Review of Federal Maritime Commission Implementation of the Federal Information Security Management Act for FY 2008
A08-07

September 2008

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

September 22, 2008

Office of Inspector General

Commissioners;

The Office of Inspector General (OIG) has completed its independent evaluation of information security pursuant to requirements contained in the Federal Information Security Management Act (FISMA) of 2002. This is the sixth annual evaluation completed by the OIG in the area of information and computer security.

As you already know, this year the Office of Information Technology (OIT) sought the assistance of an outside contractor to perform a comprehensive assessment of its information security posture. Based on that review, the OIT requested, and recently received, significant funding to address the identified weaknesses and vulnerabilities in its security program. After the security assessment was issued, but before funding was provided to implement corrective actions, the OIG began its annually-mandated review.

To use our resources most efficiently, I scaled back the OIG evaluation to focus on areas that were outside the scope of the contractor's review. This year, we (i) reviewed contingency plan testing, incident response processing, plan of action and milestones preparation, security awareness training, configuration management implementation and contractor-system oversight; (ii) followed up on infrastructure-level security issues identified by the OIT contractor; (iii) evaluated portable media policies; and (iv) assessed compliance with OMB information security-related memoranda dating back to 2005.

As importantly, we did not review Certification and Accreditation (C&A) testing. In our prior year review, we found that C&A packages did not provide enough information for management to make informed determinations as to whether systems already placed in operation were vulnerable to attack or data loss. The contractor will be focusing primarily on addressing this vulnerability in the coming months. However, as of the end of our fieldwork, this condition still existed and continues to be a significant deficiency in the Federal Maritime Commission's (FMC) information security program.

The investment needed this year to bring agency systems into compliance with Federal requirements is substantial. For too many years, emphasis was placed on production (i.e., faster servers, more powerful desktops, enhanced software, etc.) rather than on security. Now the agency has fallen behind and must spend liberally. Moving forward, it is our hope that security receives the attention it needs to protect our assets, and the assets of the organizations connected to FMC systems, from being compromised or destroyed.

Management generally agrees with our findings and recommendations, and has already taken some steps to implement the recommendations. Management comments are attached to the report in their entirety.

The OIG performed this evaluation from June, 2008 through August, 2008, and followed National Institute of Standards and Technology guidance for information systems, OMB Memorandum M-08-21, *Reporting Instructions for the Federal Information Security Management Act* (July 14, 2008) and best practices used in the industry. The OIG thanks OIT management and staff for its help and cooperation during our review.

Respectfully submitted,

Adam R. Trzeciak
Inspector General

EVALUATION SUMMARY

Introduction

On December 17, 2002, the President signed into law the E-Government Act of 2002 (Public Law 107-347), which includes Title III, the Federal Information Security Management Act (FISMA) of 2002. FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act (GISRA) of 2000, which expired in November 2002. FISMA outlines the information security management requirements for agencies, including the requirement for annual review and independent assessment by agency inspectors general. In addition, FISMA includes new provisions aimed at further strengthening the security of the federal government's information and information systems, such as the development of minimum standards for agency systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs and to develop strategies and best practices for improving information security.

The Federal Maritime Commission's (FMC) Office of Inspector General (OIG) contracted with Richard S. Carson and Associates (Carson Associates) to perform an independent FISMA evaluation of the FMC security program, along with the OIG's portion of the Office of Management and Budget (OMB) Reporting Template for IGs for FY 2008. This OIG Independent Evaluation Report, unlike the Reporting Template for IGs, focuses on performance measures, provides specific findings and, when applicable, recommendations for resolution.

Objectives

Reflecting the FISMA and security program-related tasks to be performed by the OIT contractors (discussed in Section 4.1 below),[1] the objectives of the independent evaluation of the FMC information security program are to:

1. Review select portions of FISMA that will not be addressed by the OIT's contractor during Certification and Accreditation (C&A) testing, such as contingency plan testing, incident response processing, plan of action and milestones (POA&M) preparation, security awareness training, configuration management implementation and contractor-system oversight.
2. Follow-up on the "infrastructure level security issues" reported in the *Security Compliance Status Report* by the OIT contractors.
3. Review portable media policies.
4. Assess compliance with Office of Management and Budget information security-related memoranda dating back to 2005.

