Office of Inspector General

Independent Evaluation Report of FMC's FY 2010 Implementation of FISMA

A11-01

December 2010

FEDERAL MARITIME COMMISSION

FEDERAL MARITIME COMMISSION
Office of Inspector General
Washington, DC 20573-0001

December 15, 2010

Office of Inspector General

Chairman Lidinsky:

Like all federal agencies, the FMC is becoming more dependent on information systems to carry out its regulatory mission. However such dependence increases the number and severity of threats that can have adverse impacts on its operations, assets, and employees. Given the potential for harm that can arise from environmental disruptions, human errors and "hacker" attacks, the FMC must place greater emphasis on the management of risk associated with its information systems as it carries out its mission. The cornerstone of any effort to manage organizational risk related to information systems is an effective information security program. Title III of the E-Government Act of 2002, known as the Federal Information Security Management Act (FISMA), was developed to provide a broad framework for information security programs within the federal government.

The Office of Inspector General (OIG) has completed its independent evaluation of information security pursuant to requirements contained in FISMA. This is the eighth annual evaluation completed by the OIG in the area of information and computer security.

In 2008, the Office of Information Technology (OIT) sought the assistance of an information technology contractor to perform a comprehensive assessment of its information security posture. The OIT received significant funding to address the identified weaknesses and vulnerabilities in its security program. In 2009, the contractor certified two of four agency systems. Certification is a comprehensive assessment of information system controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system. The two remaining systems did not undergo certification by the vendor. Rather, the agency planned to procure an "off-the-shelf" system to replace the two applications with plans to certify the new system after development.

In FY 2010, a new contractor began work on implementing an Enterprise Content Management (ECM) system with the goal of improving agency electronic document and records management and functional capabilities. However a dispute arose with the contractor regarding expectations and costs. Ultimately the dispute was resolved by agreement to terminate the contract. The agency intends to renew its procurement of an ECM - based on funding availability.

As a result two systems remain in production (i.e., operation) without assessment of risk to these systems and the data each houses. The two systems are the agency's Form 1, an Internet-based form to collect tariff location addresses and other specific organizational information from

conferences, ocean common carriers, transportation intermediaries and marine terminal operators; and Form 18, the agency's internet-based transportation intermediary license application. Without developing certification and accreditation (C&A) packages for these systems, FMC is unable to identify all of the risks that may be associated with operating these systems. As a result, FMC data may be exposed to unknown vulnerabilities and may not have the safeguards in-place to prevent unauthorized use, disclosure, and modification of FMC data.

The OIG contracted with Richard S. Carson and Associates to perform the independent evaluation of the FMC security program. The evaluation found that the FMC has taken steps to protect the agency's systems – most important is the accreditation two years ago of its Network and SERVCON applications - and has made progress in mitigating weaknesses which led to the prior years' significant deficiencies concerning IT risk and recovery planning. It has implemented an annual computer security awareness program with an interactive online course and a required assessment for all employees at completion. All FMC staff and contractors completed annual computer security awareness training by the end of FY 2010. The agency has taken steps to monitor contractor systems used by the agency and to update its Incident Response Policy to include breach-related procedures from the Office of Management and Budget.

In addition to two applications in production without accreditation, there are some deficiencies with the C&A packages for the FMC Network and SERVCON. Further, the agency's plan of action & milestones process needs improvement; the FMC Network Domain Administrator accounts are not formally monitored and segregated; and configuration management documentation and practices are not adequate.

FMC management cannot make credible, risk-based determinations for its systems in operation without a documented assessment and acceptance of risk to the organization. FMC management has not demonstrated a fully functional risk management process, as prescribed by the National Institute of Standards and Technology, and is not fully aware of the potential security control weaknesses in all of its systems.

I am available to discuss the report's findings and recommendations at your convenience.

Respectfully submitted,

/Adam R. Trzeciak/
Inspector General

cc: Commissioners
Managing Director

Office of Inspector General

Independent Evaluation Report

Review of Federal Maritime Commission Implementation of the Federal Information Security Management Act of 2002 For Fiscal Year 2010

December 6, 2010

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 of 2002 (FISMA). FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000 (GISRA), 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 FY 2010. This OIG Independent Evaluation Report, unlike the Reporting Template for inspectors general (IG), focuses on performance measures, provides specific findings and, when applicable, recommendations for resolution.

Objectives

The objectives of the independent evaluation of the FMC information security program are:

- Task 1 – Evaluation of Information System and Security Program: Assess compliance with FISMA and related information security policies, procedures, standards, and guidelines using criteria and methodologies contained in the Government Accountability Office (GAO) Federal Information System Controls Audit Manual (FISCAM), National Institute of Standards and Technology (NIST) Information Processing Standards and Special Publications (SP), and Office of Management and Budget (OMB) guidance. The scope of this task includes the following:
    - FMC Network
    - SERVCON
    - FORM-1
    - FORM-18

- Task 2 – Evaluation of Prior Recommendations: Review management actions to implement the OIG recommendations.
- Task 3 – Security Program Progress Review: An independent review of FMC's progress in implementing an effective information security program.

The results of our evaluations are presented in this Independent Evaluation Report, along with a number of recommendations to address vulnerabilities identified during the evaluation.

Overview of Results

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 (i) integrity—guarding against improper information modification or destruction, and ensuring information nonrepudiation and authenticity; (ii) confidentiality—preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (iii) availability—ensuring timely and reliable access to, and use of, information."

The OIG found that the FMC's Office of Information Technology (OIT) has established security safeguards to protect the agency's systems. For example, the agency conducts security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of (i) information security risks associated with their activities, and (ii) their responsibilities to comply with agency policies and procedures designed to reduce these risks. FMC had appropriate policies and procedures implemented and the process was operating effectively. However, other prescribed NIST and OMB methodologies have not been fully implemented, as detailed in this report.

In FY 2010, FORM-1 and FORM-18 continued to operate in a production environment without any documented assessment and acceptance of risk to the organization. Additionally, FMC has not corrected weaknesses identified in FY 2008 and FY 2009, including the lack of a comprehensive configuration management program. Further, no annual security control assessments or continuous monitoring was performed for any of the four FMC systems in FY 2010.

The FMC certified and accredited (C&A) two systems in FY09, including its network, and has plans to make additional improvements in its security program while implementing an enterprise content management system that would replace FORM-1 and FORM-18, complete with a C&A package. The FMC selected a contractor and is expected to complete the enterprise content management system task in the future but has not provided a written target date for completion; last year the OIG was told this would be completed by May 2010. The OIG will track the progress of the IT security program throughout FY 2011 and will follow up on the recommendations listed in this report in the OIG's FY 2011 FISMA evaluation.

In addition, the security evaluation team identified the following seven weaknesses during the FY 2010 FISMA evaluation:

- Deficiencies with the FMC C&A packages for the FMC Network and SERVCON still exist and annual assessments have not been conducted for these systems;
- The FMC plan of action & milestones (POA&M) process still needs improvement;
- FMC Network Domain Administrator accounts are not formally monitored and segregated;

- The FMC lacks an adequate Contingency Planning Program, to include policies, procedures, testing and documentation of testing;
- The FMC official system inventory is incomplete;
- Oversight of third-party (service provider) systems need improvement; and
- Configuration Management documentation and practices are not adequate.

