Review of FMC Implementation of FISMA for Fiscal Year 2007

A08-01

FEDERAL MARITIME COMMISSION

1961

November 2007

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

November 16, 2007

Office of Inspector General

Commissioners;

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

This year's review objectives were to assess compliance with FISMA and related information security policies, procedures, standards and guidelines, and to test their effectiveness on a representative subset of the agency's information systems. Specifically, this review (i) evaluated the implementation of the Federal Maritime Commission's (FMC) information security program; (ii) assessed agency progress towards correcting weaknesses addressed in the FY 2007 Plan of Actions & Milestones (POA&M); and (iii) verified and tested information security for the FMC network and wireless tools.

The FMC continues to make some progress in developing its information security program and has addressed or begun to address past security vulnerabilities identified by the OIG. Perhaps most noteworthy is the progress the agency has made in documenting policies and procedures covering many IT security issues. Also noteworthy is the new computer security on-line training program introduced this year. It is more comprehensive than the prior year training program and requires staff to pass an information security quiz at completion to ensure that security concepts and procedures were understood. The agency acquired and installed scan software, enabling the Office of Information Technology (OIT) to scan the FMC network for harmful activities and vulnerabilities and initiated planning for security control implementation at the continuity of operations (COOP) site, *Rackspace,* in suburban Maryland.

Although progress has been made, the OIG identified areas where improvements are still needed. Successful FISMA implementation requires that Federal agencies adopt an enterprise-wide security strategy. It requires a fundamental shift from policy-based compliance (with its minimal tolerance for flexibility in implementation) to a risk-based paradigm where agency missions and business functions drive security requirements and associated safeguards. Because risks differ depending on agency mission and objectives, there is no "one size fits all" security program. It is my opinion, based on the current and prior-year FISMA reviews, the agency has not yet made the shift to a risk-based approach. Nor has it fully integrated information security responsibilities beyond OIT. At the FMC, FISMA implementation is primarily an OIT function.

It is easy to look at the totality of the requirements and guidelines issued by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology

(NIST) and conclude that an agency the size of the FMC, with its limited staff and financial resources, cannot meet these standards. On the other hand, we note that OMB assesses agencies based on the progress they make toward enhancing their respective programs. The FMC should approach a NIST-compliant, risk-based security program one step at a time. This approach will comply with OMB requirements while strengthening our security posture from the start, even if total compliance requires several years to accomplish. We need to take the first step. The attached report provides a framework on how to begin.

It is important to remember that all federal agencies have some risks and vulnerabilities. OMB recognizes this and asks agencies to implement a security program that identifies them and lays out a plan to address (reduce, eliminate or accept) them based on what the agency considers to be acceptable levels of risk. It does not expect a clean slate when it comes to information security (i.e., no risks or vulnerabilities). This would be unachievable for any-size agency. On the other hand, mitigating known risks to an acceptable level is a goal achievable for all, including the FMC.

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

The OIG performed this evaluation from June 4, 2007 through August 17, 2007, and followed National Institute of Standards and Technology guidance for information systems, OMB Memorandum M-07-19, *Reporting Instructions for the Federal Information Security Management Act* (July 25, 2007) and best practices used in the industry. The OIG thanks OIT management and staff for its help and cooperation during our review.

Respectfully submitted,

Adam R. Trzeciak
Inspector General

Carson

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 2007

November, 2007

EVALUATION SUMMARY

Introduction

On December 17, 2002, the President signed into law the E-Government Act of 2002 (Public Law 107-347), which includes Title III, the Federal Information Security Management Act (FISMA) of 2002. FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act (GISRA) of 2000, which expired in November 2002. FISMA outlines the information security management requirements for agencies, including the requirement for annual review and independent assessment by agency inspectors general (IG). 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 overall effectiveness of security programs and to develop strategies and best practices for improving information security.

The Federal Maritime Commission's (FMC) Office of Inspector General (OIG), with technical assistance from IT security evaluators from Richard S. Carson, Inc., completed this Independent Evaluation Report along with the IG's portion of the Office of Management and Budget (OMB) Reporting Template for IGs for FY 2007. This OIG Independent Evaluation Report, unlike the Reporting Template for IGs, focuses on performance measures, provides specific findings and, when applicable, recommendations for resolution.

Objectives

The objectives of the independent evaluation of the FMC information security program were to:

1. Assess compliance with FISMA and related information security standards and guidelines as presented by National Institute for Standards and Technology (NIST) and the Office of Management and Budget (OMB);
2. Review FMC's certification and accreditation (C&A) program;
3. Assess the security controls protecting the FMC's network, Service Contracts Internet Based Filing System (SERVCON) and Form-1;
4. Review FMC's Plan of Action and Milestones (POA&M) process;
5. Evaluate FMC's security training program;
6. Evaluate due diligence activities over FMC's contractor systems, specifically the U.S. Department of Agriculture (USDA) National Finance Center (NFC);
7. Assess agency-wide activities toward a fully integrated information security program;
8. Scan the FMC's wireless network for vulnerabilities; and
9. Assess the effectiveness of the FMC's continuity of operations and disaster recovery plans.

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

GENERAL OVERVIEW

FISMA section 3542(b)(1)(A),(B),(C) 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."

It is critical that agencies establish a firm foundation for a mature information security program. Without a firm foundation, there is no guarantee that security enhancements added after systems are in production will provide the intended results. It's akin to building a home on a poorly constructed foundation. No modifications subsequently added to the living areas will substantially increase the stability of that house.

The National Institute of Standards and Technology (NIST) was tasked by the OMB to establish guidance to assist agencies to implement a comprehensive, risked-based security program – beginning with the foundation. NIST guidance is contained in Federal Information Processing Standards (FIPS) publications and Special Publications (SP) "800 series" reports.

