Office of Inspector General

Independent Evaluation Report of FMC's FY 2011 Implementation of FISMA

A12-02

January 2012

FEDERAL MARITIME COMMISSION

FEDERAL MARITIME COMMISSION
Washington, DC 20573

January 17, 2012

Office of Inspector General

Dear Chairman Lidinsky and Commissioners:

The Office of Inspector General submits its report on the status of information security at the Federal Maritime Commission for FY 2011. The OIG relied on the expertise of information Security evaluators from *Your Internal Controls LLC* for assistance on this mandated review.

The objectives of the independent evaluation of the FMC information security program were to evaluate the FMC's security posture by assessing compliance with the Federal Information Security Management Act (FISMA) and related information security policies, procedures, standards, and guidelines. The scope of this task included the FMC Network, and applications housing service contracts (SERVCON) tariff location filings (FORM-1) and FMC license applications (FORM-18). The OIG also assessed management actions to implement the OIG recommendations and documented the status of prior recommendations.

The FY 2011 report contains 12 subject matter findings and 20 recommendations for corrective actions. Many of the OIG recommendations have already been implemented by management. Only on one recommendation does the OIG and management continue to disagree (see recommendation 12). The OIG, together with the audit follow up official, will work to resolve the differences.

The OIG thanks FMC staff, especially the Office of Information Technology, for its assistance in helping us to meet our report objectives.

Respectfully Submitted,

/Adam R. Trzeciak/
Inspector General

TABLE OF CONTENTS

PURPOSE

Your Internal Controls (contractor), on behalf of the Federal Maritime Commission (FMC), Office of Inspector General, conducted an independent evaluation of the quality and compliance of the FMC information security program with applicable federal computer security laws and regulations. *Your Internal Controls'* evaluation focused on FMC's information security program as required by the Federal Information Security Management Act (FISMA).

This report was prepared by *Your Internal Controls* with guidance by the Office of Inspector General. The vulnerabilities discussed in this report should be included in FMC's Fiscal Year (FY) 2011 report to the Office of Management and Budget (OMB) and the Congress.

BACKGROUND

On December 17, 2002, the President signed into law H.R. 2458, the E-Government Act of 2002 (Public Law 107-347). Title III of the E-Government Act of 2002, commonly referred to as FISMA, focuses on improving oversight of federal information security programs and facilitating progress in correcting agency information security weaknesses. FISMA requires federal agencies to develop, document and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency. This program includes providing security for information systems provided or managed by another agency, contractor or other source. FISMA assigns specific responsibilities to agency heads and Inspectors General (IGs). It is supported by security policy promulgated through the Office of Management and Budget (OMB), and risk-based standards and guidelines published in the National Institute of Standards and Technology (NIST), Special Publication (SP) series.

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems. FISMA directs federal agencies to report annually to the OMB Director, Comptroller General and selected congressional committees, on the adequacy and effectiveness of agency information security policies, procedures and practices, and compliance with FISMA. In addition, FISMA requires agencies to have an annual independent evaluation performed on their information security programs and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG. Implementing adequate information security controls is essential to ensuring an organization can effectively meet its mission.

SCOPE AND METHODOLOGY

The scope of our testing focused on the FMC General Support Systems (GSS) and Major Applications (MA). We conducted our testing through inquiry of FMC personnel, observation of activities, inspection of relevant documentation and the performance of technical security testing. Some examples of our inquiries with FMC management and personnel included, but were not limited to, reviewing system security plans, access controls, risk assessments and configuration management processes.

CURRENT YEAR FINDINGS

During our FY 2011 evaluation, we noted that FMC has taken steps to improve the information security program. For example, a complete system inventory is now in place and a master listing of issues is maintained for reporting and correction. This listing of issues includes both the current year and all issues identified in prior years. On the other hand, security threats and vulnerabilities continue to increase and become more sophisticated. To help mitigate these threats, we've identified 12 areas where FMC could improve its security posture.

MANAGEMENT RESPONSES

At the conclusion of each finding, we have attached management's response to the OIG recommendation(s). In many cases, the OIG has closed the recommendation based on management's response and OIG follow up. In other instances, the OIG was unable to close the recommendation, either due to management's assertion that the recommendation would be implemented in the future, or, we could not verify actions asserted by management without detailed follow up and/or additional fieldwork. The OIG will perform all necessary verification processes in the FY 2012 FISMA cycle.