The FMC OIG did not perform an internal network scan in the FY 2008 evaluation. Instead we reviewed the results of the scans performed by the OIT contractor to gain an understanding of its methodology and results. Based on this review, the OIG relied on the contractor's testing.

The results of these various evaluations are presented in this Independent Evaluation Report along with a number of recommendations to address weaknesses identified during the evaluation.

[1] The Office of Information Technology has contracted with an IT security firm to assist it in implementing FISMA requirements. OIT informed the OIG of its plans, and discussed the deliverables the contractor will be producing during the next several months. The OIG will review areas to be addressed by the contractor in the FY 2009 FISMA evaluation.

Overview

FISMA section 3542(b) defines information security as "… protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide (A) integrity—guarding against improper information modification or destruction, and ensuring information nonrepudiation and authenticity; (B) confidentiality—preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability—ensuring timely and reliable access to, and use of, information."

The OIG found that FMC's Office of Information Technology (OIT) has established security safeguards to protect the agency's systems; however, the prescribed NIST and OMB methodologies have not been implemented. In short, the agency has not gone far enough.

While the FMC has made progress in laying the groundwork for potential effective and rapid mitigation of weaknesses in the information security program, it still falls short of the expectations OMB has for FISMA implementation throughout agencies. The independent review identified one significant deficiency.[2] While FMC senior management has begun to focus on FISMA as an agency responsibility, the following conditions were identified that contributed to the significant deficiency:

- FMC C&A documentation does not comply with NIST and OMB guidance for the FMC Network, Service Contracts Internet Based Filing System (SERVCON), and FORM-1. The documentation lacks sufficient information that would provide management with the assurance required to effectively demonstrate sound information security decisions based on risk; and
- FMC emergency preparedness documentation and Safety and Security of Employees and Operations Plan/Continuity of Operations Plan (SEOP/COOP) does not address IT recovery in sufficient detail.

In addition, the following three weaknesses were identified:

- A Plan of Action and Milestones (POA&M) process was suspended by OIT management in FY 2008;
- Key aspects of the Security Program were not implemented, including weaknesses with the annual computer security awareness documentation, e-authentication process, and FMC server configurations; and
- Removable media policies and procedures were not implemented.

FMC management cannot make credible risk-based determinations for their systems. FMC management has not demonstrated an effective risk management process, as prescribed by NIST, and is not fully aware of the potential security control weaknesses in their systems, thereby leaving their information and systems vulnerable to attack or compromise.

[2] OMB defines a significant deficiency in Memorandum 08-21 as "a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken" (Page 7).

TABLE OF CONTENTS

1. BACKGROUND

On December 17, 2002, the President signed into law the E-Government Act of 2002 (Public Law 107-347), which includes Title III, the Federal Information Security Management Act (FISMA) of 2002. FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act (GISRA) of 2000, which expired in November 2002, and outlines information security management requirements for agencies, including the requirement for annual review and independent assessment by agency inspectors general (IG). In addition, FISMA includes provisions aimed at further strengthening the security of the federal government's information and information systems, such as the development of minimum standards for agency systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs and to develop strategies and best practices for improving information security.

2. OBJECTIVES

Due to the information security evaluation and remediation to be completed by the OIT contractors (to be discussed in Section 4.1 below), the OIG reviewed select areas within the FISMA framework not included in the contractor's scope of work. The objectives of the independent evaluation of the FMC information security program are as follows:

1 Review select portions of FISMA outside of Certification and Accreditation testing, to include contingency plan testing, incident response processing, plan of action and milestones (POA&M) preparation, security awareness training, configuration management implementation and contractor-system oversight.

2 Follow-up on the "infrastructure level security issues" reported in the *Security Compliance Status Report* prepared by the OIT contractors.

3 Review portable media policies.

4 Assess compliance with OMB information security-related memoranda dating back to 2005.

The OIG reviewed the results of the internal network scans performed by the OIT contractors and relied on those results in our assessment of network vulnerability for the FY 2008 FISMA vulnerability scan.

