Office of Inspector General

Independent Evaluation Report of FMC's FY 2009 Implementation of FISMA
A10-02

January 2010

FEDERAL MARITIME COMMISSION

FEDERAL MARITIME COMMISSION

Office of Inspector General

Washington, DC 20573-0001

January 28, 2010

Office of Inspector General

Chairman Lidinsky:

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 seventh annual evaluation completed by the OIG in the area of information and computer security.

As you already know, last year the Office of Information Technology (OIT) sought the assistance of an outside 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. However, this year, at the direction of the Chief Information Officer, the agency's contracting officer issued a stop work order after two of four systems were certified and accredited. The CIO concluded that the agency would be better off scrapping the two remaining systems and procuring an "off-the-shelf" system that works better and saves the agency money in the long run.

The OIG did not review that decision as part of this security evaluation. Rather, we focused the evaluation on the two systems that were certified and accredited. As of the date of issuance of our report, the two systems that did not undergo security accreditation are in production.

The OIG contracted with Richard S. Carson and Associates to perform the independent evaluation of the FMC security program. The objectives of the independent evaluation of the FMC information security program were to:

1. Assess compliance with FISMA and related information security policies, procedures, standards and guidelines;
2. Perform an external network scan from an IP address outside FMC to identify vulnerabilities that would permit unauthorized access to agency resources and databases (open ports, missing patches, default or missing passwords, etc.);
3. Review management actions to implement prior-year OIG recommendations; and
4. Evaluate the effectiveness of the work completed by the OIT contractors.

The evaluation found that the FMC has taken concrete steps to protect the agency's systems – most important is the accreditation of its Network and SERVCON applications - and has made progress in mitigating weaknesses which led to the prior year's significant deficiency concerning IT risk and recovery planning. A significant deficiency is a weakness in an agency's overall information systems security program that restricts the capability of the agency to carry out its

mission or compromises the security of its information, information systems, personnel, operations or assets. The firewall is secure; attempts to penetrate firewall defenses by the evaluation team from a remote location were unsuccessful. Moving forward, the CIO appears to have a plan for securing information resources inside the firewall even as the agency updates its IT infrastructure.

On the other hand, the FMC lacks (i) a comprehensive configuration management program and technical privacy controls required by OMB, (ii) an adequate Contingency Planning Program, to include policies, procedures, testing and documentation of testing, and (iii) an official system inventory. Further, the FMC Network Domain Administrator accounts are not monitored.

I am encouraged by progress the agency has made to date and I support the CIO's decision to move forward with a new content management system to replace older applications that were not FISMA compliant. Yet, much still needs to be done to provide basic assurances that information and information systems are secure.

I want to thank OIT managers and staff for their assistance throughout our review. While we did not always agree, I am confident that the CIO understands the extent of the work that lies ahead and has a strategy to address it. I am available to answer any questions you have about the report.

Respectfully submitted,

/Adam R. Trzeciak/
Inspector General

Attachment

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 2009

November 18, 2009

RICHARD S. CARSON & ASSOCIATES, INC.

http://www.carsoninc.com

4720 Montgomery Lane • Suite 800 • Bethesda, MD 20814-3444 • 301.656.4565 • Fax: 301.656.4806

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 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 (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

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

1. Evaluate Information System & 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's (GAO) Federal Information System Controls Audit Manual (FISCAM), National Institute of Standards and Technology (NIST) Information Processing Standards and Special Publications (SP) and OMB guidance. The scope of this task is the FMC Network and SERVCON.
2. Perform Vulnerability Scan: Perform an external network scan from an address outside FMC to identify vulnerabilities associated with hardware and software installed facing the Internet (open ports, missing patches, default or missing passwords, etc.).
3. Evaluate Responses to Prior Recommendations: Review management actions to implement OIG recommendations.
4. Review Progress of Security Program: Perform an independent review of the FMC's progress in implementing an effective information security program as it pertains to the tasks performed by the OIT contractors.

3. SCOPE AND METHODOLOGY

The scope of this independent evaluation of the FMC fiscal year (FY) 2009 information security program included the following:

- Overall Security Program Implementation
- 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 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 (ISSO); 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 the 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-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* July 14, 2007
- 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 2, *Recommended Security Controls for Federal Information Systems*, December 2007
- 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

- *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 June 8, 2009, and September 30, 2009, at the FMC headquarters in Washington, DC.