01. Patches and Service Packs

Condition:

The FMC Office of Information Technology (OIT) uses a software product called Numara, which is used primarily to identify patches and service packs that are out of date, and classifies the patches as critical, important, etc. We obtained the latest Numara report, which was run on 9/1/11. The report indicated that servers supporting the FMC applications were missing the following patches and service packs:

- 3,404 patches (1,158 of which were identified as critical and 1,741 as important by the software)
- 1,158 service packs

The software product (Numara) did not identify specific definitions for what constitutes a critical or important patch, however, the number of patches and service packs missing is the primary focus of this issue.

Criteria:

FMC Patch Management Policy, OIT-P12, states the following:

Section 1. Purpose. "The purpose of this policy is to establish responsibilities and procedures for updating FMC systems with newest patches and security updates. The purpose of this policy is to ensure that user accounts exist only for authorized users and FMC OIT staff is required to regularly identify, disable and purge inactive accounts in a timely and coordinated manner."

Section 5. Patch Management. "OIT will, on an ongoing basis, identify, evaluate and implement patches applicable to the systems for which it is responsible."

The NIST guides used as criteria address the patching process. As patches are deployed, this may inadvertently change some of the configuration settings on a server (e.g. audit and password settings); therefore it is essential to review patches prior to deploying them. It is also essential to review the configuration settings once the patches have been deployed to ensure that an effective security posture is maintained.

NIST 800-123 Guide to General Server Security, Section 4.1 states "Once an operating system (OS) is installed, applying needed patches or upgrades to correct for known vulnerabilities is essential. Any known vulnerabilities an OS has should be corrected before using it to host a server or otherwise exposing it to untrusted users. To adequately detect and correct these vulnerabilities, server administrators should do the following:

- Create, document, and implement a patching process.
- Identify vulnerabilities and applicable patches.

- Mitigate vulnerabilities temporarily if needed and if feasible (until patches are available, tested, and installed).
- Install permanent fixes (patches, upgrades, etc.)

Section 3.3 states "Organizations should develop standardized secure configurations for widely used Operating Systems and server software. This will provide recommendations to server and network administrators on how to configure their systems securely and ensure consistency and compliance with the organizational security policy. Because it only takes one insecurely configured host to compromise a network, organizations with a significant number of hosts are especially encouraged to apply this recommendation."

Cause:

The Office of Information Technology indicated that it lacks the budget and staffing resources to comply.

Risk:

Patches are deployed to close those areas subject to exploitation. Without the latest patches being deployed, identified vulnerabilities may be exploited through known attack venues. Further, there is the potential for remote code execution through exploitation of buffer overflows (e.g. sending a request for information to the network an inordinate amount of times, ultimately crashing the server and making it inoperable), and other vulnerabilities.

Recommendation(s):

1. From the report generated via the Numara software product, identify which patches and service packs can be deployed without harming the network. Further, upon completion, review the configuration settings of the servers to ensure security settings have not changed. *(The OIG estimates the required level of effort for this recommendation to be 40 hours).*

Management Response:

FMC's OIT department has deployed the patches as recommended and has reviewed the security settings of the servers to ensure the server security settings have not been altered. A copy of the new report has been provided. Further, OIT has instituted automatic updates for the desktop environment to ensure timely patch deployment.

OIG Comments to Management Response:

OIG obtained the latest patch and service pack report via Numara and noted the following:

- 41 missing patches
- 22 missing service packs

The number of patches and services packs missing are within the reasonable limits and this appears to have been resolved at this time. The OIG agrees with management response and this issue is considered closed.

02. Audit Settings

Condition:

We reviewed the audit settings for the servers supporting the FMC applications and noted the following:

1. There is no evidence that audit logs are reviewed by IT personnel. As a result, without reviews of audit logs, there will be no actions taken to mitigate those events generated on an audit log. The audit logs identify those actions which are deemed adverse to the agency. An example of an adverse action would be an unauthorized user attempting to access and modify data.
2. The audit logs are set to storage space that is not large enough to meet the needs of the agency. Further, once the audit logs reach space capacity, they are set to overwrite, meaning that older logs will be deleted as new logs are generated. The current size settings are as follows:

    - Application audit log – 9,984KB
    - Security Log – 179,584KB
    - System log – 9,984KB

Criteria:

NIST 800-123, Guide to General Server Security, section 4.2.3 states "Auditing should also be enabled as appropriate to monitor attempts to access protected resources."

NIST 800-53, Recommended Security Controls for Federal Information Systems and Organizations, page F-25 (AU-4) states "The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded."

NIST 800-53 Recommended Security Controls for Federal Information Systems and Organizations, page F-25 (AU-4) states "a) Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and b) Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information."