FMC management cannot make credible, risk-based determinations for its systems in operation without a documented assessment and acceptance of risk to the organization. FMC management has not demonstrated a fully functional risk management process, as prescribed by the National Institute of Standards and Technology, and is not fully aware of the potential security control weaknesses in its systems thereby leaving its information and systems vulnerable to attack or compromise.

TABLE OF CONTENTS

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 of 2002 (FISMA). FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000 (GISRA), 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. 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.

OBJECTIVES

The objectives of the independent evaluation of the FMC information security program are as follows:

- Task 1 – Evaluation of Information System and Security Program: Assess compliance with FISMA and related information security policies, procedures, standards, and guidelines using criteria and methodologies contained in the Government Accountability Office (GAO) Federal Information System Controls Audit Manual (FISCAM), National Institute of Standards and Technology (NIST) Information Processing Standards and Special Publications (SP), and Office of Management and Budget (OMB) guidance. The scope of this task includes the following:
    - FMC Network
    - SERVCON
    - FORM-1
    - FORM-18

- Task 2 – Evaluation of Prior Recommendations: Review management actions to implement the OIG recommendations.
- Task 3 – Security Program Progress Review: An independent review of FMC's progress in implementing an effective information security program.

SCOPE AND METHODOLOGY

The scope of this independent evaluation of the FMC fiscal year (FY) 2010 information security program included the following:

- Overall Security Program Implementation
- Certification & Accreditation (C&A) process and package reviews of the FMC Network and SERVCON
- Configuration Management
- Contractor Oversight

- Contingency Planning and Testing
- POA&M Process
- Security Awareness Training
- Incident Response

To accomplish the review objectives, the OIG conducted interviews with Office of the Managing Director 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 (ISSO); and other FMC personnel.

The team reviewed documentation provided by the FMC including C&A documentation 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 Memorandum M-10-15, *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, April 21, 2010
- OMB M-04-04, *E-Authentication Guidance to Federal Agencies*, December 2003
- 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
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
- National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Information Technology Systems*, February 2006
- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, August 2009
- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, July 2002
- 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
- NIST SP 800-60, *Guide for Mapping Types of Information Systems to Security Categories*, August 2008
- NIST SP 800-70, *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*, September 2009
- *Quality Standards for Inspection* issued in 2003 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 July 7, 2010, and August 31, 2010, at the FMC headquarters in Washington, DC.

DETAILED FINDINGS AND RECOMMENDATIONS

The FMC has taken steps to enhance its information security program and address issues identified in the 2006, 2007, 2008, and 2009 FISMA reports, including the following:

- Creating C&A packages for the FMC Network and SERVCON.
- Implementing and monitoring 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 the end of FY 2010.
- Taking steps to implement 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 implement a POA&M process.

Agency Implementation of FISMA – FY 2010 Review

Notification of Finding # 1: Authorization (formerly C&A) packages have not been completed for Form-1 and Form-18 systems.

FIPS 200*, Minimum Security Requirements for Federal Information and Information Systems,* identifies specific "minimum security requirements for federal information and information systems in seventeen security-related areas. Federal agencies must meet the minimum security requirements as defined herein through the use of security controls in accordance with NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, as amended."

The agency's systems Form-1 and Form-18 (FMC-18), which have been in the operational maintenance phase of the system development life cycle for more than three (3) years, have not been assessed in accordance with NIST guidance and standards. Without this assessment the Designated Authorizing Authority (DAA) is not provided a clear picture of risk associated with these systems and has no foundation on which to base an accreditation decision upon. These systems therefore remain non-compliant with the FISMA statute.

FMC hired contractors during FY 2008 and FY 2009 to assist in the development of its IT security program by first certifying and accrediting its systems, however, the contractor was issued a "stop work order" after completion of the FMC Network and SERVCON C&A documentation. Furthermore, an enterprise document management system is planned to be implemented to replace the Form-1 and Form-18 systems.

The FMC's CIO has indicated that FMC will not perform certification and accreditation on these systems since the intent of the FMC is to replace these applications with updated technology. According to the CIO, the effort to replace these platforms is ongoing and it would not be useful to invest resources around security for them.

As a result, FMC continues to allow Form-1 and Form-18 systems to operate in the FMC production environment without a formal authorization to operate and without knowing the full risk that the systems pose to the FMC IT infrastructure.

Without developing accreditation (formerly C&A) packages for these systems, FMC is unable to identify all of the risks that may be associated with operating these systems and therefore does not have a foundation on which to base a risk based accreditation decision. As a result, FMC data may be exposed to unknown vulnerabilities and therefore may not have the safeguard in-place to prevent unauthorized use, disclosure, and modification of FMC data. In addition, users may be entering data into these systems under the false assumption that the systems are compliant with federal standards.

Recommendation

1. Formally document plans for Form-1 and Form-18 system replacements that includes, but is not limited to, explicit migration milestones and timelines.

Notification of Finding # 2: Deficiencies with FMC Certification and Accreditation packages for FMC Network and SERVCON exist and annual assessments have not been conducted for these systems in FY10.

Memorandum M-10-15, ***FY 2010 Reporting Instructions for Federal Information Security Management Act and Agency Privacy Management,*** states that certification and accreditation is required for all federal information systems. **(p. 9)**.

Memorandum M-04-04, ***E-Authentication Guidance to Federal Agencies,*** states that agencies are required to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance[1] and assists agencies in determining their e-government authentication needs. It establishes and describes four levels of identity assurance for electronic transactions requiring authentication. Assurance levels also provide a basis for assessing Credential Service Providers on behalf of federal agencies.

Agency business-process owners bear the primary responsibility to identify assurance levels and strategies for providing them. This responsibility extends to electronic authentication systems.

[1] The authentication process is used to verify the identity of a user, process or device, often as a prerequisite to allowing access to resources in an information system.

To successfully implement a government service electronically (or e-gorvernment), federal agencies must determine the required level of assurance in the authentication for each system. This is accomplished through a risk assessment for each system, which identifies both the risks to the system and the likelihood of their occurrence.

To determine the appropriate level of assurance in the user's asserted identity, agencies must assess the potential risks, and identify measures to minimize their impact. Authentication errors with potentially worse consequences require higher levels of assurance. Business process, policy and technology may help reduct risk. The risk from an authentication error is a function of two factors: (i) potential harm or impact, and (ii) the *likelihood* of such harm or impact.

At the FMC, required assurance levels for electronic transactions are determined by assessing the potential impact, for example, the unauthorized release of sensitive information on the agency and public. Accoridng to OMB M-04-04, the potential impact of an unauthorized release ranges from low to high depending on the following criteria:

- **Low—**at worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS PUB 199.

- **Moderate—**at worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS PUB 199.

