices, permissions, rules) based on the identity and need-to-know of users, groups, or processes.

E

Encryption. See Cryptography.

Encryption algorithm. A formula used to convert information into an unreadable format.

Enterprise life cycle. A robust methodology used to implement business change and information technology modernization.

External network. Any network that resides outside the security perimeter established by the telecommunications system.

Extranet. A private data network that uses the public telephone network to establish a secure communications medium among authorized users (e.g., organization, vendors, and business partners). An Extranet extends a private network (often referred to as an Intranet) to external parties in cases in which all parties may benefit from the exchange of information quickly and privately.

Exchange. An online marketplace in which individuals and small businesses can compare policies and buy insurance (with a government subsidy, if eligible).

F

File permission. A method of implementing discretionary access control by establishing and enforcing rules to restrict logical access of information system resources to authorized users and processes.

File server. A local area network computer dedicated to providing files and data storage to other network stations.

Firewall. Telecommunication device used to regulate logical access authorities between network systems.

Firmware. Microcode programming instructions permanently embedded into the read- only memory control block of a computer system. Firmware is a machine component of computer system, similar to a computer circuit component.

G

Gateway. An interface that provides compatibility between heterogeneous networks by converting transmission speeds, protocols, codes, or security rules. This interface is sometimes referred to as a protocol converter.

H

Host. A computer dedicated to providing services to many users. Examples of such systems include mainframes, minicomputers, or servers that provide dynamic host configuration protocol services.

I

Identification. A mechanism used to request access to system resources by providing a recognizable unique form of identification such as a Login ID, User ID, or token; see Authentication.

Information. See Data.

Information system. A collection of computer hardware, software, firmware, applications, information, communications, and personnel organized to accomplish a specific function or set of functions under direct management control.

Information system security. The protection of information systems and information against unauthorized access, use modification, or disclosure to ensure the confidentiality, integrity, and availability of information systems and information.

Integrity. The protection of information systems and information from unauthorized modification to ensure the quality, accuracy, completeness, nonrepudiation, and authenticity of information.

Internet. Two or more networks connected by a router; the world's largest network, it uses TCP/IP to connect government, university, and commercial institutions.

Intranet. A private network that uses TCP/IP, the Internet, and World Wide Web technologies to share information quickly and privately between authorized user communities, including organizations, vendors, and business partners.

K

Key. Information used to establish and periodically change the operations performed in cryptographic devices for the purpose of encrypting and decrypting information.

L

Least privilege. A security principle under which users or processes are assigned the most restrictive set of privileges necessary to perform routine job responsibilities.

M

Management controls. Security controls focused on managing organizational risk and information system security and devising sufficient countermeasures or safeguards to mitigate risk to acceptable levels. Management control families include risk assessment, security planning, system and services acquisition, and security assessment.

Malicious code. Rogue computer programs designed to inflict a magnitude of harm by diminishing the confidentiality, integrity, and availability of information systems and information.

N

Network. A communications infrastructure and all components attached thereto whose primary objective is to transfer information among a collection of interconnected systems. Examples of networks include local area networks, wide area networks, metropolitan area networks, and wireless area networks.

Node. A device or object connected to a network.

Nonrepudiation. The use of audit trails or secure messaging techniques to ensure the origin and validity of source and destination targets (i.e., senders and recipients of information cannot deny their actions).

O

Object reuse. The reassignment of a storage medium, which contains residual information, to potentially unauthorized users or processes.

Operational controls. Security controls focused on mechanisms primarily implemented by people as opposed to systems. These controls are established to improve the security of a group, a specific system, or group of systems. Operational controls require technical or specialized expertise and often rely on management and technical controls. Operational control families include personnel security, contingency planning, configuration management, maintenance, system and information integrity, incident response, and awareness and training.

Organization. A Certified Person or, as appropriate, any of its operational elements.

P

Packet. A unit of information that traverses a network.

Password. A private, protected, alphanumeric string used to authenticate users or processes to information system resources.

Patient Protection and Affordable Care Act. See Affordable Care Act.

Penetration testing. A testing method by which security evaluators attempt to circumvent the technical security features of the information system in efforts to identify security vulnerabilities.

Personally identifiable information. Any information about an individual with respect to, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual's identity (e.g., name, Social Security Number, date and place of birth, mother's maiden name, biometric records) including any other personal information linked or linkable to an individual.

Potential impact. The loss of confidentiality, integrity, or availability that could be expected to have a limited adverse effect, a serious adverse effect, or a catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Privileged user. A user that has advanced privileges with respect to computer systems. Such users in general include administrators.

Protocol. A set of rules and standards governing the communication process between two or more network entities.

R

Remnants. Residual information remaining on storage media after reallocation or reassignment of such storage media to different organizations, organizational elements, users, or processes. See Object reuse.

Residual risk. Portions of risk that remain after security controls or countermeasures are applied.

Risk. The potential adverse impact on the operation of information systems, which is affected by threat occurrences on organizational operations, assets, and people.

Risk assessment. The process of analyzing threats to and vulnerabilities of an information system to determine the potential magnitude of harm, and identify cost- effective countermeasures to mitigate the impact of such threats and vulnerabilities.

Risk management. The identification, assessment, and prioritization of risks.

Router. A device that forwards data packets between computer networks, creating an overlay internetwork.

S

Safeguards. Protective measures prescribed to enforce the security requirements specified for an information system; synonymous with security controls and countermeasures.

Security policy. The set of laws, rules, directives and practices governing how organizations protect information systems and information.

Security requirement. The description of a specification necessary to enforce the security policy. See Baseline security requirements.

Standard user. A general program user, who does not have administrative rights. Switch. A computer networking device that links network segments or network devices. System. See Information system.

System Security Plan. An official document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements (NIST SP 800-18).

T

Technical controls. Security controls executed by the computer system through mechanisms contained in the hardware, software, and firmware components of the system. Technical security control families include identification and authentication, access control, audit and accountability, and system and communications protection.

Threat. An activity, event, or circumstance with the potential for causing harm to information system resources.

U

User. A person or process authorized to access an information system.

User identifier. A unique string of characters used by an information system to identify a user or process for authentication.

V

Virus. A self-replicating, malicious program that attaches itself to executable programs.

Vulnerability. A known deficiency in an information system, which threat agents can exploit to gain unauthorized access to sensitive or classified information.

Vulnerability assessment. Systematic examination of an information system to determine its security posture, identifies control deficiencies, propose countermeasures, and validate the operating effectiveness of such security countermeasures after implementation.