A risk-based approach begins with agencies defining the sensitivity of their information systems according to the potential impact of loss. In other words, what would the impact be on the agency and its stakeholders if a system or systems went down or if data were lost or stolen? FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* (February, 2004), assists agencies to categorize their systems in terms of low, medium or high impact. The second step is to select baseline security controls to protect those information systems. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* (March, 2006) provides guidance on selecting a minimum set of controls needed to protect low, medium or high impact data. The third step requires agencies to comprehensively identify risks to the information systems as part of a risk assessment process, using NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* (February, 2005). Depending on the information impact level assigned and the agency-specific risks to the system(s), the baseline controls identified should be supplemented with tailored security controls as needed to ensure adequate security and due diligence.

The security requirements for each system and the security controls planned or in place should be documented in the security plan. Once the controls commensurate with the risks are identified, the controls are then implemented on the systems and periodically tested to ensure that they are implemented correctly, operating as intended and producing the desired outcomes.

It is essential that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems. The steps identified above should occur before systems are placed into production. Decisions to place systems into production rely on the next series of steps collectively referred to as system certification and accreditation, or "C&As."

A *security certification* is a comprehensive assessment 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. The results of a security certification are used to reassess the risks and update the system security plan, thus providing the factual basis for an authorizing official to render a security accreditation decision.

Security accreditation is the official management decision made by a senior agency official to authorize operation of an information system and explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. By accrediting an information system, an agency official accepts *responsibility* for the security of the system and is fully *accountable* for any adverse impacts to the agency if a security breach occurs. Thus, responsibility and accountability are core principles that characterize security accreditation.

The OIG believes that the FMC has not provided the necessary assurances that it knows the risks to its information and has either taken appropriate steps to mitigate the risks or has made informed decisions to accept the risks to its systems before placing them into production. Further, FMC has placed a new system into production, *Form FMC-18*, before it met security requirements on three legacy systems, contrary to OMB Memorandum M-07-19, FISMA Reporting Instructions.[1]

The agency has not fully integrated its information security program throughout the agency. Rather, information security is viewed as an IT responsibility. Yet, OIT lacks the resources to fully enforce security policy and implement an OMB-required security program that follows NIST guidelines. In meetings with agency staff, the OIG was told that the agency struggles to address all of the information security requirements given its current resource constraints.

To addresses the weaknesses identified above, the agency would need to fundamentally change its approach to FISMA in the following two ways:

1. Focus on FISMA as an agency-wide strategic planning element and not as an information technology operations exercise; and
2. Complete C&A documentation using NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* (May, 2004).

The OIG believes that the agency needs to identify progress towards these overarching goals. In the attached report, we recommend changes that will set the agency on the right course. However, we recognize that the agency is not in a position financially or structurally to change overnight. Rather it will take time <u>and</u> the commitment of managers at the highest levels of the organization.

Details on these and other related findings are presented in the attached report.

[1] "Operations of legacy (steady-state) systems must meet security requirements before funds are spent on new systems (development, modernization or enhancement). *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (July 25, 2007),* p.7

TABLE OF CONTENTS

1. Background

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

2. Objectives

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

1. Assess compliance with FISMA and related information security standards and guidelines as presented by National Institute for Standards and Technology (NIST) and OMB;
2. Review FMC's certification and accreditation (C&A) program;
3. Assess the security controls protecting the FMC's network, Service Contracts Internet Based Filing System (SERVCON) and Form-1;
4. Review FMC's Plan of Action and Milestones (POA&M) process;
5. Evaluate FMC's security training program;
6. Evaluate due diligence activities over FMC's contractor systems, specifically the U.S. Department of Agriculture (USDA) National Finance Center (NFC);
7. Assess agency-wide activities toward a fully integrated security program;
8. Scan the FMC's wireless network for vulnerabilities; and
9. Determine the effectiveness of the FMC's continuity of operations and disaster recovery plans.

3. Scope and Methodology

The scope of this independent evaluation of the FMC fiscal year (FY) 2007 information security program included:

- Review of the FMC general support system, SERVCON and Form-1
- POA&M review for completeness and accuracy
- Security Assessment review
- C&A process review
- Security Awareness Training implementation review
- Status on safeguarding personally identifiable information (PII)
- Contingency planning and disaster recovery

To accomplish the review objectives, the Office of Inspector General (OIG) conducted interviews with the FMC Office of Information Technology (OIT) staff including the Acting Chief Information Officer (CIO)/ Director of Information Technology, the Senior Information System Security Officer, the Senior Agency Official for Privacy as well as other FMC personnel. The team reviewed documentation provided by FMC including C&A documentation, privacy impact assessments, and information security related policies. In addition, the OIG performed a wireless network vulnerability scan of the FMC's wireless network and access points.

All analyses were performed in accordance with the following instructions / guidance:

- Office of Management and Budget (OMB) Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* July 25, 2007
- 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
- President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE) FISMA Framework, September 2006
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*, December 2006
- Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004
- NIST SP 800-30, *Risk Management Guide for Information Technology Systems,* July 2004
- NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems,* June 2002
- Federal Information Security Management Act of 2002 (Public Law 107-347), December 2002
- *Quality Standards for Inspection* issued by the President's Council on Integrity and Efficiency
- FMC/OIG evaluation guidance
- FMC policies and procedures

Fieldwork was conducted between June 4 and August 17, 2007.

4. Results in Brief

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

- Developing and approving several key security-related policies, to include:
    - Computer Administrative Policy, OIT- P14
    - Configuration Management Policy, OIT-P13
    - Electronic Mail Policy, OIT-P06
    - Enterprise Encryption Policy, OIT-P16
    - File Server Storage Policy, OIT-P05
    - Firewall Policy, OIT-P09
    - Inactive Accounts Policy, OIT-P04
    - Incident Response Policy, OIT-P03
    - IT Security for Personnel, OIT-P11
    - Password Policy, OIT-P01
    - Patch Management Policy, OIT-P12
    - PDA Policy, OIT-P02
    - Peer-to-Peer Policy, OIT-P07

  - Remote Access Policy, OIT-P10
  - Server Security Policy, OIT-P15
  - Wireless Communications Policy, OIT-P08

- Introducing a more in-depth annual computer security awareness program, including providing an interactive online course with a required assessment for all employees at completion;
- Documenting system security plans for the representative subset[2] of systems evaluated;
- Acquiring and implementing patch management software;
- Initiating planning efforts for security control implementation at the Continuity of Operations Plan (COOP) site, *Rackspace;*
- Documenting a service level agreement (SLA) between *Rackspace* and FMC; and
- Acquiring and deploying QualysGuard scan software which allows OIT to periodically scan the FMC network for harmful activity and vulnerabilities.