- **High—**a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS PUB 199.

NIST SP 800-37*, Recommended Security Controls for Federal Information Systems*, May 2004, states that periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually **(p. 3)**. Also a C&A package shall contain an approved security plan, a security assessment report (ST&E), and a POA&M **(p. 21)**. Additionally, SP 800-37 states that the assessment of risk and the development of system security plans (SSP) are two important activities in an agency's information security program that directly support security accreditation and are required by FISMA and OMB Circular A-130, Appendix III **(p. 4)**.

Documentation should be produced that describes the process employed and the results obtained **(p. 5)**. SP 800-37 also states that system security plans can include as references or attachments other important security-related documents such as risk assessments, contingency plans, privacy impact assessments, incident response plans, security awareness and training plans, information system rules of behavior, configuration management plans, security configuration checklists, privacy impact assessments, and system interconnection agreements **(pp. 5, 21)**.

OMB Guidance M-10-15, ***FY 2010 Repporting Instructions for the Federal Information Securuty Management Act and Agency Privacy Management****,* states that for all non-national security programs and systems agencies must follow NIST standards and guidance **(p. 4)**.

NIST SP 800-18, Revision 1, ***Guide for Developing Security Plans for Federal Information Systems,*** **February 2006**, requires the use of NIST SP 800-53 security controls in the development of the security plan **(section 3.14, pp. 24-25)**. Once the security controls are selected and tailored and the common controls identified, agencies are to describe each control. The description should contain (i) the security control title; (ii) how the security control is being implemented or planned to be implemented; (iii) any scoping guidance that has been applied and what type of consideration; and (iv) indicate if the security control is a common control and who is responsible for its implementation **(section 3.1.4, pp. 24-25)**.

NIST SP 800-30, ***Risk Management Guide for Information Technology Systems,*** **July 2002**, differentiates security testing and evaluation (ST&E) from automated vulnerability scanning and penetration testing. The purpose of system security testing is to test the effectiveness of the security controls of a system as they have been applied in an operational environment. In contrast, the potential vulnerabilities identified by automated scanning may not represent real vulnerabilities in the context of the system environment. Similarly, penetration testing is used to test the system from the viewpoint of a threat-source and to identify potential failures in the IT system protection schemes **(section 3.3.2, pp. 17-18)**.

NIST SP 800-34, ***Contingency Planning for Information Technology Systems,*** **dated June 2002**, states that recovery strategies provide a means to restore information technology (IT) operations quickly and effectively following a service disruption. The strategies should address disruption impacts and allowable outage times identified in the Business Impact Assessment (BIA). Several alternatives should be considered when developing the strategy, including cost, allowable outage time, security, and integration with larger organization-level contingency plans **(section 3.1, p. 19)**.

Federal Information Processing Standards Publication 199 (FIPS PUB 199), ***Standards for Security Categorization of Federal Information Systems,*** **February 2004**, provides standards for categorizing information and information systems. Security categorization standards for information and information systems provide a common framework and understanding for expressing security that promotes: (i) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and (ii) consistent reporting to the OMB and Congress on the adequacy and effectiveness of information security policies, procedures, and practices. Subsequent NIST standards and guidelines will address the second and third tasks cited **(section 1, p. 1)**.

Agency officials shall use the security categorizations described in FIPS PUB 199 whenever there is a federal requirement to provide such a categorization of information or information systems. Additional security designators may be developed and used at agency discretion. State, local, tribal governments, as well as private sector organizations comprising the critical

infrastructure of the United States may consider the use of these standards as appropriate **(section 2, p. 1)**.

FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006, specifies requirements for federal information and information systems in seventeen security-related areas. Federal agencies must meet the minimum security requirements as defined herein through the use of the security controls in accordance with NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, as amended.

NIST SP 800-60, *Guide for Mapping Types of Information Systems to Security Categories,* Volumes I & II, August 2008, was developed to help agencies consistently map security impact levels to types of: (i) information (e.g., privacy, medical, proprietary, financial, contractor sensitive, trade secret, investigation); and (ii) information systems (e.g., mission critical, mission support, administrative). This guideline applies to all federal information systems other than *national security systems*. *National security systems* store, process, or communicate *national security* information **(section 1.1 p. 1)**.

Certification & Accedrediation Packages

The FMC did not perform annual security control assessments on its accredited systems (the FMC Network and SERVCON) in FY10. NIST encourages agencies to consider the C&A package to be "living" documents, and control assessments should be performed on an ongoing basis to ensure that the system continues to operate at an acceptable security level.

The OIG-identified deficiencies in last year's C&A packages generally reamin uncorrected. The agency has addressed one review finding by matching the security categorizations for the FMC Network and SERVCON with the security categorizations listed in the POA&Ms. However, most deficiencies noted remain uncorrected.

We reviewed the individual documents of each package to evaluate their adherence to other relevant NIST and OMB guidance. The C&A packages contained a privacy impact assessment, security plan, risk assessment, certification and accreditation statements, POA&M, FIPS 199 system categorization, contingency plan, system test and evaluation, configuration management plan, e-authentication risk assessment and security control assessment.

Continuous Monitoring

Vulnerability scanning includes scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms. Vulnerability scans were conducted on the FMC Network and SERVCON on August 2, 2010, to partially comply with NIST guidance for continuous monitoring.

Nothwithstanding vulnerability scans, no evidence was provided to indicate that annual security control assessments were conducted in accordance with NIST SP 800-53A on these systems in

FY10 as required by NIST SP 800-37. A security control assessment is more than a scan; it is also includes the testing and/or evaluation of the management, operational and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Security Plans

While the FMC Network and SERVCON security plans were generally compliant with NIST SP 800-18 guidance, review of the security plans last year found that sections of the security plans were either not completed or completed incorrectly. In its response to the recommendation last year, management indicated that its System Security Plans (SSP) were completed according to NIST SP 800-18. However, we noted the following deficiencies again in FY10 that fall short of NIST SP 800-18 requirements:

- The security plans (and C&A packages) do not contain unique identifiers for each system.
- Certifying Agent (CA) and Designated Approving Authority (DAA) titles are not clearly identified as required by NIST SP 800-37.
- E-mail addresses for key personnel are not provided.
- Minor applications are not identified, nor is there a statement that there are no minor applications associated with the general support system (FMC Network).
- A list of user organizations was not provided (This may not be an issue based upon the size of FMC, but there was no clear discussion of the user community). Presently, this section and related table identifies switches, e-mail systems, firewalls, and gateways used by the applications.
- There is no discussion of interconnections between systems. Specifically, there should be a list of systems that share data between applications. If there are none, this should be stated in the security plan in the appropriate section.
- Security plans for systems processing privacy act information did not include the number and title of the system(s) of record and whether the system(s) is used for computer-matching activities.
- Common controls were not specifically identified, although common controls were identified in the risk assessments.
- Signature and date fields were blank on the approval sheets in the copies of the security plans provided. Additionally, the names of personnel listed as the signatories did not match the individuals who signed the C&A statements.