4. DETAILED FINDINGS AND RECOMMENDATIONS

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

- Creating Certification and Accreditation (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 (with the exception of one FMC employee on maternity leave whose account has been disabled) completed annual computer security awareness training by the end of FY 2009.
- 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 implement a POA&M process.
- Appropriately sanitizing media to prevent disclosure of sensitive information when disposing or recycling media within the agency.

4.1 Agency Implementation of FISMA – FY 2008 Follow-up

During FY 2008 and 2009, 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, used the report results to restructure the agency's information security program and create C&A documentation for two of the FMC's four information systems. FMC's Contracting Officer issued a stop work order after completion of the FMC Network and SERVCON C&A packages because FORM-1 and FMC-18 were "not ready for C&A." According to OIT, the systems were developed prior to the installment of the current OIT management and policies. If C&A activities were conducted on FORM-1 and FMC-18, management would have to absorb an

exorbitant amount of risk; therefore, the CIO decided that the agency would look into other options. The OIG notes that FORM-1 and FMC-18 continue to operate in a production environment without any documented assessment and acceptance of risk to the organization; however, the FMC plans to develop and implement an enterprise content management system that would replace FORM-1 and FMC-18, complete with a C&A package. The FMC has selected a contractor and is expected to complete the task by May 2010, in time for the OIG's FY 2010 FISMA evaluation. Therefore, the focus for the FY 2009 FISMA evaluation is the completed C&A packages for the FMC Network and SERVCON only.

The OIG is required to report on the security posture of the agency as part of its FISMA evaluation. Recognizing that the contractor completed work on two of the four systems at the FMC, the OIG must still opine on the program as it existed during the review period. In our view, the agency has taken important steps by hiring a contractor to complete C&A packages for two of the four systems at the FMC and to provide the template for a fully functional IT security program. Without minimizing the importance of this foundation and acknowledging the effort involved to bring it about, we also note that in FY 2009 many of the elements of a mature, robust and comprehensive security program still did not exist at the FMC. However, we also note that this condition is likely to change in FY 2010 with the implementation of the enterprise content management system and remediation of the findings listed below.

Notification of Finding # 1: Configuration Management Documentation is not adequate

According to NIST, it is important to document proposed or actual changes to information systems and to subsequently determine the impact of those proposed or actual changes on the system's security. Information systems will typically be in a constant state of migration with upgrades to hardware, software, or firmware and possible modifications to the surrounding environment where the system resides. Documenting information system changes and assessing the potential impact those changes may have on the security of the system is an essential aspect of continuous monitoring and maintaining the security accreditation.

NIST SP 800-53, Revision 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 formal documented configuration management policies and procedures that facilitate the implementation of associated configuration management controls.
- Develop, document and maintain a current baseline configuration of the information systems.
- Define, document and approve configuration changes to the system.
- 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.

- The organization shall establish, document and implement 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.
- Identify, document and approve exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements.
- Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

- Configure the information system to provide only essential capabilities and specifically prohibit or restrict the use of organization-defined prohibited or restricted functions, ports, protocols and/or services.

NIST SP 800-70, *Security Configuration Checklists Program for IT Products Guidance for Checklists Users and Developers,* dated May 2006, provides approved security configuration checklists for a variety of operating systems, Web browsers, firewalls, antivirus software and productivity tools.

Our review determined that the FMC has created a Configuration Management Policy, implemented the Federal Desktop Core Configuration (FDCC) and created a "server build checklist;" however, a baseline configuration for the FMC Network and deviations from the baselines are not documented.

Additionally, the SERVCON Technical Architecture document did not address security controls in sufficient detail to meet NIST guidelines. Specifically, more information should be provided on what security baselines should be used, frequency of security baseline updates and steps to ensure security baselines are being followed. The following sections were found to lack sufficient detail:

- Portal requirements table
- Cron and scheduled tasks table
- User roles and groups tables
- Firewall configuration and port allocation table
- Document sign off

During the vulnerability scans performed (as described in Section 4.3 below), two public devices were identified in the FMC.gov public subnet of which the FMC was initially unaware. Upon further investigation, it was noted that the devices were a test machine and router outside the firewall. Nevertheless, the OIG believes that proper documented configuration management and continuous monitoring would have identified the devices.

The FMC hired a contractor during FY 2008 and FY 2009 to create its IT security program; however, the Contracting Officer 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 has not allocated the necessary resources to create a fully functional configuration management program. The effect of not having completed a current and detailed configuration management program is that baseline security settings do not exist for the FMC systems. Additionally, without a baseline and documented deviations, it is difficult to determine whether security settings are in place. This could make the systems vulnerable to hacking, computer viruses and other exploits.