While we are encouraged by these signs of progress, we are also concerned that fundamental changes need to be made in how the agency approaches information security. Specifically, the FMC has to commit to a risk-based information security program, following the guidelines set forth by NIST. The agency must also make information security the responsibility of senior managers outside of OIT.

The OIG evaluation identified the following specific inadequacies in the FMC security program:

- FMC has not followed the prescribed method for classifying information and information system security categorizations in accordance with FIPS 199.
- FMC has not assessed its systems using NIST Special Publication (SP) 800-53, Revision 1, to validate the effectiveness of implemented controls.
- FMC has not produced contingency plans for agency systems.
- FMC has not produced C&A packages that can provide management with detailed information to make creditable risk-based decisions.
- FMC does not follow its own policies for those that did not complete the security awareness training by the training deadline.
- FMC has not demonstrated the active participation of the following positions as required by NIST SP 800-37: Chief Information Officer, Senior Agency Information Officer, Information System Owner, Information Owner and Information System Security Officer.
- FMC's management does not perform sufficient follow up activities over its contractor systems, specifically the U.S. Department of Agriculture (USDA) National Finance Center (NFC).
- FMC does not document all weaknesses in its POA&M and has not structured its POA&M into program-level and system-level deficiencies.
- FMC does not demonstrate adherence to documented agency policy, specifically –
  - Wireless Communications Policy, OIT-P08, and
  - IT Security for Personnel, OIT-P11.

[2] The subset of systems chosen for FY 2007 FISMA evaluation is FMC Network, SERVCON, and Form-1.

5. CERTIFICATION AND ACCREDITATION

The certification and accreditation (C&A) process, when applied to agency information systems, provides a systematic approach for assessing security controls to determine their overall effectiveness; that is, the extent to which operational, technical and managerial security controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system. Understanding the overall effectiveness of the security controls implemented in the information system is essential in determining the risk to the organization's operations and assets, to individuals and to other organizations resulting from the use of the system.

Notification of Finding # 1: Certification and Accreditation

Condition

FMC C&A documentation does not comply with revised NIST and OMB guidance for the three systems we reviewed. C&A documentation for the FMC Network, SERVCON, and FORM-1 lacks sufficient information that would provide management with the assurance required to effectively demonstrate sound information security decisions based on risk. The OIG believes that this is a significant deficiency in the agency's security posture.[3]

Criteria

OMB Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, requires that agencies "follow NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (May, 2004) for certification and accreditation work initiated after May, 2004. This includes use of the FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, to determine the information system category according to the potential impact of its loss. Further certification and accreditation requires documentation of security planning, including: risk assessments, contingency plans, 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.

NIST Special Publication (SP) 800-37 identifies the key participants involved in an agency's security certification and accreditation process: Chief Information Officer, Senior Agency Information Security Officer, Information System Owner, Information Owner, and Information System Security Officer.

[3] The Office of Management and Budget (OMB) defines a significant deficiency in Memorandum 07-19 as "a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken" (Page 23).

Security Categorization

The security categorization is the foundation from which the information system's security control baseline is selected from NIST SP 800-53, Revision 1. The efforts performed during the C&A process are only as reasonable and creditable as the security categorization determined. Without accurately documenting the identification of information types (i.e., a specific category of information such as privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization (or in some instances by a specific law, Executive Order, directive, policy, or regulation) selected from NIST SP 800-60, FMC has not demonstrated how a managerial determination was made to choose the appropriate security control baseline for protecting the information within each system. The type of information FMC stores or processes directly determines the level of security needed for the system.

System Inventory

FISMA Section 305(c)(2) states that an agency's system inventory shall identify the interfaces among all systems attached to the network. It is also crucial to be able to document all agency and contractor systems. FMC has not produced a documented, management-approved process for determining agency systems or a process to annually review the system inventory. Because the OIG received no system inventory, we have no accurate account of the FMC's information system inventory.

Security Assessments (formerly Self-Assessments)

FISMA requires the management, operational, and technical controls in each information system contained in the inventory of major information systems to be assessed with a frequency depending on risk, but no less than annually (Section 3544[b][5]). FMC performed system security control testing under the outdated NIST SP 800-26 methodology that was rescinded with the finalization of NIST SP 800-53A. OMB Memoranda 06-20, dated July 17, 2006, identifies the change in security control assessment guidance.

SP 800-26 and SP 800-53, Revision 1, differ in the approach and level of effort needed to evaluate security controls. SP 800-26 did not provide the scope and breadth of coverage for security controls that are provided by SP 800-53. SP 800-53A provides a detailed, consistent approach to testing security controls, where the evaluator must examine, interview, observe, and test to validate security control effectiveness.

Accrediting officials made decisions on the FMC Network, SERVCON, and Form-1 systems based on applying security controls in the rescinded NIST SP 800-26, instead of the required (and far more comprehensive) NIST SP 800-53 security controls and NIST 800-53(a) testing methodology. As a result, the OIG believes that accrediting officials made decisions on these systems based on incomplete information regarding vulnerabilities to the systems and the effectiveness of controls in place to manage the risks to the information housed on these systems.

Security Plans

The OIG received the latest versions of the system security plans for the FMC network dated May 2007, SERVCON dated March 2007, and Form-1 dated January 2007. In accordance with NIST guidance the security plans include system identification, operational status, general purpose/description, and system interconnection/information sharing sections. The plans additionally include "redundancy plan" sections that discuss system back-ups.