No system security plan updates were made in FY10. Therefore the deficiencies remain uncorrected.

Risk Assessments

Review of the FMC Network and SERVCON risk assessments found the risk assessments were generally based upon SP 800-30 and addressed most of the areas covered by the guidance, including the risk assessment approach, system security categorization, threats, and a detailed

analysis. The FMC Network risk assessment was completed on May 26, 2009, and the SERVCON risk assessment was completed on May 27, 2009, as part of the C&A effort. However, the following deficiencies were identified in last year's review and continue to exist:

- Accreditation boundaries for the risk assessment, which define the scope of the C&A packages, were not clearly defined. For example, all components of the information system to be authorized for operation by the authorizing official were not clearly defined.
- System and data owners were not clearly identified in the Network Risk Assessment; the data owner was not clearly identified in the SERVCON Risk Assessment.

Parts of the documents were incomplete. Specifically, the System Management Roles and the System User Group and Access tables are incomplete in each risk assessment. These tables list the roles and access levels for IT and other user groups in an effort keep them appropriately segregated.

No annual security control testing for either system was performed in FY10 and no risk assessments were performed as required by NIST SP 800-30.

E-Authentication Risk Assessments

OMB Memorandum 04-04, *E-Authentication guidance to Federal Agencies*, describes four identity authentication assurance levels for e-government transactions. In this context, assurance is the level of confidence that the individual who uses a credential or password is the individual to whom the credential (or password) was issued. There are four assurance levels:

- Level 1: Little or no confidence in the asserted identity's validity;
- Level 2: Some confidence in the asserted identity's validity;
- Level 3: High confidence in the asserted identity's validity; and
- Level 4: Very high confidence in the asserted identity's validity.

OIT performed an E-authentication risk assessment on FMC's SERVCON that concluded the system requires a Level 2 authentication. However, OIT also categorized SERVCON as a high impact system during the FIPS 199 required categorization, meaning that a breach or unauthorized access or loss of data might cause a "severe or catastrophic" adverse effect on the agency's operations, assets or individuals.

It is inconsistent to have a level 2 assurance level for a system that has been categorized at a high impact level for data confidentiality in accordance with FIPS 199. Systems with high impact levels, as is the case regarding SERVCON, require Level 4 authentication.

C&A Letters

Review of the document found that certification and authorization to operate statements (C&A letters) dated June 4, 2009, for the FMC Network and SERVCON were contained in each document. However, the C&A letters identified the following minor deficiencies:

- The CIO is not clearly identified as the Designated Approving Authority.
- The Information System Security Officer signed the certification statement as the Authorizing Official instead of the Certifying Agent, which would appear to be a conflict of interest because of a lack of segregation of duties (i.e., the same individual responsible for ensuring the security control and risk assessments are performed is also formally accepting the risk of operating the system in the production environment based on those same results).
- The certification statement does not mention the contractors who operated as independent certification agents, as required by NIST SP 800-53 for "moderate" and "high" categorized systems.

FIPS 199 Security Categorization

The security categorizations were completed for the FMC Network and SERVCON.

Contingency Plans

Contingency plans were developed for the FMC Network (dated May 18, 2009) and SERVCON (dated March 19, 2009). Our FY10 review of the completed FMC Network and SERVCON contingency plans revealed that:

- Alternates to team leads are not identified for the FMC Network contingency plan.
- The phone trees for the contingency plans are incomplete for the FMC Network contingency plan.
- Contact information for alternates to team leads is incomplete.
- The contingency plans did not include service level agreements.
- A Business/Mission Impact Analysis has not been completed for each system.

Most conditions identified last year remained in FY10. Further, no contingency plan updates for contact information were conducted in FY10.

The contractor completed the C&A documentation; however, the documentation does not fully comply with NIST guidance.

Annual security control assessments were not performed for SERVCON and the general support system (GSS). OIT officials believe that control assessments from FY09 were sufficient and that control assessments in FY10 were unnecessary notwithstanding federal requirements that mandate annual testing.

IT threats and vulnerabilities change continuously. To conclude that annual testing is unnecessary fails to recognize this reality. Without developing and maintaining comprehensive C&A packages for all systems, FMC is unable to identify all of the security vulnerabilities associated with operating their systems. Additionally, without the appropriate FMC personnel being made aware of the risk associated with the system operating in the FMC production environment and formally accepting the risks, the FMC data being processed, stored, or transmitted by these production systems may be exposed to unknown risks.

Recommendations

Most of these conditions have existed over the past two (2) FISMA engagements. Therefore, we are repeating the recommendations from the prior FISMA review. We recommend OIT:

2. Clearly identify the Certifying Agency, Designated Approving Authority, and system owner in the security plans and C&A documentation in accordance with NIST SP 800-37 as amended.
3. Conduct complete risk assessments on accredited FMC systems (FMC Network and SERVCON). Define accreditation boundaries. Ensure that risk assessments are complete in accordance with NIST SP 800-30 as amended.
4. Conduct control assessments in accordance with FIPS 200, NIST SP 800-53 as amended, and NIST SP 800-37 as amended.
5. Complete the Authority to Operate letters with the correct information and titles.
6. Correct the e-authentication risk assessment for SERVCON. SERVCON requires Level 4 authentication.

Notification of Finding # 3: The FMC Plan of Action & Milestones process is inadequate.

OMB Memorandum 04-25*, FY 2004 Reporting Instructions for the Federal Information Security Management Act* defines a POA&M as a tool identifying tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of a 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.

A POA&M can be thought of as a blueprint for prioritizing and tracking corrective actions.

Review of the FMC Network and SERVCON POA&Ms found that POA&M action items came from various sources such as system security plan findings, the office of Equal Employment Opportunity, Office of Operations, and the Office of the Managing Director.

OMB Memorandum 04-25, also requires agencies to prepare POA&Ms for all programs and systems where an IT security weakness has been found. The guidance directs CIOs and agency program officials to develop, implement, and manage POA&Ms for all programs and systems they operate and control (e.g., for program officials this includes all systems that support their operations and assets). Additionally, program officials should regularly (at least quarterly and at the direction of the CIO) update the agency CIO on their progress to enable the CIO to monitor agency-wide remediation efforts and provide the agency's quarterly update to OMB. Memorandum 04-25 also provides instructions on how POA&Ms should be structured and maintained **(pp. 14-15)**.

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, dated August 2009, states that control MP-3 requires organizations to mark, in accordance with organizational policies and procedures, removable information

system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.

FMC developed POA&Ms in FY09 for the FMC Network and FMC SERVCON. The POA&M documents generally contain the required elements as identified in OMB guidance. However, the agency has not completed POA&Ms properly. The OIG found that ID numbers are not assigned to POA&M items for either system. Most importantly, the review also found that the resources required to complete the task were not identified, and the milestones with completion dates were not identified. Without resource requirements and target dates to hold officials accountable, the POA&Ms become little more than a "to-do" list that is addressed on a "when time is available basis."