Recommendations

We recommend OIT:

1. Complete the SERVCON configuration management documentation to include missing sections (identified above). Additionally, confirm that the FMC Network and SERVCON 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
    - System and application baselines and documentation of the deviations from the baselines

2. Implement the NIST National Checklist Program and use a Security Content Automation Protocol (SCAP) scanner to document deviations from the checklists.

Notification of Finding # 2: The FMC does not fully comply with Security Requirements of OMB Memorandum M-07-16.

OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, requires agencies to encrypt all data on mobile computers/devices carrying agency data; require two-factor remote access authentication; use a 30-minute inactivity timeout function for remote access; log and verify all computer-readable data extracts from databases holding sensitive information; and require all individuals with authorized access to Personally Identifiable Information (PII) and their supervisors to sign, at least annually, a document clearly describing their responsibilities.

Through observation of configuration settings, interviews and review of documentation, the OIG noted the following weaknesses, which were also identified in the FY 2008 FISMA review:

1. Encryption is not implemented on mobile computers and devices carrying agency data.

    - OIT reported that, "due to the lack of sensitive information on these systems, it is not anticipated that this recommendation will be implemented." However, the OIG found no evidence that compensating controls, the residual risk and management sign-off of acceptance of this weakness, have been documented. Additionally, thumb drives that were distributed to field office representatives are not FIPS 140-2 compliant[1]. Therefore, the prior year recommendation is still open.

2. Network Administrator remote-access connection does not implement a 30-minute inactivity timeout.

    - Concerning follow-up in FY 2009 on this weakness, the agency has stated that "the Network Administrator's remote access connection cannot be set to time out as there is no setting for this function, which was initiated on 12/15/04. Therefore, corrective action under this recommendation is considered complete." Again, the OIG noted that compensating controls, the residual risk and management sign-off of acceptance of this weakness have not been documented; therefore, the recommendation is still open.

The FMC informed the OIG that the conditions exist because the resources were not available to implement new remote access hardware/software at the current time, but plans were made to upgrade the equipment in an upcoming hardware refresh. The OIG noted that FIPS 140-2 compliant thumb drives were purchased in prior years. However, after speaking with FMC's area representatives, it appeared they were not being used. Without implementing the technical security considerations of OMB Memorandum M-07-16, the FMC cannot ensure OMB compliance and privacy data may be at risk for unauthorized exposure.

Recommendations

We recommend OIT:

3. Evaluate FMC mobile needs and implement FIPS 140-2 encryption on mobile computers and portable devices carrying agency data.

4. Configure the Network Administrator remote-access connection to require a 30-minute inactivity timeout. If unable to complete, document the compensating controls, residual risk and management acceptance of risk.

4.2

[1] Federal Information Processing Standards Publication (FIPS) 140-2 defines the security requirements for cryptographic modules, specifically, the levels and types of encryption to be used when processing information on Federal Government information systems.

Agency Implementation of FISMA – FY 2009 Review

OMB Memorandum, M-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, contained slightly modified FISMA reporting guidance for FY 2009. The OIG evaluated the security program based upon these changes and new requirements. As a result of these evaluations and review of the FMC Network and SERVCON C&A packages, additional vulnerabilities were noted.

Notification of Finding # 3: Deficiencies with the FMC Certification and Accreditation (C&A) packages for the FMC Network and SERVCON exist.

Memorandum M-09-29, *Memorandum for Heads of Executive Departments and Agencies*, states that C&A is required for all federal information systems. Section 3544(b)(3) of FISMA discusses "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems" and does not distinguish between major or other applications. Smaller "systems" and "applications" may be included as part of the assessment of a larger system, as allowable in NIST guidance, provided an appropriate risk assessment is completed and security controls are implemented (OMB M-09-29, p. 11).

Memorandum M-04-04, *Memorandum to the Heads of All Departments and Agencies,* states that agencies are required to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. 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 (CSP) on behalf of federal agencies. Memorandum M-04-04 assists agencies in identifying their e-government authentication needs. Agency program officials bear the primary responsibility to identify assurance levels and strategies for providing them. This responsibility extends to electronic authentication systems.