System security plans (SSPs) do not comply with NIST guidance, specifically, the provisions of SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems* (February 2006). For example, system security plans do not detail security controls as required by NIST SP 800-18, Revision 1. NIST guidance requires each control to be fully described in the system security plan and include 1) the security control title; 2) how the security control is being implemented or planned to be implemented; 3) any scoping guidance that has been applied and what type of consideration; and 4) whether the security control is a common control and the person responsible for its implementation.

Risk Assessments

Risk assessments do not comply with NIST SP 800-30, *Risk Management Guide for Information Technology Systems* (July 2002). Vulnerabilities identified in C&A's security control assessments must be assessed according to risk to the system and FMC operating environment. There is no evidence OIT conducted an assessment of security controls or an identification of potential threats based on the documentation submitted for our evaluation.

Risk assessments should be conducted and updated at least annually or whenever the system undergoes a significant change. At the completion of the risk assessment activities, areas noted where corrective actions are needed should be added to the system's POA&M.

Effect

When performed properly, the C&A process provides a systematic approach for determining whether appropriate security controls are in place, functioning properly, and producing the desired outcome. In short, systems containing FMC data and information are placed into production lacking assurances that their systems are secure. Without the discipline and documentation of the C&A process, accrediting officials do not have reasonable assurance that controls are implemented correctly, operating as intended, or producing the desired outcome with respect to meeting the security requirements of FMC. In addition, FMC management is not fully aware of the security control weaknesses in their systems, thereby leaving their information and systems vulnerable to attack or compromise. C&A documentation prepared using NIST SP 800-37 provides authorizing officials with the information they need to make informed decisions based on familiarity with the remaining risks.

Cause

FMC officials explained to the OIG that agency size (approx. 125 staff) coupled with limited resources (OIT consists of five full time staff) limits its ability to address all of the requirements in NIST SP 800-37. To undertake the detailed and comprehensive requirements put forth by NIST would require either reassigning the ISSO to work full time on testing and documenting the agency's security program or hiring of additional staff. In essence, the agency has looked at all requirements and decided that it would do its best with the resources that it has.

Recommendation(s)

Notwithstanding the agency's approach to implementing controls over information, the OIG believes that the task is overwhelming when viewed as an all or nothing proposition. It is especially difficult to justify given the absence of credible threats to FMC and the competing needs for resources. We believe that the agency should set modest, achievable goals for itself, beginning with establishing a solid foundation for its information security program.

1. For the three systems identified in its inventory, OIT should lay a firm foundation for a mature and integrated IT security program by using FIPS 199 to identify impact levels of the three systems in its inventory, identifying minimum security requirements for these levels based on FIPS 200, and implement required security controls using NIST SP 800-53, Revision 1.
2. Once the FMC has established minimum required controls, FMC should test these controls to ensure that they are fully implemented, working as intended and producing the desired results. OIT should consider contracting this task to an independent contractor with experience in performing security testing and evaluation.[4]

6. AGENCY IMPLEMENTATION OF FISMA

FMC continues to move forward, albeit slowly, in implementing an effective information security program. While the FMC has made strides in making enhancements to the program, it still falls short of the expectations OMB has for FISMA implementation throughout agencies. FISMA involves coordination throughout the program offices to protect agencies' information, assets, and employees. FISMA is the responsibility of the agency's information technology department and its program offices.

Notification of Finding # 2: Agency Implementation of FISMA

Condition

The FMC information security program falls short of OMB and NIST goals for a robust and fully integrated information security program. Specifically, FMC management is not focusing on FISMA as an agency responsibility.

Criteria

FISMA Sections 3544(a) (3) and (5) require the agency head to "delegate to the agency Chief Information Officer the authority to ensure compliance with the requirements imposed on the agency under this subchapter and ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions."

[4] OIT officials told the OIG that it was already considering this action prior to our presenting the recommendation in the draft report as a result of interim discussions with the review team.

FISMA Sections 3544(a) (1) and (2) requires the agency head to ensure that "information security management processes are integrated with agency strategic and operational planning processes;" and that "senior agency officials provide information security for the information and information systems that support the operations and assets under their control."

Cause

FMC senior management is not focusing on FISMA as an agency responsibility as required by the E-Government Act of 2002 with specific responsibilities for the agency head, Chief Information Officer, and Senior Information Security Officer because FISMA implementation at the FMC is largely an OIT responsibility. However, OIT lacks the authority and the resources to effectively document, implement, and enforce a strong information security program, resulting in inconsistent compliance with OMB and NIST guidance.

Because OIT was positioned within the Office of Administration, its ability to effectively report on the status of FMC's information security program to the FMC Chairman was minimized. For example, OIT does not receive a line item in the budget and makes financial requests through the Office of Administration. Furthermore, there is no line item for information security.

Effect

Because FMC management is not focusing on FISMA as an agency responsibility, OIT has been tasked to coordinate with organizational departments to strengthen information security concepts and responsibilities solely. Until FMC effectively and fully implements an agency-wide information security program, FMC data and systems will be vulnerable and will not be adequately safeguarded to prevent unauthorized use, disclosure, and modification.

Examples of an incomplete integration of its information security program throughout the agency include the following:

- FMC's inability to produce C&A packages that can provide management with detailed information to make creditable risk-based decisions.
- FMC's inability to attain a 100% employee completion rate for completing the annual security awareness training by its internally established target completion date.
- FMC's inability to demonstrate the active participation in the C&A process of the following positions as required by NIST SP 800-37: Chief Information Officer, Senior Agency Information Officer, Information System Owner, Information Owner, and Information System Security Officer.
- FMC's inability to document the overall effectiveness of the security controls implemented in the FMC information systems, which is essential in determining the risk to the organization's operations and assets, to individuals, and to other organizations.
- FMC's inability to produce an IT contingency plan for systems evaluated in our subset of systems.