Through inspection of the documentation and interviews with OIT staff, the OIG determined that the OIT staff has minimally utilized the FMC Network and SERVCON POA&Ms. That is, no tasks have been added over the past year, and only one low-risk item (Voice Over Internet Protocol (VOIP) now implemented) has been closed for each system respectively. The FMC had a total of 60 POA&M items in FY09 and 59 in FY10 for the Network and SERVCON respectively. Most of these open POA&M items have scheduled completion dates of 2009.

Through inspection of the documentation and interviews with OIT staff, the OIG determined that the OIT staff have minimally utilized the FMC Network and SERVCON POA&Ms, but have not allocated sufficient resources to implement a more effective POA&M process.

Without an effective POA&M process, including the tracking of resources required to complete tasks and milestones with completion dates, it is more difficult for the agency to identify and prioritize weaknesses or track the status of the corrective actions being taken to resolve identified deficiencies. This could lead to vulnerabilities not being corrected and the continued exposure of FMC systems to higher levels of risk.

Recommendations

With regard to systems that will be retained, FMC OIT should develop and document an OMB-compliant POA&M process (i.e., one that closes POA&M items more efficiently and reduces the risk to sensitive FMC information).

In summary FMC OIT should:

7. As recommended in FY09, develop a POA&M process for systems that will be retained complete the POA&Ms in accordance with current OMB and NIST guidance, and maintain evidence of the closure of each item.

Notification of Finding # 4: FMC Network Domain Administrator accounts are not formally monitored and segregated.

NIST SP 800-53, Revision 3, ***Recommended Security Controls for Federal Information Systems and Organizations****,* dated August 2009, recommends that organizations shall:

- Establish and administer privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and tracks and monitors privileged role assignments.
- Employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
- Review and analyze information system audit records at an organization-defined frequency for indications of inappropriate or unusual activity, and report findings to designated organizational officials.

NIST SP 800-53, Revision 3*, Recommended Security Controls for Federal Information Systems and Organizations*, dated August 2009, also recommends that the information system protects against an individual falsely denying having performed a particular action.

FMC has stated that only the senior network engineer has access to the domain administrator account and that the password to this account is locked in a safe. This permits the administrator to perform actions without being accountable for those actions because the domain administrator account is not assigned to a specific individual. In addition, because the administrator is the only person who knows the administrator authenticators, she/he constitutes a single point of failure. For example, should the administrator become unavailable for any reason FMC would be unable to continue IT operations effectively.

The creation of an administrator group and the assignment of administrator privileges to individuals under this group permits administrators to perform activities that can be traced directly back them. This is an industry best practice and OIT officials told us that the FMC employs this practice with four FMC administrators. However, allowing any administrator using the Domain Administrator Account, which does not reside under this group except under the most controlled circumstances, permits the administrator to perform those activities without being held accountable. This is because the Domain Administrator Account cannot be unequivocally assigned to one person in a manner that allows the system logs to identify a specific individual within the log files themselves. Accountability for the use of this account must be established and tracked by other means.

As was the case in FY09, a formal process for segregating and monitoring user and privileged accounts, including the Domain Administrator account, is not implemented.

In its FY09 response to this recommendation, management told the OIG that it was developing a process by which every 90 days the domain administrator account password would be manually changed and physically secured in a designated location so it is only available in authorized and documented network changes and/or emergencies. This process will be in place by the end of the first quarter of fiscal year 2010. In this report, management continued as follows: “[FMC OIT] realize[s] the need for a proactive network access monitoring process and will seek to identify a hardware or software solution that will allow the ISSO the ability to receive alerts based on predetermined criteria relating to network access. This process will be in place by the end of the third quarter of fiscal year 2010.”

The cause, as communicated by management for the last three years, for utilizing the domain administrator account for performing administrative duties is that it is not practical to follow industry best practice to log each use. The FMC also informed the OIG that informal monitoring by the ISSO is performed on a monthly basis; therefore, a formal monitoring process is not necessary.

Without changing the password of the FMC Network domain administrator account, and restricting access to the password so that it is only available for authorized and documented network changes and/or emergencies, there is no assurance of accountability and there exists a potential single point of failure. Further, without appropriately monitoring usage of the privileged FMC Network account(s), authorized and unauthorized changes to the network may occur without the necessary accountability, which may affect the overall confidentiality, integrity, and availability of the system.

Recommendations

We recommend OIT –

8. Review and implement FMC's policies and procedures (and, if determined necessary, hardware and/or software) for the ISSO to monitor the actions of all FMC Network user, and privileged (super user) accounts such as the top tier Domain Administrator Account and the administrator accounts under the Domain Administrator Group.

9. The FMC Network Domain Administrator user account should be changed in accordance with FMC password policy, and physically secured to restrict its access. The CIO or his designated representative should control the access and use of the password so that this password is only made available for authorized and documented network changes and/or emergencies. This would ensure accountability and avoid any potential for a single point of failure. The process for handling the FMC Domain Administrator account should be documented.

10. If regular Domain Administrator Account use is deemed necessary without employing the recommended procedures or other means that effectively enforces user accountability, FMC should:

    a. Document the reason for this need.

    b. Perform a risk assessment in accordance with NIST SP 800-30 to determine the level of risk associated with this practice.

    c. Develop a stand-a-lone document, or update the FMC LAN system security plan to reflect the acceptance of risk.

    d. The designated approval authority for the FMC LAN should accept responsibility for the risk associated with this practice in writing.

Notification of Finding # 5: FMC lacks an adequate Contingency Planning Program to include policies, procedures, testing, and documentation of testing.

According to NIST SP 800-34, *Contingency Planning for Information Technology Systems*, dated June 2002, recovery strategies provide a means to restore IT operations quickly and effectively following a service disruption. The strategies should address disruption impacts and

allowable outage times identified in the Business Impact Assessment (BIA). Several alternatives should be considered when developing the strategy, including cost, allowable outage time, security, and integration with larger, organization-level contingency plans.

The selected recovery strategy should address the potential impacts identified in the BIA and should be integrated into the system architecture during the design and implementation phases of the system life cycle. The strategy should include a combination of methods that complement one another to provide recovery capability over the full spectrum of incidents. A wide variety of recovery approaches may be considered. The appropriate choice depends on the incident, type of system, and its operational requirements. Specific recovery methods further described in section 3.4.2 should be considered and may include commercial contracts with cold-, warm-, or hot-site vendors, mobile sites, mirrored sites, reciprocal agreements with internal or external organizations, and service level agreements (SLA) with the equipment vendors. In addition, technologies such as Redundant Arrays of Independent Disks, automatic fail-over, uninterruptible power supply, and mirrored systems should be considered when developing a system recovery strategy.