3. SCOPE AND METHODOLOGY

The scope of this independent evaluation of the FMC fiscal year (FY) 2008 information security program included the following:

- Configuration management
- Contractor oversight
- Security Awareness Training implementation review
- Incident response
- Follow-up on OIT contractor "infrastructure level security issues"
- Portable media policy review
- OMB memoranda on IT security - compliance review

To accomplish the review objectives, the OIG conducted interviews with Office of Administration (OA) staff, including the Chief Information Officer (CIO); Office of Information Technology (OIT) staff, including the Director of Information Technology and the Senior Information System Security Officer;

the Office of the Secretary (OS), including the Deputy Secretary; the Office of the General Counsel (OGC) staff, including the Senior Agency Official for Privacy (SAOP) and other FMC personnel.

The team reviewed documentation provided by FMC including C&A documentation, privacy impact assessments, and information security related policies.

All analyses were performed in accordance with the following guidance:

- Federal Information Security Management Act of 2002 (Public Law 107-347), December 2002
- Office of Management and Budget (OMB) Memorandum M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* July 14, 2007
- OMB Memorandum M-08-09, *New FISMA Privacy Reporting Requirements for FY 2008,* January 18, 2008
- OMB Memorandum M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 14, 2008
- OMB Circular A-130, Transmittal Memorandum No. 4, *Management of Federal Information Resources,* November 18, 2000
- Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Revision 1, *Guide for Developing Security Plans for Information Technology Systems*, February 2006
- NIST SP 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*, December 2006
- NIST SP 800-30, *Risk Management Guide for Information Technology Systems,* July 2004
- NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems,* June 2002
- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004
- *Quality Standards for Inspection* issued by the President's Council on Integrity and Efficiency
- President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency FISMA Framework, September 2006
- FMC/OIG audit guidance
- FMC policies and procedures

The OIG performed fieldwork between May 15 and July 31, 2008, at the FMC headquarters in Washington, DC.

4. Detailed Findings and Recommendations

The FMC has taken significant steps to enhance its information security program and address issues identified in the 2006 and 2007 FISMA report, including the following:

- Developing and approving several key security-related policies, to include–
    - Computer Administrative Policy, OIT-P14
    - Configuration Management Policy, OIT-P13
    - Electronic Mail Policy, OIT-P06

  - Enterprise Encryption Policy, OIT-P16
  - File Server Storage Policy, OIT-P05
  - Firewall Policy, OIT-P09
  - Inactive Accounts Policy, OIT-P04
  - Incident Response Policy, OIT-P03
  - IT Security for Personnel, OIT-P11
  - Password Policy, OIT-P01
  - Patch Management Policy, OIT-P12
  - PDA Policy, OIT-P02
  - Peer-to-Peer Policy, OIT-P07
  - Remote Access Policy, OIT-P10
  - Server Security Policy, OIT-P15
  - Wireless Communications Policy, OIT-P08

- Continuing implementation and monitoring of the annual computer security awareness program, to include providing an interactive online course with a required assessment for all employees at completion. All FMC staff and contractors completed annual computer security awareness training by July 22, 2008.
- Performing contractor system oversight to ensure the information systems meet government policies and regulations.
- Updating the Incident Response Policy to include Breach Related Procedures from OMB Memorandum M-07-16.
- Taking steps to comply with select security-related OMB memoranda.

4.1 Agency Implementation of FISMA – FY 2007 Follow-Up

During FY 2008, the OIT hired an IT security consulting firm (the contractor) to perform an inventory of its (OIT) information security program. The results of this inventory were presented to OIT in the "*Security Compliance Status Report*." OIT, with assistance from the contractor, will use the report results to restructure the agency's information security program and create C&A documentation for each of FMC's four information systems. The contractor is expected to complete the task by the Spring of 2009, in time for the OIG's FY 2009 FISMA evaluation.

The OIG is required to report on the security posture of the agency as part of its FISMA evaluation. Recognizing that the contractor has just begun to address vulnerabilities, the OIG must still opine on the program as it existed during the review period. In our view, the agency has taken two concrete steps to address its IT security vulnerabilities. First, it now recognizes the extent of the task. Second, it has sought, and received, substantial funding to bring the security program up to Congressional and OMB standards and expectations. Without minimizing the importance of this foundation and acknowledging the effort involved to bring it about, the fact of the mater is that, in FY 2008, many of the elements of a mature, robust and comprehensive security program simply did not exist at the FMC. However, we also note that this condition is likely to change in FY 2009.