Cause:

The cause is primarily a lack of personnel, budget, or time constraints to adequately monitor the network.

Risk:

Without appropriate reviews of the audit logs, IT personnel may not be aware of any adverse actions taken against the FMC network. This may lead to data corruption or other violations against the agency. Furthermore, without appropriate space requirements for the audit logs, the audit logs generated may either stop working (because the log filled up) or overwrite the existing logs, making the audit logs irrelevant. The storage space requirements should be changed immediately, as there should be no cause for these settings.

Recommendation(s):

2. Ensure that audit logs are reviewed monthly and necessary actions are taken to respond to those audit events generated as a result of adverse actions. *(The OIG estimates the required level of effort for this recommendation to be 5 hours per month.)*

3. Set the audit logs to a size that can sustain the logs being generated. Also, as the logs fill up, they should be moved to another storage medium so that current logs are maintained. *(The OIG estimates the required level of effort for this recommendation to be 4 hours.)*

Management Response:

FMC in following the recommendations of the Office of the Inspector General has increased the size of the audit logs to 1024 megabytes and has implemented a monthly log retention and review process whereby the server logs are reviewed on the first Monday of every month. Once reviewed, the logs will be moved to a designated log folder in the OIT shared area.

OIG Comments to Management Response:

OIG will retest this issue during the next FISMA cycle, as evidence for management response has not been verified or tested.

03. Data Center

Condition:

We obtained a list of users with access to the Data Center. There were a total of 28 badges with access to the Data Center. The badges were assigned as follows:

- 10 – OIT
- 6 – Janitorial, Building and Property services
- 12 badges to non-OIT personnel. Some of those badges were issued to contractors.

Criteria:

NIST 800-53 Recommended Security Controls for Federal Information Systems and Organizations page F-78 (PE-3) states "The organization enforces physical access authorizations to the information system independent of the physical access controls for the facility." Enhancement Supplemental Guidance: "This control enhancement applies to server rooms, media storage areas, communications centers, or any other areas within an organizational facility containing large concentrations of information system components. The intent is to provide additional physical security for those areas where the organization may be more vulnerable due to the concentration of information system components. Security requirements for facilities containing organizational information systems that process, store, or transmit Sensitive Compartmented Information (SCI) are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. See also PS-3, security requirements for personnel access to SCI."

Cause:

The primary cause is the lack of knowledge of access requirements with respect to accessing the Data Center.

Risk:

Only select IT personnel should have access to the Data Center. Providing access to individuals without a bona fide need increases monitoring costs as well as the likelihood that non-OIT users can sabotage server and data controls. Simply put, the more people that have access to sensitive areas and systems, the more that can go wrong. Access should be based on job requirements.

Recommendation(s):

4. Ensure only IT personnel and others with a job-related need have access to the Data Center by reviewing non-OIT personnel access badges and disabling as appropriate. *(The OIG estimates the required level of effort for this recommendation to be 3 hours.)*

Management Response:

FMC in following the recommendations of the Office of the Inspector General has reduced the number of data center access badges from 28 to 15. A copy of the current individuals with data center access is provided. Further, OIT will review access to these spaces on a regular basis.

OIG Comments to Management Response:

The OIG agrees with management's response. An updated listing of data center access has been obtained and this issue has been corrected. This issue is considered closed.

04. Contingency Plan

Condition:

We obtained the latest Contingency Plans for the network GSS and SERVCON and noted the following:

1. The latest Contingency Plans had not been signed or finalized.
2. The latest Contingency Plans were completed in March 2009 and are due for review and updates (if applicable).
3. There have been no formalized tests of a simulated disaster contingency to be prepared in the event of a disaster.
4. There are no software products deployed to operate the network in the event of a disaster. For example, if the network becomes inoperable, the FMC customers will not be able to access their data (e.g. via SERVCON and email).

Disaster Recovery Planning and Implementation

On May 31, 2011, the FMC headquarters building and surrounding area experienced a massive power outage that lasted over two days. Such events, although rare, are generally addressed in agency Continuity of Operations Plans (COOP) and Disaster Recovery Plans (DRP), with the intent of enabling agencies to continue essential functions for staff and stakeholders alike should events occur.

Beginning in FY 2006, the OIG issued security evaluation findings critical of the agency's COOP and DRP. For example, our 2006 evaluation noted that the agency lacked plans for specific incidents, to include power outages and hardware failures. In November 2007, the OIG reported that the FMC's emergency procedures documentation did not address IT recovery in sufficient detail and that it omitted the FMC network entirely. We warned that the FMC was likely to experience delays in recovering IT operations after an emergency. In our 2009 evaluation, we noted that the FMC lacked an adequate contingency planning program, to include policies, procedures, testing and documentation.

