Office of Inspector General

Review of the FMC's FY 2010 Privacy and Data Protection

A11-01A

November 2010

FEDERAL MARITIME COMMISSION

FEDERAL MARITIME COMMISSION
800 North Capitol Street, N.W.
Washington, DC 20573

November 8, 2010

Office of Inspector General

TO: Chairman Richard A. Lidinsky
Commissioner Joseph E. Brennan
Commissioner Rebecca F. Dye
Commissioner Michael A. Khouri

FROM: /Adam R. Trzeciak/
Inspector General

SUBJECT: OIG Report on Privacy and Data Protection

The Office of Inspector General (OIG) performed a review of privacy and data protection policies and procedures to determine if the Federal Maritime Commission (FMC) is complying with Section 522 of the Consolidated Appropriations Act, 2005, (42 U.S.C.A. § 2000ee-2).

Section 522 requires an independent third-party review of agency use of personally identifiable information (PII) and of its privacy and data protection policies and procedures at least every two years. PII is information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. This evaluation satisfies the required third-party review.

The FMC has made progress in implementing privacy and data protection practices since our 2008 review. For example, it updated its Incident Response Policy to include breach-related procedures, prepared draft privacy impact assessment (PIA) policies and templates and completed select PIAs. The Senior Agency Official for Privacy has taken a more active role in data protection activities and the agency's annual security awareness training includes sections on privacy and data protection.

We also noted areas where improvements are possible. The agency needs to finalize its policies and procedures and perform federally-required PIAs on all agency systems that require a PIA. Further the agency has not performed a risk assessment for FMC-18 (on-line license application form) and there is no assurance that appropriate controls have been implemented.

The OIG met with management who generally concurs with our findings and recommendations. Management comments are attached to this report.

The OIG wishes to thank the Privacy Act Officer, the Senior Agency Official for Privacy and the Chief Information Officer for their assistance. I am available at your convenience to discuss the report's findings and recommendations.

cc: Ronald Murphy, Managing Director
Karen Gregory, Secretary
Anthony Haywood, Chief Information Officer

Privacy and Data Protection Evaluation Report

Office of the Inspector General
Review of the Federal Maritime Commission's Implementation of the Federal Information Security Management Act (FISMA) For Fiscal Year 2010

November 8, 2010

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Section 522 of the Consolidated Appropriations Act, 2005 (42 U.S.C.A. § 2000ee-2) (Section 522) requires an independent third-party review of agency use of personally identifiable information (PII) and of its privacy and data protection policies and procedures at least every two years. OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, defines PII as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." This review satisfies the required third-party review.

While the FMC has made progress in implementing privacy and data protection practices, additional work is still necessary to ensure that controls around PII in both paper and electronic form are implemented. Our findings and recommendations are summarized on the chart below.

Finding	Recommendation
#1 – The FMC does not fully comply with OMB Memorandum M-03-22, *Implementing the Privacy Provision of the E-Government Act of 2002*.	1. Develop and implement policies and procedures to require privacy impact assessments (PIA) to be completed for each applicable information system.
#2 – The FMC does not fully comply with security requirements of OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.	2. Remove the FMC-18 (Form-18) PIA from the publicly accessible web that incorrectly states, "A risk assessment has been conducted and the appropriate controls have been implemented" as no authorization (formerly Certification & Accreditation (C&A)) package was created for this system. 3. Create a planning document for multifactor authentication that correlates with the IT capital planning and investment control process. Utilize multifactor authentication for remote authentication for FMC systems to authenticate users' identities for Level 3 and Level 4 users in accordance with National Institute of Standards and Technology (NIST) 800-63. 4. Create policies and/or procedures to log, verify and reassess data extracts from database holding sensitive information after 90 days.

