Office of Inspector General

OIG

Office of Inspector General
Consulting Engagement

NTIS Assessment

201819-23

Background

- Limited Access Death Master File (LADMF)
  - Contains identifying information for deceased individuals including: first and last name, social security number, date of birth, and date of death.
- National Technical Information Service (NTIS)

Statutes and Guidelines

- 15 CFR 1110
  - Defines requirements to become a Certified Person in order to obtain access to Limited Access Death Master File.

- NTIS LADMF Security Guidelines
  - provides guidance to assist certified persons in ensuring their policies, practices, controls, and safeguards adequately protect LADMF information.

Conformity Assessment

- NTIS has stopped providing Limited Access Death Master File Information.
- Motorist Services requested the OIG to conduct a Conformity Assessment.
- Accredited Conformity Assessment Body's review or assessment must be conducted every three years.

Results:

- Access Controls
- MOUs
- Policies
- Awareness Training

Access Controls

- NTIS Security Guidelines, Section 7.3.1.6, requires access only be provided to individuals who require data to perform their duties.
- Server for the complete LADMF data file (**which includes SSN, DOB, Name, and DOD**) originally created with a share, which was incorrectly set up.
- Approximately 4500 Department and AST members had ability to access.
- Permissions have been updated reducing access to approximately 60 users.

Access Controls (cont'd)

- Reviewed a sample of 30 Department Users for each of 3 applications which display date of death(DAVID, FDLIS, and Motorist Maintenance).

- After audit inquiry the following changes were made to DAVID Users:

  - 1 user was inactivated.
  - 1 user had 2 separate login accounts, but one was inactivated due to a job change.
  - 1 user was not active but was updated to active.
  - 1 user updated her last name in DAVID.

Access Controls (cont'd)

- After reviewing Motorist Maintenance Access, OIG staff noted the following:
  - 3 users were listed as active but were no longer employed with the Department and there were no requests to deactivate the users.
  - 3 users were listed as having not logged into the system since 2017, but upon audit inquiry it was determined they are active users and the system had captured the wrong dates.
  - 1 user was terminated on 4/3/19 and still had access.

Access Controls (cont'd)

- After reviewing FDLIS access we determined all 30 users were current employees and had accessed FDLIS within the last 30 days.

Access Controls Recommendations

- We recommend the Department periodically review user access to Limited Access Death Master File servers, applications, and data to determine if users should still have access.

- We also recommend ISA review and comply with NTIS Death Master File Security Guidelines Section 7.3 Information Security Control Requirements.

- We further recommend ISA periodically review access and security settings to ensure they comply with applicable statutes, codes, and best practices.

MOUs

OIG staff reviewed a sample of MOUs with External Partners for DAVID and FDLIS to determine if they comply with NTIS requirements.

- Our review determined the following:
  - The FDLIS MOU does not cover LADMF information requirements.
  - Currently, the Department is in the process of having all external partners agree to and sign the LADMF DAVID Amendment (755 of 757 have been signed) as of the time of our review.
  - The Department has submitted the LADMF DAVID Amendment to Federal agencies and is in the process of working with them to gain NTIS compliance.

MOUs Recommendations

- We recommend Motorist Services continue to work with external partners to ensure all external partners agree and sign the LADMF DAVID Amendment.

- We also recommend Motorist Services update the FDLIS MOU with LADMF requirements and have all external partners accessing FDLIS agree and sign an updated MOU.

Policies

- OIG staff reviewed the following Department policies to determine if they comply with NTIS requirements:
  - The Information Security Manual;
  - Department Policy 8.01: Information Technology Security;
  - Department Policy 8.03: Acceptable Use of Information Technology Resources;
  - Department Policy 8.07: Security Breach of Personal Information;
  - Department Policy 9.02: Personal Information Exempted from Public Disclosure;
  - Department Policy 9.03: Providing Records to the Public; and
  - Department Policy 9.04: Records Management.

Policies (Cont'd)

Our review determined the Department has controls for governing access, information distribution, and purging, but the policies need to be updated to include controls which comply with 15 CFR 1110 and NTIS Security Guidelines.

Policies Recommendations

We recommend the Department update all policies regarding Public Records, Data Access, Data Dissemination, and Records Destruction to comply with all NTIS requirements.

Awareness Training

NTIS Security Guidelines, Section 5.3, states prior to granting an employee or contractor access to LADMF information, each employee or contractor should certify his or her understanding of the security policy and procedures for safeguarding LADMF information.

OIG staff reviewed user training and annual certification for FDLIS, DAVID, and Motorist Maintenance to determine if it is adequate and meets standards for Limited Access Death Master File (LADMF) information requirements.

- After review, OIG staff determined the following:
  - There was no authorized training required to access Motorist Maintenance and FDLIS.
  - DAVID has a training requirement, but it does not cover LADMF information.

Awareness Training Recommendations

- We recommend the Department develop or revise current training for employees, contractors, and external partners accessing information prior to, and annually thereafter, accessing applications and servers which house Limited Access Death Master File Information.

Summary

- Access Controls
- MOUs
- Policies
- Awareness Training