Notification of Finding # 1: FY 2007 FISMA Weaknesses Have Not Been Addressed

E-Government Act of 2002 (Public Law 107-347), which includes Title III, the *Federal Information Security Management Act (FISMA) of 2002*, details the following federal agency responsibilities:

- Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification or destruction of information collected or maintained by or on behalf of the agency and information systems used or operated by an agency, by a contractor, or by an agency or other organization on behalf of an agency
- Ensuring that senior agency officials provide information security for the information and information systems that support the operations and assets under their control
- Delegating to the agency Chief Information Officer the authority to ensure compliance with the requirements imposed on the agency
- Ensuring that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards and guidelines
- Ensuring that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions
- Developing, documenting and implementing an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes the following:
    - Periodic assessments of the risk and magnitude of the harm
    - Policies and procedures based on risk that are cost-effective, ensure security is addressed throughout the life cycle of each system, and ensure compliance with stated requirements
    - Provisions for adequate security
    - Security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency
    - Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices to be performed with a frequency depending on risk, but no less than annually
    - Process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency
    - Procedures for detecting, reporting, and responding to security incidents consistent with standards and guidelines issued
    - Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency

Although the FMC has made progress in the areas of security awareness training, incident response, compliance with OMB memoranda and assuring service agency information system compliance, the FMC information security program falls short of OMB and NIST goals for a robust and fully integrated information security program and continues to be a significant deficiency, consistent with OMB Memorandum 08-21 (July 2008).[4] While FMC senior management has begun to focus on FISMA as an agency responsibility, the following serious conditions identified in the *FY 2007 FISMA Independent Evaluation of FMC Information Security Program* report remain:

- FMC C&A documentation does not comply with NIST and OMB guidance for the FMC Network, SERVCON, and FORM-1. The documentation lacks sufficient information that would provide management with the assurance required to effectively demonstrate sound information security decisions based on risk.

  The OIG notes that while FORM-18 is in the production environment, it was implemented prematurely by past personnel, and C&A documentation is currently being developed.

- FMC emergency preparedness documentation and the Safety and Security of Employees and Operations Plan/Continuity of Operations Plan (SEOP/COOP) do not address IT recovery in sufficient detail.

Until FMC effectively and fully implements an agency-wide information security program, FMC data and systems may be vulnerable to potential unknown threats and will not be adequately safeguarded to prevent unauthorized use, disclosure and modification.

The OIG noted that OIT has only recently secured funding for a contractor to update the C&A documentation for each of the information systems and to lay the framework for an overhaul of the OIT security program. As such, no recommendation will be issued for this finding. However, the FMC OIG will monitor the progress that OIT and the OIT contractor make in the FY 2009 FISMA Evaluation.

Notification of Finding # 2: Plan of Action and Milestones (POA&M) Process Not Implemented

OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001, requires that each agency implement a POA&M process, which is used to identify tasks that need to be accomplished, including resource requirements, interim milestones in meeting the task, and scheduled completion dates. The purpose of this POA&M is to assist agencies in identifying, assessing, prioritizing and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

The CIO told the OIG that OIT ceased documenting weaknesses in its POA&M because of the planned IT contractor evaluation of the entire security program. According to the CIO, a new POA&M process that documents vulnerabilities at the program and system levels will be established and all vulnerabilities will be tracked at that time.

[4] OMB defines a significant deficiency in Memorandum 08-21 as "a weakness in an agency's overall information systems security program or management control structure, or within one (1) or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken." (Page 7).

The OIG believes that POA&Ms are a critical piece of a security program and disagrees with management's decision to discontinue the use of POA&Ms in 2008. Because funding for this effort has been approved, no recommendation will be issued for this finding. However, the FMC OIG will monitor OIT and OIT contractor progress toward addressing this requirement in the FY 2009 FISMA Evaluation.

4.2 Agency Implementation of FISMA – FY 2008 Review

OMB Memorandum, M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, contained new FISMA reporting guidance for FY 2008. The OIG evaluated the security program based upon these changes and new requirements. As a result of these evaluations, additional vulnerabilities were noted.

