

**Privacy and Data Protection
Evaluation Report**

A08-08



September 2008

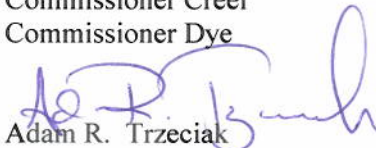


FEDERAL MARITIME COMMISSION
800 North Capitol Street, N.W.
Washington, DC 20573

September 22, 2008

Office of Inspector General

TO: Commissioner Brennan
Commissioner Creel
Commissioner Dye

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. Section 522 also requires certain agencies (including the FMC) to assign a privacy act officer who is responsible for identifying and safeguarding PII. This evaluation satisfies the required third-party review.

While the FMC has made progress in implementing privacy and data protection practices, it has not always gone far enough to ensure that controls over PII in both paper and electronic form are implemented. For example, the agency posted its privacy policy on the FMC website, and created a Privacy Impact Assessment (PIA) review tool. However, there are no procedures or guidance for conducting PIA's on electronic information systems. A PIA review had only been conducted on one of the agency's four systems. Further, the web-posted policy was not posted in standardized, machine-readable format to ensure that individuals using any one of a number of web browsers can access it.

The OIG also noted that, contrary to OMB policy, the agency has not taken certain steps to safeguard against a breach of PII. For example, the agency has not encrypted all data on mobile computers/devices carrying agency data; required two-factor remote access authentication;

implemented a 30-minute inactivity timeout function for remote access; or logged and verified all computer-readable data extracts from databases holding sensitive information.

Without implementing OMB's technical security considerations, privacy data may be vulnerable to unauthorized exposure.

The OIG met with management, which generally concurs with our findings and recommendations. Management informed the OIG that most of the findings will be addressed by the agency's recently-hired information security contractor, who is tasked with bringing the agency's information security program up to current FISMA and OMB standards. Details of our results are attached.

The OIG wishes to thank the privacy act officer, the senior agency official for privacy, the CIO and the Director, OIT, for their help on this review.

cc: Peter King, General Counsel (Acting)
Karen Gregory, Assistant Secretary
Anthony Haywood, CIO

EXECUTIVE SUMMARY

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-05-19, *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.” Section 522 also requires certain agencies to assign a Chief Privacy Officer (CPO) who is responsible for identifying and safeguarding PII. This audit 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 over PII in both paper and electronic form are implemented. Our findings and recommendations are summarized below.

Finding	Recommendation
#1 – The FMC does not fully comply with OMB Memorandum M-03-22, <i>Implementing the Privacy Provision of the E-Government Act of 2002</i> .	<ol style="list-style-type: none"> 1. Develop and implement policies and procedures to require privacy impact assessments (PIA) to be completed for each information system as part of the certification and accreditation (C&A) packages. 2. Translate the privacy policies on FMC.gov into a standardized, machine-readable format, such as the Platform for Privacy Preferences Project Protocol (P3P).
#2 – Job-specific privacy training not implemented.	<ol style="list-style-type: none"> 3. Provide and track job-specific privacy training to personnel directly involved in the administration of personal information, information technology systems, or with significant information security responsibilities.
#3 – The FMC does not fully comply with security requirements of OMB Memorandum M-07-16, <i>Safeguarding Against and Responding to Breach of Personally Identifiable Information</i> .	<ol style="list-style-type: none"> 4. Implement encryption on mobile computers and portable devices carrying agency data. 5. Configure the FMC employee remote-access connection to require two-factor authentication. 6. Configure the Network Administrator remote-access connection to require a 30-minute inactivity timeout. 7. Develop and implement policies and procedures for extracting and verifying database extracts containing PII. 8. Develop and implement policies and procedures to require all individuals with authorized access to PII and their supervisors to sign, at least annually, a document clearly describing their responsibilities.

TABLE OF CONTENTS

Executive Summary	i
1. Background	1
2. Objectives, Scope and Methodology	2
3. Detailed Findings and Recommendations	3
3.1 FISMA, Reporting Section D – Template for the SAOP	4
Finding #1 – The FMC Does Not Fully Comply with OMB Memorandum M-03-22 ...	4
3.2 OMB Memorandum M-07-16	5
Finding #2 – Privacy Job-Specific Training Not Implemented.....	5
Finding #3 – The FMC Does Not Fully Comply with Security Requirements of OMB Memorandum M-07-16.....	5

1. BACKGROUND

The Federal Maritime Commission (FMC) was established as an independent regulatory agency by Reorganization Plan No. 7, effective August 12, 1961. Prior to that time, the Federal Maritime Board was responsible for both the regulation of ocean commerce and the promotion of the United States Merchant Marine. Under the reorganization plan, the shipping laws of the U.S. were separated into two categories: regulatory and promotional. The newly created FMC was charged with the administration of the regulatory provisions of the shipping laws. The Commission is responsible for the regulation of ocean-borne transportation in U.S. foreign commerce. The passage of the Shipping Act of 1984 brought about a major change in the regulatory regime facing shipping companies operating in U.S. foreign commerce. The subsequent passage of the Ocean Shipping Reform Act of 1998, with its deregulatory amendments and modifications to the Shipping Act of 1984, further signaled a significant paradigm shift in shipping regulation. 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 all maintain evidence of financial responsibility.
- Ensures passenger vessel operators demonstrate adequate financial responsibility for casualty and non-performance.