Agencies shall determine assurance levels using the following steps, described in Section 2.3 of M-04-04:

1. Conduct a risk assessment of the e-government system.
2. Map identified risks to the applicable assurance level.
3. Select technology based on e-authentication technical guidance.
4. Validate that the implemented system has achieved the required assurance level.
5. Periodically reassess the system to determine technology refresh requirements.

NIST Special Publication (SP) 800-37, *Recommended Security Controls for Federal Information Systems*, May 2004, states that a C&A package shall contain an approved security plan, a security assessment report (ST&E) and a Plan of Action and Milestones (POA&M) (SP-800-37, p. 21). Additionally, SP 800-37 states that the assessment of risk and the development of system security plans 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 (SP 800-37, p. 4). Documentation should be produced that describes the process employed and the results obtained (SP 800-37, 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 (SP 80-37, pp. 5, 21).

The OMB Guidance M-06-20, *Memorandum for Heads of Executive Departments and Agencies,* states that for all non-national security programs and systems, agencies must follow NIST standards and guidance (OMB, M-06-20, p. 2).

NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, dated 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 is 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 (SP 800-18 Section 3.1.4, pp 24 - 25).

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, dated July 2002, differentiates security testing and evaluation 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 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).

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).

C&A Packages

The evaluation team reviewed packages for the FMC Network and SERVCON to determine if the packages adhere to NIST SP 800-37 guidance. A review of the individual documents of each package was then conducted to evaluate their compliance with other relevant NIST and OMB guidance. The C&A packages contained a privacy impact assessment, security plan, risk assessment and certification and accreditation statements; Plan of Action and Milestones (POA&M), FIPS 199 system categorization, contingency plan and system test and evaluation plan and report; and a configuration management plan (SERVCON only) and self-assessment. Security plans and certification and accreditation forms for these systems were provided separately.

The review team concludes that the FMC Network and SERVCON packages were generally completed using NIST guidance. However we also identified minor instances of noncompliance with NIST that could weaken the overall assurances of what the packages are intended to provide. These deficiencies are detailed in the following sections:

Security Plans

While the FMC Network and SERVCON security plans were generally compliant with NIST SP 800-18 guidance, review of the security plans found that sections of the security plans were either not completed or completed incorrectly. For example:

- 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 indicating 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 the FMC, but there was no clear discussion of the user community.) Presently, this section and related table identify 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.
- 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) are 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.

Risk Assessments

Review of the FMC Network and SERVCON risk assessments found that 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. However, the following weaknesses were identified:

- Accreditation boundaries for the risk assessment, which define the scope of the C&A packages, were not clearly defined.
- System and data owners were not clearly identified.
- Parts of the documents were incomplete. Specifically, the System Management Roles table 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 to keep them appropriately segregated.

E-Authentication Risk Assessments

Systems requiring e-authentication have not been identified, and e-authentication risk assessments have not been conducted on information technology systems. Additionally, due to a lack of documentation, we could not determine whether the agency has validated whether its systems have operationally achieved the required assurance level as defined in NIST Special Publication 800-63**.**

C&A Letters

Review of the C&A memoranda dated June 4, 2009, found that certification and authorization to operate statements for the FMC Network and SERVCON were contained in each document. However, the review found the following weaknesses:

- The CIO is not clearly identified as the Designated Approving Authority.
- The ISSO signed the certification statement as the "Authorizing Official" instead of the "Certifying Agent," which would appear to be a conflict of interest.
- The statement does not mention the contractors who operated as an independent certification agent, under the role of the ISSO, as required by NIST SP 800-53 for "moderate" and "high" categorized systems.

Privacy Impact Assessment (PIA)

Review of the C&A packages provided by the FMC confirmed PIA assessments were completed for the FMC Network and SERVCON. Review of the PIAs found that they described the PIA process, identified who is responsible for completing the PIA and when a PIA is required, and described the Privacy Act requirements. Review of the assessment confirmed that personal identifiers collected by each system were identified and addressed the PIA requirements. On the other hand, we noted that the PIA documents did not contain the following required information:

- System of Records Number (SORN)
- OMB unique system identifier
- System Code

We also noted that the PIAs were not signed, and Section 3 of the PIA, Determination by the FMC Privacy Advocate, is incomplete. There is a section title, but no statement or signature from the FMC Privacy Advocate to indicate whether the system PIAs have been approved.

FIPS 199 Security Categorization

The security categorizations were not consistent across the FMC Network and SERVCON documents. Specifically, the security categorizations for the FMC Network and SERVCON did not match the security categorizations listed in the POA&Ms.