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* dated August 2009, states that organizations shall test and/or exercise the contingency plan for the information system to determine the plan's effectiveness and the organization's readiness to execute the plan and that organizations shall provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

FMC took part in the Federal Emergency Management Agency's Eagle Horizon 2009 continuity mandatory exercise for all federal executive branch departments and agencies. Additionally, according to an e-mail message from the FMC Director of OIT, a test in FY 2010 focused on the following items: reconfigured continuity of operations site primary domain controller, tested connectivity to FMC domain, tested replication of data, tested remote/Virtual Private Network, application access, telephone service, and e-mail access in the event of a disruption. However, based upon review of the contingency plans and documentation provided, the following conditions were noted:

- FMC does not have documented contingency planning policies and procedures for identifying the frequency of testing, types of testing, and preparing and updating of contingency documentation;
- The following FMC applications have not been tested:
    - SERVCON
    - Form-1
    - Form-18 (FMC-18)
- The following systems do not have contingency plans:
    - Form-1
    - Form-18 (FMC-18)
- The FMC Network contingency plan test in 2010 and results documentation do not adequately test or document the FMC Network contingency plan. No information was available to describe the scenario that was being tested. Testing appeared to concentrate

on determining if the applications were working, e-mail could be sent, or the Internet could be accessed. No recommendations or lessons learned were identified.

As was the case in FY09, FMC has not allocated the necessary resources to create a fully functional contingency planning program to include appropriate testing and documentation of the testing.

Delays, confusion, and the potential introduction of vulnerabilities when recovering from a system failure are likely when contingency plans are incomplete and have not been tested. Not testing contingency plans could result in errors or incorrect steps being embedded in the security plan, which could further hinder the recovery process.

Recommendations

We are repeating the following recommendation made in FY09:

11. Develop a contingency plan policy and procedures that address the creation, review, testing, and maintenance of contingency plans. Test contingency plans and document results in accordance with NIST SP 800-34 and NIST SP 800-53.

Notification of Finding # 6: FMC official system inventory is incomplete.

NIST SP 800-53, Revision 3, ***Recommended Security Controls for Federal Information Systems and Organizations*****, dated August 2009**, states that control (CM-8) requires organizations to develop, document, and maintain an inventory of information system components that meet the following requirements:

- Accurately reflects the current information system;
- Is consistent with the authorization boundary of the information system;
- Is at the level of granularity deemed necessary for tracking and reporting;
- Includes organization-defined information deemed necessary to achieve effective property accountability; and
- Is available for review and audit by designated organization officials.

The FISMA states the following:

> ‘‘(c) INVENTORY OF MAJOR INFORMATION SYSTEMS—(1) The head of each agency shall develop and maintain an inventory of major information systems (including major national security systems) operated by or under the control of such agency.”
> “(2) The identification of information systems in an inventory under this subsection shall include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.”

The following condition also existed in FY09:

During FY 2008, OIT hired contractors to create a security program and to certify and accredit FMC's systems. The contractors distributed inventory forms to all FMC departments to identify the systems in operation. The returned forms became the "FMC inventory." In addition to the FMC Network and SERVCON systems, which the contractor created C&A packages for, the forms were returned from each FMC department and identified the following systems:

- BEAA
- BOE Index
- e-agreements
- Form-1
- Form-18 (FMC-18)
- OIG
- PIERS
- SERVCON (External)
- Training

A complete inventory, in addition to simply identifying systems, must contain IT system interfaces according to FISMA. An interface is a common interconnection between systems by which equipment or programs communicate information from one system to another.

Additionally, the following systems, which were identified in the system inventory under the heading Database System Inventory Assets, did not have C&A packages and were not identified in the official system inventory as subsystems under the GSS:

- BEAA
- eAgreements
- PIERS
- Training
- BOE Index
- OIG

Through inspection of the documentation and interviews with OIT staff, it was determined that the OIT staff was relying on documentation produced and distributed by the contractor.

The inventory does reflect a hirarchtical structure that clearly depicts which systems are major applications that require an accreditation (formerly C&A) packages from the systems which are minor applications that reside under a major application.

Without documenting and implementing an effective inventory process, FMC management may not be aware of all FMC systems in operation in the IT environment. Without the official system inventory being consistent with the authorization boundaries of the information systems and without diagrams detailing system interconnections, FMC may not scope and tailor the security controls for each system correctly.

Recommendations

We recommend OIT –

12. Complete and maintain an official system inventory of all FMC systems and interfaces.
13. Organize the FMC inventory in a hierarchal fashion (i.e., which systems are subordinate to the GSS).

Notification of Finding # 7: Third-Party Oversight deficiencies.

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, dated August 2009:

- Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
- Defines and documents government oversight and user roles and responsibilities with regard to external information system services.
- Requires organizations to monitor security control compliance by external service providers.

We requested a copy of the documented FMC methodology for performing oversight and evaluation on contractor systems and systems hosted at other government agencies and were informed that none existed. Also SLAs and contracts were not provided for all systems.

OIT did not know the answers to the following items:

- The number of contractor systems that service FMC by FIPS 199 category
- The number of contractor systems that service FMC by C&A status
- The number of contractor systems that service FMC by whether annual testing occurred
- The number of contractor systems that service FMC by whether a tested contingency plan exists
- The number of agency-owned and contractor systems that service FMC assessed at e-authentication levels 3 or 4

Oversight methodology should be included in a SLA with the external service provider. The government Contracting Officer's Technical Representative reserves the right to verify that the contractor is complying with the contract. At the defined frequency for this process (to be at least once a year), FMC should meet with the contractor and, if necessary, create findings on the POA&M. A document/memo should be created each time that oversight is performed.

The Authority to Operate (ATO), Interconnection Security Agreement (ISA), and Memorandum of Understanding (MOU) between FMC and the Bureau of Public Debt (BPD) have all expired as of FY09. The ATO, ISA, and MOU between FMC and the National Finance Center (NFC)

were current. We noted that the ATO and MOU between FMC and OPM for eOPF were current. However, the ISA between FMC and OPM was not provided.

The FMC informed the OIG that it is not FMC's responsibility to perform these monitoring activities. However according to NIST 800-53, oversight of third parties is a responsibility of FMC.

Without appropriately monitoring security control compliance by external service providers, the risk of security incidents increases that could potentially affect the overall confidentiality, integrity, and availability of the FMC data shared with an external system.

Recommendations

We recommend that FMC:

14. Define and document policies and procedures for an oversight methodology of external information system services with contractors. At the defined frequency for this process (at least once a year), FMC should meet with the contractor and, if necessary, create findings on the POA&M. A document/memo should be created each time that oversight is performed.
15. Monitor security control compliance by external service providers and maintain an inventory of the following items:

    - The number of contractor systems that service FMC by FIPS 199 category
    - The number of contractor systems that service FMC by C&A status
    - The number contractor systems that service FMC by whether annual testing occurred
    - The number of contractor systems that service FMC by whether a tested contingency plan exists
    - The number of agency-owned and contractor systems that service FMC assessed at e-authentication levels 3 or 4
16. Maintain Authority to Operate (ATO) letters, Interconnection Security Agreements (ISA), and Memoranda of Understanding (MOU) between FMC and external service providers.

Notification of Finding # 8: Configuration Management documentation and practices are not adequate.