2. OBJECTIVES, SCOPE AND METHODOLOGY

The Office of Inspector General (OIG) of the FMC contracted with Richard S. Carson and Associates Inc. to conduct a review of privacy and data protection policies and procedures and, specifically, to determine if the FMC is complying with the following:

1. Federal Information Security Management Act of 2002 (FISMA), 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 E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36); and
2. Office of Management and Budget (OMB) Memorandum M-07-16.

To accomplish the review objectives, the OIG conducted interviews with the FMC Office of the Secretary (OS), including the Assistant Secretary; Office of Administration (OA) staff, including the Chief Information Officer (CIO); the Senior Agency Official for Privacy (SAOP); Office of Information Technology (OIT) staff, including Director of Information Technology and the Senior Information System Security Officer; and the Office of the General Counsel (OGC) 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 (FISMA) (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 Breach of Personally Identifiable Information*
- OMB Memorandum M-07-18, *Ensuring New Acquisitions Include Common Security Configurations*
- OMB Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*

- OMB Memorandum M-08-09, *New FISMA Privacy Reporting Requirements for FY 2008*
- OMB Memorandum M-08-21, *FY 2008 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, Volumes I & II: *Guide for Mapping Types of Information and Information Systems to Security Categories*
- 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

The OIG and Carson Associates security consultants conducted fieldwork between May 15 and July 31, 2008, at the FMC headquarters in Washington, DC.

3. DETAILED FINDINGS AND RECOMMENDATIONS

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

- Implementing the following privacy and data protection policies:
 - Commission Order 56 – Automated Information Security Plan
 - Commission Order 63 - Workforce Discipline and Adverse Actions
 - Commission Order 80 – Security
 - Commission Order 89 – Privacy Act Implementation and Incident Response
 - Information Security Incident Response (ISIR) Policy, Breach Notification Plan
- Reviewing the System of Records, and updating the Systems of Records Notice (SORN)
- Conducting a review of Social Security numbers (SSN)
- Documenting PIA templates
- 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 significant improvements in its privacy and data protection program, the OIG has also noted weaknesses in the program. These are documented below.

3.1 FISMA, Reporting Section D – Template for the SAOP

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

Office of Management and Budget (OMB) 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).

While conducting the review, the OIG noted that a privacy policy was posted on the FMC website, and a PIA review and PIA template had been created. As defined by OMB Memorandum M-03-22, a PIA is an analysis of how information is handled to (i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. However, there was no policy or procedure to require and provide guidance for conducting PIAs on all electronic information systems. Additionally, a PIA review had only been conducted on FMC Form-18. Without properly assessing 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 OIG also noted that FMC.gov did not translate privacy policies into a standardized, machine-readable format, such as the Platform for Privacy Preferences Project Protocol (P3P). Without properly formatting the privacy policy on the agency's webpage, the agency has no assurances that all visitors to the site are able to access the policy.

The OIT informed the OIG that supplemental funding was recently approved by the Commission to hire an IT contractor whose responsibilities will include reviewing all systems and performing an assessment of all related PIA requirements. 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.

Recommendations

1. OIT develop and implement policies and procedures to require PIAs to be completed for each information system as part of the certification and accreditation (C&A) packages.
2. OIT translate the privacy policies on FMC.gov into a standardized, machine-readable format.

3.2 OMB Memorandum M-07-16

Finding #2 – Privacy Job-Specific Training not Implemented

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

The OIG noted that the agency administered computer security awareness training on an annual basis, to include privacy information, but additional or advanced job-specific privacy training for personnel directly involved in the administration of personal information, information technology systems, or with significant information security responsibilities, did not exist. Without proper job-specific privacy training, the FMC cannot ensure that privacy information is handled in a manner that maximizes both privacy and security.

OIT managers informed the OIG that it plans to include training upgrades as part of its contract with the agency's new IT security contractor.

Recommendation

3. Provide and track job-specific privacy training to personnel directly involved in the administration of personal information, information technology systems or with significant information security responsibilities.

Finding #3 – 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; require two-factor remote access authentication¹; use a 30-minute inactivity timeout function for remote access; log and verify all computer-readable data extracts from databases holding sensitive information; and require all individuals with authorized access to PII and their supervisors to sign, at least annually, a document clearly describing their responsibilities.

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

- Encryption is not implemented on mobile computers and devices carrying agency data.
- FMC employee remote-access connection (i.e. “Employee SSL VPN”) currently utilizes one-factor authentication.
- Network Administrator remote-access connection does not implement a 30-minute inactivity timeout.
- Policies and procedures have not been developed and approved for database extracts containing PII.
- FMC has not ensured that all individuals with authorized access to PII and their supervisors sign, at least annually, a document clearly describing their responsibilities.

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.

The FMC informed the OIG that the conditions exist because the resources were not available to monitor the requirements in order to implement the settings. Funding has recently been approved for an IT contractor to update C&A packages and the security program for the OIT.

Recommendations

4. Implement encryption on mobile computers and portable devices carrying agency data.
5. Configure the FMC employee remote-access connection to require two-factor authentication.
6. Configure the Network Administrator remote-access connection to require a 30-minute inactivity timeout.
7. Develop and implement policies and procedures for extracting and verifying database extracts containing PII.
8. Develop and implement policies and procedures to require all individuals with authorized access to PII and their supervisors sign, at least annually, a document clearly describing their responsibilities.

¹ Human authentication factors are usually classified into one of the following cases: something the user **has** (i.e., ID card or security token), something the user **knows** (i.e., a password or personal identification number (PIN)), and something the user **is or does** (i.e., fingerprint or other biometrics).