INTRODUCTION

The Office of Inspector General (OIG) of the Federal Maritime Commission (FMC) contracted with Richard S. Carson & Associates to conduct a review of privacy and data protection policies and procedures and, specifically, to determine if the FMC is complying with Section 522 of the Consolidated Appropriations Act of 2005. The review was conducted using the Federal Information Security Management Act of 2002 (FISMA), Reporting Section D – Template for the Senior Agency Official for Privacy (SAOP) and Office of Management and Budget (OMB) Memorandum M-07-16, *Safeguarding Against and Responding to Breach of Personally Identifiable Information*. This report is organized into the following sections:

- Background
- Objectives, Scope and Methodology
- Detailed Findings and Recommendations

BACKGROUND

The Federal Maritime Commission was established as an independent regulatory agency by Reorganization Plan No. 7, effective August 12, 1961. The principle statutes or statutory provisions administered by the Commission are the Shipping Act of 1984; the Foreign Shipping Practices Act of 1988; Section 19 of the Merchant Marine Act, 1920; and Public Law 89-777. Most of these statutes were amended by the Ocean Shipping Reform Act of 1998, which took effect on May 1, 1999.

The Federal Maritime Commission:

- Monitors activities of ocean common carriers, marine terminal operators, conferences, ports, and ocean transportation intermediaries (OTI) that operate in U.S. foreign commerce to ensure they maintain just and reasonable practices.
- Maintains a trade monitoring and enforcement program designed to assist regulated entities in achieving compliance and to detect and appropriately remedy malpractices and violations set forth in Section 10 of the Shipping Act.
- Monitors the laws and practices of foreign governments that could have a discriminatory or otherwise adverse impact on shipping conditions in the U.S.
- Enforces special regulatory requirements applicable to ocean common carriers owned or controlled by foreign governments (controlled carriers).
- Processes and reviews agreements and service contracts.
- Reviews common carriers' privately published tariff systems for accessibility and accuracy.

- Issues licenses to qualified OTIs in the U.S. and ensures each maintains evidence of financial responsibility.

OBJECTIVES, SCOPE AND METHODOLOGY

Richard S. Carson & Associates, under contract to the FMC/OIG conducted a review of privacy and data protection policies and procedures to determine if the FMC is complying with the following:

1. Federal Information Security Management Act of 2002, Reporting Section D – Template for the Senior Agency Official for Privacy (SAOP), which is based on privacy-related laws and regulations, including the Privacy Act of 1974 and the E-Government Act of 2002, (Public Law 107-347, 44 U.S.C. Ch 36).

2. Office of Management and Budget Memorandum M-07-16

To accomplish the review objectives, security specialists conducted interviews with the FMC Office of the Secretary, including the Assistant Secretary; Office of the Managing Director staff, including the Chief Information Officer and the Senior Agency Official for Privacy; Office of Information Technology staff, including the Director of Information Technology and the Senior Information System Security Officer; as well as the Office of the General Counsel and other FMC personnel.

The team reviewed documentation provided by the FMC, including policies and procedures, privacy impact assessments and privacy-related policies.

All analyses were performed in accordance with the following guidance:

- Privacy Act of 1974
- Section 522 of the Consolidated Appropriations Act, 2005 (42 U.S.C.A. § 2000ee-2)
- Federal Information Security Management Act of 2002 (Public Law 107-347)
- OMB Memorandum M-03-18, *Implementation of E-Government Act of 2002*
- OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*
- OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*
- OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*
- OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*

- OMB Memorandum M-07-18, *Ensuring New Acquisitions Include Common Security Configurations*
- OMB Memorandum M-08-09, *New FISMA Privacy Reporting Requirements for FY 2008*
- OMB Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*
- Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*
- FIPS PUB 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- The E-Government Act of 2002, Section 208, HR 2458
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories,* Volumes I & II
- NIST SP 800-63, *Electronic Authentication Guideline*
- OMB Circular A-130, *Management of Federal Information Resources,* Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals
- Consolidated Appropriations Act, 2005 (Public Law 108-447)
- FMC/OIG audit guidance
- FMC policies and procedures

Fieldwork was conducted between July 7 and August 31, 2010, at the FMC Headquarters in Washington, DC.

DETAILED FINDINGS AND RECOMMENDATIONS

The FMC has made progress in its privacy and data protection program in the last year, including the following:

- Reviewing the System of Records and updating the Systems of Records Notice
- Documenting Privacy Impact Assessment (PIA) policies and templates currently under review by the Office of General Counsel
- Involving the SAOP in numerous privacy and data protection-related activities

- Conducting annual security awareness training that includes sections on privacy and data protection

While the FMC has made improvements in its privacy and data protection program, the security team has noted weaknesses in the program. These are documented below.