Additionally, the OIG was unable to conclude on FMC contingency plan testing during FY 2008. OIT management informed the OIG that contingency plan testing is scheduled prior to the end of FY 2008; however, it had not been completed by the issuance of this report. The OIG will follow-up on contingency plan testing in FY 2009.

Notification of Finding # 3: Key Aspects of Security Program Not Implemented

OMB Memorandum M-04-26, *Personal Use Policies and "File Sharing" Technology*, September 8, 2004, requires that agency IT security or ethics training must train employees on agency personal use policies and the prohibited uses of file sharing. Training must be consistent with OMB Circular A-130, appendix III paragraph (3)(a)(b), which states that agencies must "ensure that all individuals are appropriately trained in how to fulfill their security responsibilities.... Such training shall assure that employees are versed in the rules of the system, be consistent with guidance issued by NIST and OPM, and apprise them about available assistance and technical security products and techniques."

OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, dated December 16, 2003, requires that agencies review new and existing electronic transactions to ensure the authentication processes provide the appropriate level of assurance. It establishes and describes four levels of identity assurance for electronic transactions requiring authentication. An e-authentication application is an application that is web-based, requires authentication, and extends beyond the borders of an enterprise (e.g., multi-agency, government-wide, or public facing).

The E-Government Act of 2002 (Public Law 107-347), which includes Title III, the *Federal Information Security Management Act (FISMA) of 2002*, details the following federal agency responsibilities:

- Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency and information systems used or operated by an agency, by a contractor, or by an agency or other organization on behalf of an agency.

Through meeting with FMC employees and inspecting documentation, the OIG noted the following conditions:

- Computer security awareness training does not explain policies regarding the use of collaborative Web technologies and peer-to-peer file sharing.

- Systems requiring e-authentication have not been identified and e-authentication risk assessments have not been conducted on IT systems; therefore, corresponding levels have not been assigned.
- OIT does not utilize NIST checklists to configure the 12 FMC servers.

By not educating staff and contractors about the policies concerning collaborative Web technologies and peer-to-peer file sharing, unauthorized information may be disclosed. Also, without identifying systems requiring e-authentication and conducting e-authentication risk assessments, the FMC cannot ensure secure, remote authentication by individuals to a federal IT system. Furthermore, without implementing commonly- accepted security configurations on the servers, the FMC cannot ensure the confidentiality, integrity, and availability of the information for specific servers. Lastly, without testing the contingency plans on all IT systems, the FMC may easily experience delays in recovering IT operations after an emergency.

The OIG noted that OIT has only recently secured funding for a contractor to update the C&A documentation for each of the information systems and to lay the framework for an overhaul of the OIT security program. However, because the above conditions were not identified in the OIT Contractor's Security Compliance State Report, we are making the following recommendations:

Recommendations

1. Update the computer security awareness training to include an explanation of policies regarding the use of collaborative Web technologies and peer-to-peer file sharing.
2. Identify systems that utilize e-authentication; perform and document an e-authentication risk assessment; assign a level; and implement the appropriate e-authentication policies, procedures, and technologies.
3. Implement NIST's Configuration Checklists on all FMC servers.

4.3 Portable Media Policy Review

As part of this year's independent evaluation, the OIG performed a *Removable Media* policy review. The objective of this review was to examine the policies and procedures implemented relating to digital media.[5] While the OIT has implemented access control mechanisms in other areas of IT, we identified vulnerabilities concerning removable media, as described below.

Notification of Finding # 4: Removable Media Policies and Procedures Not Implemented

NIST SP 800-53, Revision 2, requires the following policies and procedures for IT systems which the agency, following Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems* categorizes as "moderate:"

- Media Protection (MP)-1 – "develop, disseminate, and periodically review/update: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities,

[5] National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 2, December 2007, provides multiple examples of "media," including both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). For the purposes of this review, the OIG focused on digital media devices.

management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls."

- MP-2 – "restrict access to information system media to authorized individuals."
- MP-2(1) – "employ automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted."
- MP-4 – "physically control and securely store information system media within controlled areas."
- MP-5 – "protect and control information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel."
- MP-5(1) – "protect digital and non-digital media during transport outside of controlled areas using [Assignment: organization-defined security measures, e.g., locked container, cryptography]."
- MP-5(2) – "document, where appropriate, activities associated with the transport of information system media using [Assignment: organization-defined system of records]."
- MP-6 – "sanitize information system media, both digital and non-digital, prior to disposal or release for reuse."