Contingency Plans

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

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

Through inspection of the documentation and interviews with staff, it appears that the contractor completed the C&A documentation to a satisfactory level. However, the documentation does not fully comply with NIST guidance. This outcome is likely the result of inadequate oversight of the contractor's final deliverables. Without developing comprehensive C&A packages for the FMC Network and SERVCON, the FMC is unable to identify all of the security vulnerabilities associated with operating its systems. Additionally, without the appropriate personnel formally accepting the risks of running these systems in the production environment, the FMC data and systems may be vulnerable to potential unknown threats and will not be adequately safeguarded to prevent unauthorized use, disclosure and modification.

Recommendations

We recommend OIT:

5. Conduct security categorizations on the FMC Network and SERVCON in accordance with FIPS 199 and NIST SP 800-60.
6. Clearly identify the Certifying Agency, Designated Approving Authority and system owner in the FMC Network and SERVCON security plans and C&A documentation in accordance with NIST SP 800-37.
7. Conduct complete risk assessments on the FMC Network and SERVCON. Define accreditation boundaries. Ensure that risk assessments are complete in accordance with NIST SP 800-30.
8. Complete security plans for the FMC Network and SERVCON in accordance with NIST SP 800-18.
9. Standardize security categorizations across the FMC and SERVCON C&A documents.
10. Develop contingency plans for the FMC Network and SERVCON in accordance with NIST SP 800-34 and NIST SP 800-53.
11. Complete the FMC Network and SERVCON Authorization to Operate letters with the correct information and titles.

Notification of Finding # 4: The 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 Analysis. 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 (SLAs) with the equipment vendors. In addition, technologies such as Redundant Arrays of Independent Disks (RAID), automatic fail-over, uninterruptible power supply (UPS) 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 provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise or failure (SP 800-53, CP-10).

The FMC took part in the Federal Emergency Management Agency's (FEMA) Eagle Horizon 2009 continuity mandatory exercise for all federal executive branch departments and agencies. This test evaluated the accessibility and functionality of the FMC-18, e-mail, Registered Person Index (RPI), CADRS' database, MSWord and Adobe in the event of a disruption. However, based upon review of the contingency plans and documentation provided, the following weaknesses were noted:

- The FMC does not have documented contingency planning policies and procedures for identifying the frequency and types of tests and preparing and updating of contingency documentation.

- The SERVCON contingency plan was not tested.

- The FMC Network contingency plan test (Eagle Horizon 2009) and results documentation does not adequately test or document the FMC Network and SERVCON contingency plans. This test focused on the FMC's e-mail, Adobe, Internet access, FMC-18, Content Management System (CMS), RPI and CADRS' database. No information was available to describe the scenario that was being tested. Testing appeared to concentrate on determining if the applications were working and if e-mail could be sent

or the Internet could be accessed. Some test results were inconclusive (e-mail was sent out requesting replies from the recipient, but no responses were received); however, no recommendations or lessons learned were identified.

The 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 recommend OIT:

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

Notification of Finding # 5: The FMC does not have an official system inventory.

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

- 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.
- Is available for review and audit by designated organizational officials.

During FY 2009, OIT hired contractors to create a security program and to certify and accredit the FMC's systems. The contractors distributed inventory forms to all the FMC departments to identify the systems in operation. The returned forms became the "FMC inventory." In addition to the FMC Network and SERVCON systems for which the contractor created C&A packages, the forms were returned from each of the FMC departments 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 the following:

- IT System ID
- IT System interfaces
- IT System boundary
- IT System Operability and Agreements
- IT System and Data Sensitivity
- Overall IT System Sensitivity Rating
- IT System Sensitivity Rating
- Any indication as to whether the system is a GSS, major application or minor application

The OIG notes that other federal agencies annually query their business units on the IT systems they are using or plan to use in the future, as well as identify IT systems that are used outside of the agency. This information is then compiled by the IT department into an official documented inventory.

Through inspection of the documentation and interviews with OIT staff, it was determined that an inventory process had not been implemented at the FMC and that OIT staff was relying on documentation produced and distributed by the contractor. Further, this "inventory" was not vetted for accuracy and completeness by OIT or its contractor. Without documenting and implementing an effective inventory process, the FMC management may not be aware of all the FMC systems in operation and, therefore, cannot fully realize the risk in the IT environment.