Recommendation(s)

We recommend that:

3. The CIO provide regular reporting to the agency Chairman on the status of the FMC information security program that reflects the requirements of FISMA.

4. The CIO, with the support of the agency head, require program officials to work with OIT throughout all phases of the system development life cycle to ensure protection of FMC's information.

7. POA&M Review

A Plan of Actions and Milestones (POA&M) is used by agencies to identify and prioritize their security weaknesses. The document, required by OMB, is to include weaknesses identified by all sources.

The OIG reviewed FMC's POA&M tracking and reporting process to determine how effectively it is performing these activities. The OIG also evaluated how closely FMC followed OMB guidance for documenting POA&Ms. We reviewed the agency's POA&M, dated June 1, 2007, which included 11 identified agency deficiencies. All 11 items were reported as closed by OIT without independent verification. The OIG believes that six of the 11 POA&M items should remain open because they have not been sufficiently addressed. Either insufficient documentation was provided to support closing the POA&M items, or OIG analysis concluded the deficiency still exists. Although there was consistency in the numbers FMC has been reporting quarterly to OMB, those reports were not fully inclusive of the agency's weaknesses. The items the IG identifies as still open are as follows:

- POA&M #2 Reportable Condition - FMC IT policies are not finalized and many other needed policies have not been developed. For example, the agency does not have POA&M or system development lifecycle (SDLC) policies.
- POA&M #3 Reportable Condition - FMC is not tracking and reporting POA&M performance in accordance with OMB guidance and is not using the POA&M as a management tool to track vulnerabilities as envisioned by OMB. For example, POA&Ms vulnerabilities are not separated by program or system.
- POA&M #4 - FMC's Contingency Plan may be incomplete and needs to be consolidated and tested. The existing plan does not permit the effective recovery of systems or system components on-site or off-site.
- POA&M #6 - There are personnel, operational and technical control deficiencies that may affect the security of SERVCON and the FMC Network because the latest NIST guidance was not used.
- POA&M #7 - Access control policies and procedures are not documented, and technical access controls are not always implemented.
- POA&M #11 - Programming changes and security-related documentation for FMC-1 are needed to improve security of this major application. For example, security controls used to assess the system's security are obsolete.

Notification of Finding # 3: POA&M

Condition

FMC does not document "all" weaknesses in its POA&M and has not structured its POA&M into program-level and system-level deficiencies.

Criteria

OMB Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, dated October 17, 2001, requires each agency to submit "a plan of action with milestones to address all weaknesses identified by program reviews and evaluations."

OMB Memorandum 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, dated August 23, 2004, provides the following guidance:

> "OMB policy 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."
>
> "An agency should develop a separate POA&M for every program and system for which weaknesses were identified in the FISMA reports, as well as those discovered during other reviews including GAO audits, financial system audits, and critical infrastructure vulnerability assessments. Thus, the POA&Ms should either reflect consolidation with, or be accompanied by, other agency plans to correct security weaknesses found during any other review done by, for, or on behalf of the agency, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments."

OMB FISMA reporting guidance specifically requires agencies to "prioritize information technology security weaknesses to help ensure significant information technology security weaknesses are addressed in a timely manner and receive appropriate resources" (OMB Memorandum 07-19, Page 32). OMB Memorandum M-04-25 provides guidance on completing the POA&M.

Effect

The purpose of the 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 (OMB Memorandum 07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*). Without a complete POA&M, FMC may not be fully aware of the vulnerabilities and weaknesses inherent in the operation of FMC and contractor systems and thus cannot prioritize its needs. The FMC has consistently understated its information security posture to OMB by understating the number of information security weaknesses in its quarterly submissions. Consequently, OMB does not have a clear view of FMC's progress in addressing information security weaknesses.

FMC's POA&M does not demonstrate that weaknesses are arranged in priority of resolution. Based on review of the FMC's POA&M dated June 1, FMC had 11 weaknesses identified. The OIG believes that this total is understated based on our review and because the FMC has not assessed the security controls for systems in accordance with the specified guidance, leaving FMC with an inaccurate understanding of security control implementation and effectiveness. According to the POA&M, OIT identified no security control weakness during FY 2007.

Developing remedial action plans is key to ensuring that corrective actions are taken to address significant deficiencies and reduce or eliminate known vulnerabilities. The POA&M is a tool that identifies tasks that need to be accomplished. The POA&M details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones.

Cause

FMC management has not emphasized the importance of identifying deficiencies, documenting and prioritizing the weakness on the POA&M, and working towards resolution.

Recommendation

We recommend that:

5. FMC develop a process that ensures that all vulnerabilities noted throughout the agency are included on the POA&M. In addition, the documents or tools chosen to track the FMC POA&Ms should comply with OMB POA&M criteria.

8. CONTRACTOR SYSTEM CONCLUSIONS AND FINDINGS

OMB directed IGs to "include some contractor systems in their 'representative subset of agency systems,'"(OMB Memorandum 07-19, Question 37). OIG chose to evaluate the contractor system located at the U.S. Department of Agriculture, National Finance Center (NFC).

Notification of Finding # 4: Contractor System Review - National Finance Center

Condition

FMC management should do more to receive assurances regarding the security of FMC data processed at the U.S. Department of Agriculture National Finance Center (NFC), its payroll service provider.

Criteria

FISMA, Section 3544(a)(1)(A)(ii) states: "The head of each agency shall be responsible for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." Section 3544(b) requires that each agency develop, document and implement an agency-wide information security program, to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source." The Office of Management and Budget reiterates the previously-noted statutory requirements through its annual FISMA guidance in Memorandum 03-19 (page 5), 04-25 (page 5), 05-15 (page 7) 06-20 (page 9), and 07-19 (page 3).

OMB consistently provided specific guidance on the definition and required documentation from service providers: "Service providers encompass typical outsourcing of system or network operations, telecommunications services, or other managed services (including those provided by another agency and subscribing to software services). Agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed and such must be included in the terms of the contract. Agencies must ensure identical, not 'equivalent,' security procedures. For example, annual reviews, risk assessments, security plans, control testing, contingency planning, and C&A must, at a minimum, explicitly meet guidance from NIST." (Memorandum 05-15 [Question 16], Memorandum 06-20 [Question 28], and Memorandum 07-19 [Question 37]).