An information system is typically in a constant state of change in response to new or enhanced hardware and software capability, patches for correcting errors to existing components, new security threats, and changing business functions, etc. Implementing information system changes almost always results in some adjustment to the system baseline configuration. To ensure that the required adjustments to the system configuration do not adversely affect the information system security, a well-defined security configuration management process is needed.

Configuration Management comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems. The practice of configuration management is implemented through the establishment of the baseline configuration.

The configuration of an information system and its components has a direct impact on the security posture (i.e., the ability to protect the confidentiality, integrity, and availability of information stored, processed, or transmitted) of the system. How those configurations are established and maintained requires a disciplined approach for providing adequate security.

FISMA requires agencies to establish "minimally acceptable system configuration requirements" within their information security program, and NIST SP 800-53 defines a set of security controls which support this requirement.

NIST SP 800-53 rev. 3*, Recommended Security Controls for Federal Information Systems and Organizations,* dated August 2009 states that organizations shall:

- Develop, disseminate and revive/update at an organization-defined frequency:
  a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
  b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

- Develop, document, and maintain under configuration control, a current baseline configuration of the information systems.
- Determine the types of changes to the information system that are configuration controlled;
- Approve configuration-controlled changes to the system with explicit consideration for security impact analyses;
- Document approved configuration-controlled changes to the system;
- Retain and review records of configuration-controlled changes to the system;
- Audit activities associated with configuration-controlled changes to the system; and
- Coordinate and provide oversight for configuration change control activities through an organization-defined configuration change control element (e.g., committee, board) that convenes at an: organization-defined frequency to discuss organization-defined configuration change conditions.

In addition, NIST requires agencies to:

- Analyze changes to the information system to determine potential security impacts prior to change implementation.
- Define, document, approve and enforce physical and logical access restrictions associated with changes to the information system.

- Establish and document mandatory configuration settings for information technology products employed within the information system using organization-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements;
- Implement the configuration settings;
- Identify, document, and approve exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
- Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.
- Configure the information system to provide only essential capabilities that specifically prohibits or restricts the use of organization-defined prohibited or restricted functions, ports, protocols, and/or services.
- Develop, document, and implement a configuration management plan for the information system that:

    a. Addresses roles, responsibilities, and configuration management processes and procedures;
    b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and
    c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

NIST SP 800-37 ***Guide for the Security Certification and Accreditation of Federal Information Systems*** **dated May 2004**, identifies configuration management and configuration control processes as part of a critical aspect of the security certification and accreditation process during the post-accreditation period involving the continuous monitoring of security controls in the information system over time. The guidance goes on to state that it is important to document the proposed or actual changes to the information system and to subsequently determine the impact of those proposed or actual changes on the security of the system.

NIST SP 800-70 ***Security Configuration Checklists Program For IT Products Guidance for Checklists Users and Developer*** **dated May 2005**, provides approved security configuration checklists for a variety of operating systems, web browsers, firewalls, antivirus software, and productivity tools.

The OIT provided a Configuration Management Policy, dated May 16, 2007. The evaluation team noted that the policy requires a baseline configuration, change control and testing when changing the baseline configuration. All FMC servers utilize a Server Build Document when configuring the servers and uses the Group Policy Objects and Desktop Authority scripts on the "ghost" image; all other configuration management is performed according to an undocumented process. Additionally, the ISSO explained that additional thumb drive restriction policies had been implemented through ScriptLogic. The senior network engineer applies software patches in a timely and secure manner in accordance with Patch Management Policy OIT-P12.

The review determined that FMC has created a Configuration Management Policy, implemented the Federal Desktop Core Configuration for its workstations, and created a "server build checklist." However, a baseline configuration for the FMC Network and deviations from the baselines are not documented.

Additionally, the GSS and SERVCON Technical Architecture documents did not address security controls in sufficient detail. Specifically, NIST requires that information should be provided on security baselines to be used, frequency of security baseline updates and steps to ensure security baselines are being followed. The following sections were found to be incomplete:

- Portal requirements table;
- User roles and groups tables;
- Firewall configuration; and
- Document sign off.

FMC hired a contractor who worked during FY 2008 and FY 2009 to create its IT security program, however, the contractor was issued a "stop work order" after completion of the FMC Network and SERVCON C&A documentation. Through inspection of the documentation and interviews with OIT staff, the OIG determined that OIT staff has not allocated the necessary resources to create a fully-functional configuration management program.

The effect of not having a completed, up to date and detailed configuration management program is that baseline security settings do not exist for FMC systems. Without a baseline for servers and documented deviations, there could be confusion among individuals responsible for configuring or validating security settings as to whether security settings are in place and/or create a false sense of security. This could make the systems vulnerable to hacking, computer viruses, and other exploits.

Recommendations

These conditions have existed over the past two (2) FISMA engagements. Therefore, we are repeating the recommendations from the prior FISMA review. We recommend OIT –

17. Complete the SERVCON and GSS configuration management documentation to include the sections missing, as identified in the condition section, above. Additionally, confirm that the SERVCON and future configuration management plans address the following sections, in accordance with NIST SP 800-53 Revision 3:

    - Security control, port and firewall settings
    - Allowable and non-allowable services
    - Hardware and software requirements
    - Patches and service packs
    - Establish system and application baselines and document the deviations from the baselines.

18. Implement the NIST National Checklist Program for FMC servers and utilize a Security Content Automation Protocol (SCAP) scanner to verify NIST baseline security configurations for servers. Additionally, document any deviations from the baseline security configurations along with the reasons.

UNITED STATES GOVERNMENT FEDERAL MARITIME COMMISSION

Memorandum

TO : Office of the Inspector General **DATE:** December 9, 2010

FROM : Chief Information Officer

SUBJECT : Responses to FY 2010 FISMA Notification of Findings

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

Finding 1

Recommendation 1: Formally document plans for Form-1 and Form-18 system replacements that includes but is not limited to explicit migration milestones and timelines.

Response: Management is reassessing Form-1 and Form-18 system replacements. At the appropriate time, plans that include milestones and timelines will be developed. Various factors, including new policies and procedures, combined with contractual and funding impediments, have delayed progress. An update on agency progress for this recommendation will be provided at the end of the third quarter of FY 2011.

Finding 2

Recommendation 2: Clearly identify the Certifying Agency, Designated Approving Authority, and system owner in the security plans and C&A documentation in accordance with NIST SP 800-37 as amended.

Response: Evidence satisfying this recommendation was provided at a meeting on October 26, 2010 with the Inspector General, the Chief Information Officer, the Director of the Office of Information Technology, the Information Systems Security Officer, and the contracted auditors from Richard S. Carson & Associates. Evidence is again provided in the accompanying CD. **Corrective action under this recommendation is considered completed.**

Recommendation 3: Conduct complete risk assessments on accredited FMC systems (FMC Network and SERVCON). Define accreditation boundaries. Ensure that risk assessments are complete in accordance with NIST SP 800-30 as amended.