Recommendation

We recommend OIT:

14. Complete and maintain an official, documented system inventory of all the FMC systems and interfaces.

Notification of Finding # 6: The FMC Plan of Action & Milestones process needs improvement.

In Memorandum M-04-25, *Memorandum for Heads of Executive Departments and Agencies*, OMB 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 shall 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. M-04-25 also provides instructions on how POA&Ms should be structured and maintained (M-04-25, pp. 14-15).

Based on the documents reviewed, the FMC developed POA&Ms for the FMC Network and SERVCON. The POA&M documents contain the required elements as identified in OMB guidance. However, review of the POA&Ms noted the following weaknesses:

- The POA&M process may not be implemented agency-wide.
- The POA&M process may not be fully utilized.

Review of the FMC Network and SERVCON POA&Ms found that POA&M action items originated from various sources, such as system security plan findings, the Office of Equal Employment Opportunity, OIG, Office of Operations, Office of Administration and the Office of Financial Management. However, POA&Ms were not provided for all of the FMC applications. The POA&M process has not been implemented agency-wide and may not incorporate all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.

The OIG found that the POA&Ms for the FMC Network and SERVCON were not completed properly and, therefore, the process may not be fully utilized. Review of the POA&Ms noted the following weaknesses:

- Sensitivity/criticality levels for the FMC Network and SERVCON systems did not match sensitivity/criticality levels reported in FIPS 199 for the FMC Network and SERVCON. The FIPS 199 security categorization for the FMC Network was reported as High/High/High (corresponding to levels for confidentiality, integrity and availability categories for each IT system, respectively); while, the POA&M identified it as High/Moderate/High. The FIPS 199 security categorization for SERVCON was identified as High/Moderate/High; while, the security categorization listed in the POA&M was marked as Moderate/Moderate/Moderate in the SERVCON POA&M. Based on these categorizations, the agency sets it controls and security of the information. Controls for moderate systems are not as stringent as those for high risk systems.
- ID numbers were not assigned to POA&M items for the FMC Network and SERVCON.
- The sensitivity of the POA&M document was not printed on the document.

- Resources required to complete the task were not identified.
- Milestones with completion dates were not identified.

Through inspection of the documentation and interviews with OIT staff, the OIG determined that OIT staff have utilized the FMC Network and SERVCON POA&Ms, but have not allocated sufficient resources to create an agency-wide POA&M process (i.e., a process that tracks vulnerabilities from various sources within the agency). Without an effective POA&M process, the agency may not be able to easily identify and prioritize weaknesses or track the status of the corrective actions being taken to resolve deficiencies identified. This could lead to vulnerabilities not being corrected and the continued exposure of the FMC systems to higher levels of risk.

Recommendations

We recommend OIT –

15. Develop an agency-wide POA&M process to include all systems that meet OMB requirements.
16. Complete the POA&M spreadsheets in accordance with current OMB and NIST guidance and maintain evidence of the closure of each item.

Notification of Finding # 7: The FMC Network Domain Administrator accounts are not appropriately segregated and monitored.

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: (a) organizes information system and network privileges into roles; and (b) 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.

Six members of the OIT staff, including one contractor and the ISSO, have the FMC Network Domain Administrator permissions on their user accounts. Additionally, a formal process for monitoring user and privileged accounts, including the Domain Administrator account, is not implemented.

The FMC informed the OIG that the conditions exist because the size of the OIT requires multiple individuals to make changes to the FMC Network on a daily basis. The FMC also

informed the OIG that informal monitoring by the OIT Director is performed and, therefore, a formal monitoring process is not necessary. The OIG is not convinced that monitoring is not needed based on OIT's rationale. Without appropriately limiting the access rights and monitoring usage of the 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:

17. Change the password of the FMC Network Domain Administrator account and physically secure the password so that it is only available for authorized and documented network changes and/or emergencies.
18. Restrict the FMC Network Domain Administrator privileges to OIT staff whose job functions require the access privileges; remove access for the ISSO to maintain segregation of duties.
19. Document and implement policies and procedures (and if determined necessary hardware and/or software) for the ISSO to monitor the actions of all the FMC Network users, privileged users (super users) and domain administrator accounts.

4.3 Vulnerability Scan

The OIG performed a vulnerability assessment on the FMC Network from external sources on October 6, 2009. The review was conducted using NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment,* September 2008, as methodology. It was noted that no high-risk vulnerabilities were discovered. Completed scan results were provided to OIT management immediately after our tests were concluded.