FISMA Reporting

Finding #1 – The FMC Does Not Fully Comply with OMB Memorandum M-03-22

Office of Management and Budget Memorandum M-03-22*, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, requires the following actions on the part of federal agencies:

- Conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available.
- Post privacy policies on agency websites used by the public.
- Translate privacy policies into a standardized, machine-readable format.
- Report annually to OMB on compliance with Section 208 of the E-Government Act of 2002 (now covered by FISMA).

The FMC performed a Privacy Impact Assessment review and created a PIA template. As defined by OMB Memorandum M-03-22, a PIA is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. While FMC has a draft privacy policy and associated procedure to require and provide guidance for conducting PIAs on all electronic information systems they have not been signed. PIAs were not completed for all FMC systems that require a PIA. For example, Form-18 had a completed PIA; however, Consumer Affairs & Dispute Resolution Services system did not.

Without properly assessing and documenting the data within each information system, the FMC cannot ensure that privacy information is handled in a manner that maximizes both privacy and security.

The SAOP informed the OIG that due to the small size and early-stage development of FISMA compliance mechanisms, the SAOP did not previously have PIA policies. Per discussions with the SAOP, the PIA policy has been written and is under review by the General Counsel. Management agrees with our recommendation and will complete all PIAs by May 30, 2011.

Recommendations

1. Formally implement policies and procedures to require PIAs to be completed for each applicable information system.

OMB Memorandum M-07-16

Finding #2 – The FMC Does Not Fully Comply with Security Requirements of OMB Memorandum M-07-16

OMB Memorandum M-07-16*, Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, requires agencies to:

- Encrypt all data on mobile computers/devices carrying agency data
- Employ two-factor remote access authentication
- Require the session or device used to perform remote access to FMC networks to time out after 30-minute inactivity
- Log and verify all computer-readable data extracts from databases holding sensitive information
- Require all individuals with authorized access to PII and their supervisors to sign, at least annually, a document clearly describing their responsibilities to ensure their understanding of their responsibilities

Furthermore, the following security requirements should be implemented as a foundation to ensure PII is protected:

a. Assign an impact level to all information and information systems. Agencies must follow the processes outlined in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, to categorize all information and information systems according to the standard's three levels of impact (*i.e.*, low, moderate, or high). Agencies should generally consider categorizing sensitive personally identifiable information (and information systems within which such information resides) as moderate or high impact.

b. Implement minimum security requirements and controls. For each of the impact levels identified above, agencies must implement the minimum security requirements and minimum (baseline) security controls set forth in FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, and NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, respectively.

c. Certify and accredit information systems. Agencies must certify and accredit (C&A) all information systems supporting the operations and assets of the agency. The specific procedures for conducting C&A are set out in NIST Special Publication 800-37, *Guide for the Security*

Certification and Accreditation of Federal Information Systems, and include guidance for continuous monitoring of certain security controls. Agencies' continuous monitoring should assess a subset of the management, operational, and technical controls used to safeguard such information (*e.g.*, Privacy Impact Assessments).

d. Train employees. Agencies must initially train employees (including managers) on their privacy and security responsibilities before permitting access to agency information and information systems. Thereafter, agencies must provide at least annual refresher training to ensure employees continue to understand their responsibilities. Additional or advanced training should also be provided commensurate with increased responsibilities or change in duties.

NIST Special Publication (SP) 800-63*, Electronic Authentication Guideline,* April 2006, states that authentication systems are often categorized by the number of factors that they incorporate. Authentication is generally required to access secure data or enter a secure area. The requestor for access or entry shall *authenticate* her or himself based on proving *authentically* her or his identify by means of:

- What the requestor individually *knows* as a secret, such as a password; or
- What the requesting owner uniquely *has*, such as a physical token or an ID-card; or
- What the requesting bearer individually *is*, such as biometric data, like a fingerprint.

Multifactor authentication is a common term used to describe authentication methods that employ two or more factors to authenticate or validate the identity of a user. Some systems require three factor authentication; specifically those systems that process, store, or transmit information with the highest levels of sensitivity. Systems with this level of sensitivity have been categorized at the "High" level for data confidentiality. Systems that have been categorized at the "Moderate" level may only require two-factor authentication.