Response: Evidence satisfying this recommendation was provided at a meeting on October 26, 2010 with the Inspector General, the Chief Information Officer, the Director of the Office of

Information Technology, the Information Systems Security Officer, and the contracted auditors. Evidence is again provided in the accompanying CD. **Corrective action under this recommendation is considered completed.**

Recommendation 4: Conduct control assessments in accordance with FIPS 200, NIST SP 800-53 as amended, and NIST SP 800-37 as amended.

Response: Management concurs, and advice concerning control assessments will be provided by the end of the third quarter of FY 2011.

Recommendation 5: Complete the Authority to Operate letters with the correct information and titles.

Response: Evidence satisfying this recommendation was provided at a meeting on October 26, 2010 with the Inspector General, the Chief Information Officer, the Director of the Office of Information Technology, the Information Systems Security Officer, and the contracted auditors. Evidence is again provided in the accompanying CD. **Corrective action under this recommendation is considered completed.**

Recommendation 6: Correct the e-authentication risk assessment for SERVCON. SERVCON requires Level 4 authentication.

Response: Management will reevaluate whether raising the risk level for SERVCON is warranted. Advice concerning this recommendation will be provided by the end of the third quarter of FY 2011.

Finding 3

Recommendation 7: As recommended in FY 09, develop a POA&M process for systems that will be retained, complete the POA&Ms in accordance with current OMB and NIST guidance, and maintain evidence of the closure of each item.

Response: Evidence satisfying this recommendation was provided at a meeting on October 26, 2010 with the Inspector General, the Chief Information Officer, the Director of the Office of Information Technology, the Information Systems Security Officer, and the contracted auditors. Evidence is again provided in the accompanying CD. **Corrective action under this recommendation is considered completed.**

Finding 4

Recommendation 8: Review and implement FMC's policies and procedures (and, if determined necessary, hardware and/or software) for the ISSO to monitor the actions of all FMC Network user [sic], and privileged (super user) accounts such as the top tier Domain Administrator Account and the administrator accounts under the Domain Administrator Group.

Response: Management will review its current policies and, if necessary, will take appropriate action to develop revised written procedures by the end of FY 2011.

Recommendation 9: The FMC Network Domain Administrator user account should be changed in accordance with FMC password policy, and physically secured to restrict its access. The CIO or his designated representative should control the access and use of the password so that this password is only made available for authorized and documented network changes and/or emergencies. This would ensure accountability and avid any potential for a single point of failure. The process for handling the FMC Domain Administrator account should be documented.

Response: Management does not agree with this opinion, and is in the process of formulating policies and written procedures for the use and monitoring of the Domain Administrator account. Management's decision concerning this recommendation will be provided by the end of the third quarter of FY 2011.

Recommendation 10: If regular Domain Administrator Account use is deemed necessary without employing the recommended procedures or other means that effectively enforces user accountability, FMC should: (a) Document the reason for this need; (b) Perform a risk assessment in accordance with NIST SP 800-30 to determine the level of risk associated with this practice; (c) Develop a stand-a-lone [sic] document, or update the FMC LAN system security plan to reflect the acceptance of risk; and (d) The designated approval authority for the FMC LAN should accept responsibility for the risk associated with this practice in writing.

Response: Management is in the process of formulating policies and written procedures for the use and monitoring of the Domain Administrator account. Management's decision concerning this recommendation will be provided by the end of the third quarter of FY 2011.

Finding 5

Recommendation 11: Develop a contingency plan policy and procedures that address the creation, review, testing, and maintenance of contingency plans. Test contingency plans and document results in accordance with NIST SP 800-34 and NIST SP 800-53.

Response: As noted by the auditors, contingency plans have been developed for the FMC's systems that have been certified and accredited. Management will continue to improve and refine its contingency plan testing procedures.

Finding 6

Recommendation 12: Complete and maintain an official system inventory of all FMC systems and interfaces.

Response: Evidence satisfying this recommendation was provided at a meeting on October 26, 2010 with the Inspector General, the Chief Information Officer, the Director of the Office of Information Technology, the Information Systems Security Officer, and the contracted auditors. Evidence is again

provided in the accompanying CD. **Corrective action under this recommendation is considered completed.**

Recommendation 13: Organize the FMC inventory in a hierarchal fashion (i.e., which systems are subordinate to the GSS).

Response: Management disagrees with this recommendation, and has determined that the FMC inventory is satisfactory. **Corrective action under this recommendation is considered completed.**

Finding 7

Recommendation 14: Define and document policies and procedures for an oversight methodology of external information system services with contractors. At the defined frequency for this process (at least once a year), FMC should meet with the contractor and, if necessary, create findings on the POA&M. A document/memo should be created each time that oversight is performed.

Response: Management agrees with this recommendation and will document our current procedure to contact contractors yearly for their C&A status, which will satisfy the need to provide external information systems oversight. Updated advice concerning this recommendation will be provided by the end of the third quarter of FY 2011.

Recommendation 15: Monitor security control compliance by external service providers and maintain an inventory of (1) the number of contractor systems that service FMC by FIPS 199 category; (2) the number of contractor systems that service FMC by Certification and Accreditation status; (3) the number of contractor systems that service FMC by whether annual testing occurred; (4) the number of contractor systems that service FMC by whether a tested contingency plan exists; and (5) the number of agency-owned and contractor systems that service FMC assessed at e-authentication levels 3 or 4.

Response: Management disagrees with this recommendation and has concluded that receipt of the C&A letter from the contracted agencies is sufficient evidence of monitoring their security control compliance. **Corrective action under this recommendation is considered completed.**

Recommendation 16: Maintain Authority to Operate (ATO) letters, Interconnection Security Agreements (ISA), and Memoranda of Understanding (MOU) between FMC and external service providers.

Response: Evidence satisfying this recommendation was provided at a meeting on October 26, 2010 with the Inspector General, the Chief Information Officer, the Director of the Office of Information Technology, the Information Systems Security Officer, and the contracted auditors. Evidence is again provided in the accompanying CD. **Corrective action under this recommendation is considered completed.**

Finding 8

Recommendation 17: Complete the SERVCON and GSS configuration management documentation to include the sections missing, as identified in the condition section. Additionally, confirm that the SERVCON and future configuration management plans address the following sections, in accordance with NIST SP 800-53 Revision 3: (1) security control, port and firewall settings; (2) allowable and non-allowable services; (3) hardware and software requirements; (4) patches and service packs; and (5) establish system and application baselines and document the deviations from the baselines.

Response: Management is in the process of developing new configuration management framework, which will include the outlined recommendation. Updated information will be provided by the end of the third quarter of FY 2011.

Recommendation 18: Implement the NIST National Checklist Program for FMC servers and utilize a Security Content Automation Protocol (SCAP) scanner to verify NIST baseline security configurations for servers. Additionally, document any deviations from the baseline security configurations along with the reasons.

Response: The FMC will apply the Federal Server Core Configuration security settings to our servers. Any deviations will be documented. Results will be provided by the end of the third quarter of FY 2011.

Anthony Haywood
Chief Information Officer

Attachment (CD)

cc: Managing Director/Audit Follow-up Official
Director, Office of Information Technology