Cause

The agency informed the OIG that it has in the past requested such documentation from its service providers, but does not routinely follow up with them when the requested documentation is not provided.

Effect

FMC does not have reasonable assurance that controls are implemented correctly, are operating as intended, and are producing the desired outcome with respect to meeting the security requirements over its personnel and payroll data. The agency is still responsible for safeguarding FMC data and ensuring that other entities protect FMC data commensurate with FMC and FISMA requirements, regardless of whether the contractor is another Federal agency.

Recommendation

We recommend:

6. FMC at a minimum, annually request the accreditation letter for all contractor systems to validate security control effectiveness and implement due diligence activities on external entities that handle FMC's information. Document attempts to obtain the information and report to the contracting officer.

9. Security Awareness Training Conclusions and Findings

FMC has taken significant steps to enhance security awareness by introducing a more in-depth annual computer security awareness program, including providing an interactive online course with a required "quiz" by employees at completion and developing the *IT Security for Personnel Policy, OIT- P11*, to further strengthen employee awareness. The new security awareness training provides much needed understanding of information security concepts and emerging technology-related threats.

The security awareness training was thorough; however, there were few references to FMC policies. It is extremely beneficial to incorporate agency policy and practices into annual training, so that employees can directly relate what they are learning to their workplace environment.

- The vendor that developed the training course also facilitated the recording of employees that completed the training course. The OIG reviewed the course participants spreadsheet used to track security awareness training provided by OIT. According to the data, only seven of 119 employees failed to take the course by the appointed deadline. OIT staff contacted the employees' supervisor to emphasize the importance of the training. Within the first week after the deadline, four of the remaining employees had completed security training. By the end of the second week all FMC employees had completed training.

Notification of Finding # 5: Adherence to the Agency Policy, IT Security for Personnel Policy, OIT-P11

Condition

The FMC *IT Security for Personnel Policy* has not been enforced. Specifically OIT did not disable accounts of employees or contractors who did not complete the security awareness training by the FMC imposed deadline as called for in the policy.

Criteria

FISMA Section 3544(b)(4)(A) and (B) requires each agency "to develop, document, and implement an agency-wide information security program, to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks."

FMC *IT Security for Personnel Policy*, OIT-P11 (May 16, 2007) states: "If employees or contractors do not take the security training within the required timeframe, upon their next login into the network they will be automatically redirected to the training class and access to the network will not be granted until the training has been successfully completed."

Cause

Management decision. Due to the substantial impact on staff's ability to perform its duties and responsibilities, management delayed enforcement of the policy for one year.

Effect

If the imposed deadlines are not enforced, we would expect to see the security training participation rate drop, with larger numbers of staff not taking the required training in successive years.

Recommendation

The OIG spoke to the Director of Administration (DA) regarding management's decision to enforce policy. He explained that it was his decision not to terminate network access for the affected employees due to the policy's recent effective date. While not enforcing the policy, management identified the employees who did not take the training and spoke with their respective supervisors to ensure that training was completed before the end of the fiscal year. We support the DA's decision in the initial year, but will monitor the policy's enforcement in the out years.

10. Contingency Planning Conclusions and Findings

The OIG reviewed OIT's contingency planning efforts to assess how prepared the agency is to recover from a disruption. As part of the evaluation, OIG reviewed the *Federal Maritime Commission (FMC) Safety and Security of Employees and Operations Plan/Continuity of Operations Plan (SSEOP/COOP)* dated July 25, 2006.

A COOP is defined as "a predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations" (NIST SP 800-34). In contrast, a disaster recovery plan applies to major, usually catastrophic events, that deny access to the normal facility for an extended period. Frequently, disaster recovery plans refer to an IT-focused plan designed to restore operability of the target system, application or computer facility at an alternate site after an emergency. The disaster recovery plan scope may overlap an IT contingency plan; however, the disaster recovery plan is narrower in scope and does not address minor disruptions that do not require relocation.

IT contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of IT systems, operations, and data after a disruption. Contingency planning generally includes one or more of the approaches to restore disrupted IT services:

- Restoring IT operations at an alternate location
- Recovering IT operations using alternate equipment
- Performing some or all of the affected business processes using non-IT (manual) means (typically acceptable for only short-term disruptions)

FMC OIT developed the SSEOP/COOP that identifies the agency's mission-critical systems:

- NFC Payroll
- Bureau of Public Debt (BPD) – Accounting/Travel/Procurement
- E-mail
- Agency Web site
- Service Contracts Internet Based Filing System (SERVCON)

Non-critical applications would be reestablished once the critical systems are functioning. Reestablishing access to contractor-owned systems is also discussed.

The SSEOP/COOP identifies the roles and responsibilities of key personnel at the agency:

- The FMC Chairman
- Director of Administration
- All office heads
- Deputy Director of Administration
- Director of OIT
- OIT staff
- Director of Office of Management Services
- Director of Office of Financial Management
- Director of Human Resources

The SSEOP/COOP identifies operating procedures in four different disaster scenarios. Recovery procedures address office space reconstruction, telecommunications (voice and data), and some aspects of system recovery for key systems. Key recovery documents and emergency contact information are also identified. Restoration of non-critical applications is also discussed.

On May 31, 2007, the FMC conducted a test of the SSEOP/COOP. OIT documented the testing results, which included applications tested, strengths, areas of improvement, and potential follow-up items. Testing results show the successful recovery of many FMC applications, however; there were noted issues with testers accessing the mission-critical application SERVCON.

Notification of Finding # 6: FMC emergency preparedness documentation and SSEOP/COOP does not address IT recovery in sufficient detail.