Two-factor authentication uses any two authentication methods (e.g., password plus value from physical token) to increase the assurance that the bearer has been authorized to access secure systems. For example, the owner of secure data or the operator of such secure systems may implement two-factor authentication on laptops because of the inherent security risks in mobile computers.

Through observation of configuration settings, interviews, and reviews of documentation, the OIG noted the following weaknesses:

- A risk assessment has not been conducted for FMC-18 and there is no assurance that appropriate controls have been implemented since no accreditation (formerly C&A) package was completed for FMC-18 (Form-18). Additionally, the FMC-18 PIA, which is posted on the web, incorrectly states, "A risk assessment has been conducted and the appropriate controls have been implemented."

- The FMC Secure Socket Layer [1] Virtual Private Network [2]only utilizes one-factor authentication via username and password. Therefore the remote authentication process

[1] Secure Sockets Layer, is a cryptographic protocol that provides security for communications over networks such as the Internet.

Footnote continues on next page.

is missing a second factor such as something a user has or something a user is (i.e. biometric) to validate identity. Further, FMC policy does not define requirements for multifactor authentication for NIST 800-63 Level 3 and Level 4 systems.

- No policies or procedures have been created or implemented to log, verify and reassess data extracts from databases holding sensitive information after 90 days due to budgetary constraints.

Without implementing the technical security considerations of OMB Memorandum M-07-16, the FMC cannot ensure OMB compliance and privacy data may be at risk for unauthorized exposure.

Recommendations

2. Remove the FMC-18 (Form-18) PIA from the publicly accessible web that incorrectly states, "A risk assessment has been conducted and the appropriate controls have been implemented" as no authorization (formerly C&A) package was created for this system.

3. Create a planning document for multifactor authentication that correlates with the IT capital planning and investment control process. Utilize multifactor authentication for remote authentication for FMC systems to authenticate users' identities for Level 3 and Level 4 users in accordance with NIST 800-63.

4. Create policies and/or procedures to log, verify and reassess data extracts from databases holding sensitive information after 90 days.

[2] A Virtual Private Network encapsulates data transfers between two or more networked devices which are not on the same private network to keep the transferred data private from other devices on one or more intervening local or wide area networks.

Memorandum

TO : Inspector General **DATE:** October 20, 2010

FROM : Senior Agency Official for Privacy (SAOP)

SUBJECT : Comments on Review of FY 2010 Privacy Independent Evaluation

We have reviewed the recommendations in the instant Draft Report. Below are our comments regarding said recommendations.

Finding #1: FMC does not fully comply with OMB M-07-16

Recommendation #1. Complete Privacy Impact Assessments (PIA) assessments for all FMC systems that require a PIA.

Response: We concur in the recommendation. The SAOP has recently developed new PIA Procedures and plans to use the new procedures/template to evaluate all systems, but most particularly systems containing personally identifiable information. We would intend that the PIAs be accomplished by May 30, 2011.

Recommendation #2. Remove the FMC-18 (Form-18) PIA from the publicly accessible web that incorrectly states "A risk assessment has been conducted and the appropriate controls have been implemented" as no authorization (formerly C&A) package was created for this system.

Response: The inaccurate language has been removed from the PIA, and the updated version will be posted to the FMC website. We feel that the necessary security controls, although not documented, are in place to allow for the functionality of the FMC-18 system.

Recommendation #3. Create a planning document for multifactor authentication that correlates with the IT capital planning and investment control process. Utilize multifactor authentication for remote authentication for FMC systems to authenticate users' identities for Level 3 and Level 4 users in accordance with NIST 800-63.

Response: FMC will determine which systems, if any, require multifactor authentication and take necessary steps thereafter.

Recommendation #4. Create policies and/or procedures to log, verify, and reassess data extracts from databases holding sensitive information after 90 days.

Response: This recommendation will be addressed by the contractor conducting the Form FMC-18 System Upgrade during FY 11, pending availability of funds.

/Ronald D. Murphy/
Senior Agency Official for Privacy

Attachment

cc: Privacy Act Officer
Chief Information Officer
Director, Office of Information Technology