The OIG met with OIT personnel, viewed system configurations and noted that portable media policies and procedures were not documented or implemented. Without implementing policies, procedures and technologies to protect information on portable media, the FMC may be vulnerable to unauthorized disclosure of agency information on such devices. Additionally, by not controlling access to portable media devices, malicious code may be loaded onto FMC IT systems, which may affect the confidentiality, integrity, and availability of agency information. The OIG notes that portable media encryption was found to be a weakness in the IT environment as documented in the contractor's *Privacy and Data Protection Evaluation Report for FY 2008.*

The OIT has only recently secured funding for a contractor to update the C&A documentation for each of the information systems and to lay the framework for an overhaul of the OIT security program. As such, no recommendation will be issued for this finding. However, the FMC OIG will monitor the progress that OIT and the OIT contractor have made in the FY 2009 FISMA Evaluation.

4.4 OMB Memoranda Review

The OIG performed a compliance review of select OMB memoranda issued since FY 2005. The OIG selected the following OMB memorandum for the compliance review:

- M-05-16, *Regulation on Maintaining Telecommunications Services During a Crisis or Emergency in Federally-owned Buildings*, June 30, 2005;
- M-05-24, *Implementation of Homeland* Security *Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, August 5, 2005;
- M-07-06, *Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials*, January 11, 2007;
- M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, March 22, 2007;
- M-07-18, *Ensuring New Acquisitions Include Common Security Configurations*, June 1, 2007;

- M-08-01, *HSPD-12 Implementation Status*, October 23, 2007;
- M-08-05, *Implementation of Trusted Internet Connections (TIC)*, November 20, 2007; and
- M-08-16, *Guidance for Trusted Internet Connection Statement of Capability Form (SOC)*, April 4, 2008.

The OIG interviewed FMC staff, reviewed documentation, and noted that FMC appears to be in compliance or has appropriate plans to be in compliance with the memorandum listed above.

4.5 Infrastructure Level Security Issues Follow-up

The OIG also followed up on the "Infrastructure Level Security Issues" reported in the *Security Compliance State Report* by the OIT contractors. The OIG reviewed the report and noted that the five "Infrastructure Level Security Issues" addressed vulnerabilities in access controls. Through interviews with the OIT staff and inspection of documentation, the OIG noted that one of the issues relating to firewall configuration was unsubstantiated and found to be erroneous, one issue relating to usernames had been corrected and the remaining three issues relating to services would be resolved by the OIT contractors by the end of FY 2008.

5. SUMMARY

The agency has recognized that it has much to do to comply with Federal IT security regulations and guidance. But it has taken the first step with the commitment of significant resources to fully test, certify and accredit its four major systems and to prepare a comprehensive plan for continuity in the face of numerous disaster / emergency scenarios.

The OIG reminds OIT that threats posed by security are constantly changing. Therefore the agency's security program must change to meet the threats. Resting on one's accomplishments will lead to complacency and, within a short while, OIT will again find itself having to renovate its program from the ground up. Nor is it prudent to speculate on the FMC as a target of hackers, especially juxtaposed next to sister departments and agencies, such as the Security and Exchange Commission, Federal Bureau of Investigation, Homeland Security and Social Security Administration. For hackers, it is often the challenge, not the subject matter, that interests them. It is also important to remember that the FMC is connected to other Federal agencies for payroll and various administrative processing services. The FMC could be a target for no other reason than to link to one or more of these agencies.

The OIG will monitor OIT progress throughout the fall and winter as it upgrades its information security program. We will be reporting to the Commission, OMB and the Congress on the success of its efforts in the FY 2009 FISMA Independent Evaluation.

Memorandum

TO : Inspector General **DATE:** August 25, 2008

FROM : Chief Information Officer

SUBJECT : Comments on Review of FMC's Implementation of FISMA for FY 2008

I have reviewed the recommendations in the instant Review. Below are our comments regarding corrective actions which will be effected to address the recommendations.