Condition

FMC emergency preparedness documentation does not address IT recovery in sufficient detail and omits the FMC Network. Specifically, documentation is not detailed enough to provide sufficient guidance in recovering FMC's IT infrastructure; the SSEOP /COOP does not specifically focus on the recovery of IT resources and does not provide sufficient detail to substitute for a Disaster Recovery Plan or Contingency Plan. The OIG additionally noted a discrepancy in the documented recovery time expectation for remote e-mail service. In section 8(C) of the COOP, the recovery time expectation is 48 hours; while, section 8(D) states 72 hours is the expected remote e-mail recovery time.

Additional weaknesses identified included the following:

- OIT vendor agreements and required equipment are not included in the SSEOP/COOP.
- The emergency contact list was not provided with the SSEOP/COOP.
- Emergency contact information for all agency IT staff was not provided.
- The SSEOP/COOP does not contain detailed recovery instructions. For example, the SSEOP/COOP does not provide detail instructions to initiate operation from the alternate processing site
- Tape backup and recovery procedures were not included in the SSEOP/COOP.

Criteria

FISMA Section 3544(b)(8) identifies agency responsibility to include the development of "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."

NIST Special Publication 800-34, *Contingency Planning for Information Technology Systems*, dated June 2002, provides "instructions, recommendations, and considerations for government IT contingency planning. Contingency planning refers to interim measures to recover IT services following an emergency or system disruption."

Cause

FMC management has not ensured key organizations coordinate to produce an agency COOP that incorporates the usage of NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002. FMC has not demonstrated the incorporation of the following documents into the FMC SSEOP/COOP:

- Disaster Recovery Plan
- Contingency Plan
- Occupant Emergency Plan

Effect

FMC is likely to experience delays in recovering IT operations after an emergency, no matter what the degree of significance. Without a documented contingency plan, there is no way to ensure repeatability, consistency and recovery procedures.

Recommendation(s)

We recommend FMC:

7. Require a disaster recovery plan be documented to cover areas the contingency plan does not address, including the alternate processing site.
8. Require contingency planning and disaster recovery activities to stay updated with the identification and contact information for remote operating sites, vendor agreements, and backup/recovery procedures, recovery time expectations, contact information for emergency personnel and detailed system recovery procedures for all major applications.

11. Wireless Network Vulnerability Scan Conclusions and Findings

The OIG performed a wireless network vulnerability scan to identify weaknesses within the agency's wireless environment. A wireless access point discovery test was conducted in order to determine if any unauthorized wireless networks were deployed and if the authorized access points were in compliance with the FMC wireless technology policy at the following FMC facility:

800 North Capitol Street, NW
Washington DC 20537

On August 22, 2007, from 11:40AM to 12:30PM, an external wireless access point discovery was conducted from ground level across the street from the FMC facility. During this portion of the engagement, a wireless access point was detected using a yagi unidirectional wireless high-gain antenna that was broadcasting a Service Set Identifier (SSID) of FMCWA. The access point detected was later confirmed to be the SSID of one of two approved FMC wireless network access points.

On August 22, 2007, from approximately 1:15PM to 2:20PM, a floor-by-floor rogue wireless access point discovery sweep was conducted by OIG information security experts accompanied by OIG staff. There were no rogue wireless access points detected from within any of the FMC offices. No other access points were identified as being broadcast from facilities outside the FMC facility.

Notification of Finding # 7 Adherence to the Agency Policy, Wireless Communication Policy, OIT- P08

Condition

The FMC wireless network is broadcasting a SSID named "FMCWA" which identifies the FMC's wireless network to potential hackers. In addition, the SSID name is in non-compliance with the *Wireless Communication Policy, OIT-P08*. The OIG performed its wireless network vulnerability activities to assess FMC's wireless network security posture. The wireless network is running the IEEE 802.11g protocol and Temporal Key Integrity Protocol encryption, which provide sufficient security for the network. Furthermore, the wireless technology products used at FMC do provide AES-encryption consistent with FIPS 197.

Criteria

FISMA Section 3544(b)(4)(A) and (B) requires each agency "to develop, document, and implement an agency-wide information security program, to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks."

FMC *Wireless Communication Policy*, OIT- P08 (May 16, 2007) provides the following guidance:

- "The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier (Section 5.c)."
- "Configure the SSID in accordance with this policy (Section 6.a.i)."

Cause

OIT has not fully enforced FMC's *Wireless Communication Policy.*

Effect

The wireless network broadcasting the SSID "FMCWA" makes FMC information recognizable to those within the broadcast signal of the wireless access point, e.g., non-FMC staff outside of FMC offices. Based on the type of information FMC is entrusted with, intellectual property is at risk of casual exposure.

Recommendation

9. We recommend that the OIT rename the wireless network SSID that is broadcasting to a name less attributable to FMC.

12. Safeguarding Personally Identifiable Information (PII)

FMC has made progress in implementing the provisions set forth in OMB Memorandum 06-15 dated May 22, 2006. FMC has named a Senior Agency Official for Privacy (SAOP) and management has taken steps towards educating employees about protecting sensitive information and safeguarding PII. The newly introduced computer security awareness training discusses various topics related to protecting sensitive information and explains ramifications of not safeguarding PII.

The newly appointed SAOP did not conduct any reviews that covered all administrative, technical, and physical means used by FMC to control PII, including but not limited to procedures and restrictions on the use or removal of PII beyond agency's premises or control. On the other hand, the OIG has identified signs of progress in this area and will re-evaluate the implementation status of the PII requirements in next year's FISMA evaluation.

MANAGEMENT'S COMMENTS

FEDERAL MARITIME COMMISSION

Memorandum **Date**: November 14, 2007

To : Inspector General

From : Acting CIO

Subject : Comments on Review of FMC's Implementation of FISMA for FY2007

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

Finding #1: Certification & Accreditation

Response: We acknowledge that the current C&A documentation for FMC's three systems does not comply with the most-recently revised NIST and OMB guidance, and that this constitutes a significant deficiency. We also agree that setting modest, achievable goals over a period of years will provide a long-term solution to the deficiency. We will report this significant deficiency in our next FMFIA Report (to be contained within the FY 2008 PAR), and will establish appropriate POA&M(s) to address the issues. It is our understanding that completion of Recommendations #1 and #2 immediately below will be a major step in addressing the significant deficiency.