UNITED STATES GOVERNMENT FEDERAL MARITIME COMMISSION

Memorandum

TO : Inspector General **DATE:** January 26, 2010

THROUGH : **/**Director, Office of Administration/

FROM : CIO

SUBJECT : FISMA Audit 2009

This is in response to your recently provided FISMA audit report.

Notification of Finding # 1: Configuration Management Documentation is not adequate

Recommendation(s)

We recommend OIT:

1. Complete the SERVCON configuration management documentation to include missing sections (identified above). Additionally, confirm that the FMC Network and SERVCON 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
   - System and application baseline and documentation of the deviation from the baselines

Management's Response

FMC acknowledges finding # 1 recommendation 1; the SERVCON Technical Architecture document did not address security controls in sufficient detail. Specifically, more information should be provided regarding security control, port and firewall settings, allowable and non-allowable services, hardware and software requirements, patches and service packs, on what security baselines should be used, frequency of security baseline updates, and steps to ensure security baselines are being followed.

FMC will follow the recommendation of the Office of the Inspector General by ensuring that configuration management plans address the above referenced sections in accordance with NIST SP 800-53, Revision 3.

2. Implement the NIST National Checklist Program and use a Security Content Automation Protocol (SCAP) scanner to document deviations from the checklists.

Management's Response

FMC will follow the recommendation of the Office of the Inspector General in regards to the implementation of the NIST National Checklist Program and the utilization of a Security Content Automation Protocol (SCAP) scanner to document deviations from the checklists.

Notification of Finding # 2: The FMC does not fully comply with Security Requirements of OMB Memorandum M-07-16

Recommendation(s)

We recommend OIT:

3. Evaluate FMC mobile needs and implement FIPS 140-2 encryption on mobile computers and portable devices carrying agency data.

Management's Response

FMC acknowledges finding # 2 recommendation 3. FMC is in the process of identifying a FIPS 140-2 compliant encryption solution to implement on mobile computers and portable devices carrying agency data.

4. Configure the Network Administrator remote-access connection to require a 30-minute inactivity timeout. If unable to complete, document the compensating controls, residual risk and management acceptance of risk.

Management's Response

FMC acknowledges finding # 2 recommendation 4. The FMC has stated that the Network Administrator's remote access connection cannot be set to time out, as there is no setting for this function. FMC will document the compensating controls, residual risk, and provide management sign off of acceptance of this risk until corrected.

Notification of Finding # 3: Deficiencies with FMC Certification and Accreditation (C&A) packages for FMC Network and SERVCON exist

Recommendation(s)

We recommend OIT:

5. Conduct security categorizations on the FMC Network and SERVCON in accordance with FIPS 199 and NIST SP 800-60.

Management's Response

Security categorizations have been conducted on the FMC GSS and SERVCON systems in accordance with FIPS 199 and NIST SP 800-60.

6. Clearly identify the Certifying Agency, Designated Approving Authority, and system owner in the FMC Network and SERVCON security plans and C&A documentation in accordance with NIST SP 800-37.

Management's Response

The C&A letters have been corrected to clearly identify the Certifying Agent, Designated Approving Authority, and System Owner in the security plans and C&A documentation in accordance with NIST SP 800-37.

7. Conduct complete risk assessments on the FMC Network and SERVCON. Define accreditation boundaries. Ensure that risk assessments are complete in accordance with NIST SP 800-30.

Management's Response

Risk Assessments that define the accreditation boundaries have been completed for the FMC GSS and SERVCON systems in accordance with NIST SP 800-30.

8. Complete security plans for the FMC Network and SERVCON in accordance with NIST SP 800-18.

Management 's Response

Security plans have been completed for the FMC GSS and SERVCON systems in accordance with NIST SP 800-18.

9. Standardize security categorizations across the FMC and SERVCON C&A documents.

Management's Response

Security categorizations have been standardized across all FMC GSS and SERVCON C&A document.

10. Develop contingency plans for the FMC Network and SERVCON in accordance with NIST SP 800-34 and NIST SP 800-53.

Management's Response

As part of the certification and accreditation process performed by IES, a contingency plan was developed for both the GSS and SERVCON systems that identify testing procedures, frequency of testing, and the types of test to be performed. FMC will conduct a contingency plan test in the second quarter of FY 2010 using the contingency plan test process developed by IES for the FMC GSS and SERVCON systems and document the results in accordance with NIST SP 800-34 and NIST SP 800-53.