Finding #1: FY 2007 FISMA Weaknesses Have Not Been Answered
Finding #2: Plan of Action and Milestones (POA&M) Process Not Implemented

Response: As referred to in our response to the FY 07 FISMA Evaluation, the CIO, with the knowledge and concurrence of the IG, committed to a multi-year process by which the FMC would contract for expert outside assistance to assist the agency in drafting comprehensive C&A documentation, compliant with NIST and OMB guidance, for all FMC systems. This will include a related review and update by the contractor of FMC emergency preparedness documentation and SSEOP/COOP. The FMC completed the initial step in this multi-year process, which was to obtain an external evaluation of FMC's current C&A documentation in order to determine what tasks would be included in the statement of work (SOW).

Since the receipt of management's response to the FY07 FISMA recommendations, the IG has been kept aware of the agency's efforts to prepare an SOW needed to identify a new contractor to undertake a C&A package, and the significant budgetary issues related thereto. As you know, staff has reviewed and forwarded a recommendation to the Commission seeking funding to procure a contractor to assist OIT in the preparation of FMC's C&A packages for FMC network, SERVCON, and Form 1, as well as the information security program, including policies and procedures. In addition, the IG was briefed at the June 18 opening conference by the contractor of its findings and its proposal to bring the FMC up to speed on these requirements. Subject to Congressional approval of reprogramming of funds for this FISMA project, the contractor will be on board prior to the end of FY 08.

Likewise with respect to implementation of a specific Plan of Action and Milestones which would accomplish FISMA compliance, the Acting CIO's response to the FY 07 FISMA Evaluation stated that a POA&M procedure would be completed by September 30, 2008; the contractor, who will be on board prior to the end of FY 08, will be tasked with assisting OIT with developing a comprehensive POA&M process for the FMC.

Finding #3: Key Aspects of Security Program Not Implemented

Recommendation #1. Update the computer security awareness training to include an explanation of policies regarding the use of collaborative Web technologies and peer-to-peer file sharing.

Response. To comply with this recommendation, the FMC updated the computer security awareness training, effective August 7, 2008, to include an explanation of policies regarding the use of collaborative Web technologies and peer-to-peer file sharing. A link to FMC's Electronic Mail Policy and FMC's Peer to Peer Policy has been added to the end of the computer security awareness training for FY 09. To complete the mandatory training, FMC staff and contractors must view the policy and acknowledge acceptance by clicking on the "I accept" button on the policy acceptance form.

Recommendation #2. Identify systems that utilize e-authentication; perform and document an e-authentication risk assessment; assign a level; and implement the appropriate e-authentication policies, procedures, and technologies.

Response: This recommendation will be addressed by OIT's contractor as part of its comprehensive information security program review beginning in FY 08, contingent upon Congressional approval of reprogramming of funds for this FISMA project. This process will include the classification of the systems and the application of the corresponding security controls.

Recommendation #3. Implement NIST's Configuration Checklists on all FMC servers.

Response: This recommendation will be addressed by OIT's contractor as part of its comprehensive information security program review beginning in FY 08, contingent upon Congressional approval of reprogramming of funds for this FISMA project.

Finding #4: Removable Media Policies and Procedures Not Implemented

Response: This recommendation will be addressed by OIT's contractor as part of its comprehensive review beginning in FY 08, pending the approval of reprogramming of funds for this FISMA project.

Finding #4.5: Infrastructure Level Security Issues Follow-up

Response: Below are listed the three outstanding Infrastructure Security Issues identified in the contractor's June 10, 2008, report entitled "Security Compliance State Report":

Issue #1: POP services were open on numerous devices.

Issue #2: Telnet was open on numerous devices. SSH should be used instead of Telnet for remote administration.

Issue #3: The following TCP ports were open on numerous devices: 21, 25, 42, 53, and 110.

All of the ports mentioned are open on internal devices only. The FMC firewall prevents access into and out of the FMC on ports 21, 42, and 110. The firewall controls access into and out of the FMC network for ports 25 (SMTP MAIL) and 53 (DNS). Since the FMC firewall prevents information to traverse these ports to the Internet, there is no need to change our TCP port setting in response to Issue #3.

Anthony Haywood

cc: Director, Office of Information Technology