Recommendation 1. For the three systems identified...OIT should [use] FIPS 199 to identify impact levels...identifying minimum security requirements...based on FIPS 200, and implement required security controls using NIST SP 800-53, Revision 1.

Response: We intend to address these matters by involving an experienced contractor in the process. OIT contracted with Cogent in late FY2007 to begin the development of appropriate FISMA documentation identified in the IG's Report. Further, the FMC soon will bring on board a new Deputy Director/CIO. Due to the significant complexity of tasks necessary to address these recommendations, we are not providing a corrective action completion date for this recommendation in order to allow the new CIO time to familiarize himself with the recommendation and establish an appropriate corrective action due date. It is our understanding that the OIG has no objection if the CIO develops a schedule of corrective actions for this and other recommendations by January 15, 2008.

Recommendation #2. Once the FMC has established the minimum required controls, FMC should test these controls...OIT should consider contracting this task to an independent contractor with experience in performing security testing and evaluation.

Response: We intend to do appropriate testing once Recommendation #1 is implemented, and will consider the related experience of contractors as a factor in determining which should be selected to accomplish testing and evaluation. Action on this Recommendation cannot be initiated until Recommendation #1 is accomplished. For the reasons identified in Recommendation #1 above, we are not providing a corrective action completion date for this recommendation at this time. It is my understanding that the OIG has no objection if the CIO provides a schedule of corrective actions for this and other recommendations by January 15, 2008.

Recommendation #3. The CIO provide regular reporting to the agency Chairman on the status of the FMC information security program....

Response: As you know, the Commission has been without an agency Chairman for almost one year, and has had a succession of CIO/acting CIOs during that timeframe. We agree that, due to that confluence of events, regular reporting has become less than regular. However, a new CIO will come on board shortly to fill the position on a permanent basis; further, it is our hope that the current Senate confirmation process for a permanent FMC Chairman also will be completed shortly. We intend to re-establish regular reporting procedures on IT information security issues and have established March 30, 2008, as a corrective action completion date for this recommendation. By that time, we will be able to provide dates and times when the CIO provided reports to the agency head to establish that regular reporting is taking place.

Recommendation #4. The CIO, with support of the agency head, require program officials to work with OIT throughout all phases of the system development life cycle to ensure protection of FMC's information.

Response: We continue to take issue with the characterization of OIT's role within the agency as the sole entity charged with IT security responsibility. The role of CIO has been formally recognized by the Commission as part of its organizational structure at 46 C.F.R. 501.5(k)(2), where these duties are made the responsibility of the Deputy Director of Administration. The Deputy Director is responsible for OIT activities and exercises substantive oversight over all such IT activities; the CIO also coordinates with FMC senior management on IT security matters. Further, the FMC's budget process ensures complete transparency of funding for IT and the position of the CIO ensures that senior management at the highest level is aware of IT needs. Evidence of this is the significant expenditure of funds in FY 2007 for IT requirements upon presentation of issues to senior management by the Acting CIO, and subsequently to the Commission. Further, we believe that OIT has established an exemplary record of working directly with program officials on matters related to their applications.

Those perceived failures identified in the Review are not the result of a lack of "visibility" and subsequent dismissal of IT requirements, but of other factors which the OIG has been advised of. However, we understand that we can do more to memorialize our commitment to FISMA as an agency responsibility; we will ensure that System Development Life Cycle documentation is amended to be more specific regarding such coordination, including the protection of agency information. We have established a corrective action completion date of September 30, 2008, for accomplishment of this action.

Recommendation #5. FMC document and distribute a POA&M policy and develop a process that ensures that all vulnerabilities noted throughout the agency are included on the POA&M. In addition, the documents or tools chosen to track the FMC POA&Ms should comply with OMB POA&M criteria.

Response: With respect to the Recommendation, we will develop and distribute a POA&M procedure which includes a process to capture all weaknesses and include them on the POA&M in line with OMB criteria. We have established a corrective action completion date of September 30, 2008, for accomplishment of this action.

Recommendation #6. FMC at a minimum, annually request the accreditation letter for all contractor systems to validate security control effectiveness and implement due diligence activities on external entities that handle FMC's information. Document attempts to obtain information and report to the contracting officer.

Response: We will request the accreditation letter from our contractor systems, and will document all attempts to obtain the information and report same to the contracting officer. We have established a corrective action completion date of March 30, 2008, for accomplishment of this process.

Recommendation #7. Require a disaster recovery plan be documented to cover areas the contingency plan does not address, including the alternate processing site.

Response: We will review the efficacy of additions to the disaster recovery plan, including that recommended, and will make appropriate changes. For the reasons listed in response to Recommendation #1 above, we are not providing a corrective action completion date for this recommendation at this time. It is my understanding that the OIG has no objection if the CIO provides a schedule of corrective actions for this and other recommendations by January 15, 2008.

Recommendation #8. Require contingency planning and disaster recovery activities to stay updated with the identification and contact information for remote operating sites, vendor agreements, and backup/recovery procedures, recovery time expectations, contact information for emergency personnel and detailed system recovery procedures for all major applications.

Response: We will update and expand our contingency plan and disaster recovery packages to provide for all IT-related items mentioned in the recommendation. For the reasons listed in response to Recommendation #1 above, we are not providing a corrective action completion date for this recommendation at this time. It is my understanding that the OIG has no objection if the CIO provides a schedule of corrective actions for this and other recommendations by January 15, 2008.

Recommendation #10. We recommend that the OIT rename the wireless network SSID that is broadcasting to a name less attributable to FMC.

Response: This Recommendation was completed on September 1, 2007.

James Woods

cc: Director of Administration