11. Complete the FMC Network and SERVCON Authorization to Operate letters with the correct information and titles.

Management's Response

Completed 10/16/09

Notification of Finding # 4: FMC lacks an adequate Contingency Planning Program, to include policies, procedures, testing, and documentation of testing.

Recommendation(s)

We recommend OIT –

12. Develop a contingency plan policy and procedures that address the creation, review, testing, and maintenance of contingency plans.

Management's Response

FMC does not have documented contingency planning policies and procedures for identifying the frequency of testing, types of testing, preparing and updating of contingency documentation. The FMC has recently completed migrating from its previous COOP site (Rack Space) to its new COOP site (Recovery Point) from which FMC participated in the Eagle Horizon contingency plan test. As part of the certification and accreditation process performed by IES, a contingency plan was developed for both

the GSS and SERVCON systems that identify testing procedures, frequency of testing, and the types of test to be performed.

13. Test contingency plans and document results in accordance with NIST SP 800-34 and NIST SP 800-53.

Management's Response

The FMC Network contingency plan test (Eagle Horizon 2009) and results documentation does not adequately test or document the FMC Network and SERVCON contingency plans. FMC will conduct a contingency plan test in the second quarter of FY 2010 using the contingency plan test process developed by IES for the FMC GSS and SERVCON systems and document the results in accordance with NIST SP 800-34 and NIST SP 800-53.

Notification of Finding # 5: FMC does not have an official system inventory.

Recommendation(s)

We recommend OIT –

14. Complete and maintain an official system inventory of all FMC systems and interfaces.

Management's Response

The FMC has inventoried the GSS and SERVCON systems using a process that conforms to NIST SP 800-53 rev 3, recommended Security Controls for Federal Information Systems and Organizations control CM-8 as required during its recertification of SERVCON in FY 2009.

Notification of Finding # 6: The FMC Plan of Action & Milestones process needs improvement.

Recommendation(s)

We recommend OIT –

15. Develop an agency-wide POA&M process to include all systems, that meet OMB requirements.

Management's Response

An agency wide POA&M process that meets OMB requirements has been implemented in regards to FMC's GSS and SERVCON systems.

16. Complete the POA&M spreadsheets in accordance with current OMB and NIST guidance and maintain evidence of the closure of each item.

Management's Response

The FMC acknowledges finding # 6 recommendation 16. The POA&M spreadsheets have been completed in accordance with current OMB and NIST guidance. The sensitivity/criticality levels for the systems were corrected to correspond with the sensitivity/criticality levels reported in the Federal Information Processing Standards (FIPS) 199 for FMC Network and SERVCON. The FIPS 199 security categorization for the FMC Network was reported as Confidentiality-High/ Availability-High/ Integrity-High. The FIPS 199 security categorization for SERVCON was identified as Confidentiality-High/ Availability-Moderate/ Integrity-High during its recertification of SERVCON in FY 2009.

Notification of Finding # 7: The FMC Network Domain Administrator accounts are not appropriately segregated and monitored.

Recommendation(s)

We recommend OIT –

17. Change the password of the FMC Network Domain Administrator account and physically secure the password so that it is only available for authorized and documented network changes and/or emergencies.

Management's Response

The Office of Information and Technology, in conjunction with the CIO is in the process of developing a process by which every ninety days the Domain Administrator account password is manually changed and physically secured in a designated location so it is only available in authorized and documented network changes and/or emergencies in accordance with finding #7, recommendation 17. This process will be in place by the end of the first quarter of fiscal year 2010.

18. Restrict the FMC Network Domain Administrator privileges to OIT staff whose job functions require the access privileges; remove access for the ISSO to maintain segregation of duties.

Management's Response

All Office of Information and Technology staff members that require elevated access privileges have in addition to their regular user account, an account that is a member of the Domain Admin group through which additional access rights are provided. These accounts were created to provide Office of Information and Technology staff the ability to perform their necessary job functions while providing accountability in regards to

network access and configuration changes. The ISSO has additional duties within the Office of Information and Technology which requires additional access privileges.

19. Document and implement policies and procedures (and if determined necessary hardware and/or software) for the ISSO to monitor the actions of all the FMC Network users, privileged users (super users) and domain administrator accounts.

Management's Response

FMC Office of Information and Technology currently employs a process that captures the server logs and moves them to a designated network location. The server/ Network logs consist of application, security, and system logs and are kept for three years. The FMC based on recommendation finding # 7, recommendation 19 realize 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.