In the FY 2010 evaluation, we noted that the SERVCON contingency plan was not tested, nor were there any contingency planning policies and procedures to identify the frequency and types of tests to perform. The OIG warned of likely delays when recovering from a system failure due to incomplete and untested contingency planning.

In FY 2010, management informed the OIG that it took part in the Federal Emergency Management Agency's (FEMA) Eagle Horizon 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, it now appears that the connections tested were, in fact, the headquarters datacenter, and not those at the COOP site.

The power outage impacted critical business operations because the agency could not rely on its COOP site and its disaster recovery plan to take over for the temporarily non-functioning FMC servers. Commission staff was without email, phones and internet access for over 48 hours. Further, critical online business applications, including SERVCON were down. Importantly, no FMC applications were accessible at the COOP site. Only one server – Form FMC-1 – was in place but it was not connected. No other servers were in place.[1]

At the same time, the agency was spending approximately $24,000 per year over three years to maintain the COOP site in the event of an emergency, even though, unbeknownst to senior management, it was not functional.[2] When management discovered the situation in June of 2011, it cut funding at the site until such time that a DRP could be prepared and implemented.

Moving forward, the agency has begun discussions with Health and Human Services (HHS) regarding the agency's disaster recovery plan as a first step in establishing a comprehensive agency wide COOP plan. Specifically the agency is exploring "contracting" its data replication needs to facilities within HHS. For about $79,000 per year, the agency can purchase a full contingency back up. Once up and running, the agency plans to transition its data center to NIH, eliminating the need to maintain a data center at the FMC. The agency would then rely on security provided by HHS, reducing the agency's costs for many security requirements. The agency is also considering a scaled-down version whereby it could replicate data from its file server, email and SERVCON application for about $27,000 annually. The OIG believes that these approaches have merit and should be seriously considered as a viable and cost effective solution to addressing OIT's contingency needs and FISMA requirements.

[1] The FMC battery backups at its headquarters datacenter worked as designed. All servers were provided power to safely shut down without any data loss. However, these battery backups were not designed to power servers to keep them running. Consequently, the agency temporarily lost all net-based services.

[2] The amount spent by the agency over this three year period to rent space for FMC servers that were never installed represents funds put to better use by the FMC totaling $72,000.

Criteria:

NIST 800-34 Contingency Planning for Federal Information Systems 3.6 states "To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure and policies. During the Operation/Maintenance phase of the Software Development Life Cycle (SDLC), information systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that the Information System Contingency Plan (ISCP) be reviewed and updated regularly as part of the organization's change management process to ensure that new information is documented and contingency measures are revised if required.

NIST 800-34 Contingency Planning for Federal Information Systems 3.5 states "Plan Testing, Training, and Exercises (TT&E)… An ISCP should be maintained in a state of readiness, which includes having personnel trained to fulfill their roles and responsibilities within the plan, having plans exercised to validate their content, and having systems and system components tested to ensure their operability in the environment specified in the ISCP. In addition, as indicated in Step 4 (Assess Security Controls) of the RMF, the effectiveness of the information system controls should be assessed by using the procedures documented in NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*. NIST SP 800-84, *Guide to Test, Training and Exercise Programs for Information Technology Plans and Capabilities,* provides guidelines on designing, developing, conducting, and evaluating test, training, and exercise (TT&E) events so that organizations can improve their ability to prepare for, respond to, manage, and recover from adverse events. While the majority of TT&E activities occur during the Operations/Maintenance phase, initial TT&E events should be conducted during the Implementation/Assessment phase of the SDLC to validate ISCP recovery procedures."

"Organizations should conduct TT&E events periodically, following organizational or system changes, or the issuance of new TT&E guidance, or as otherwise needed. Execution of TT&E events assists organizations in determining the plan's effectiveness, and that all personnel know what their roles are in the conduct of each information system plan. TT&E event schedules are often dictated in part by organizational requirements. For example, NIST SP 800-53 includes a control (CP-4) for federal organizations to conduct exercises or tests for their systems' contingency plans around an organization-defined frequency. Section 3.5.4 provides guidance on the type of TT&E identified for each FIPS 199 impact level."

"For each TT&E activity conducted, results are documented in an after-action report, and lessons learned corrective actions are captured for updating information in the ISCP." The NIST SP 800-84 provides detailed information on how to plan and conduct TT&E activities.

Cause:

The lack of personnel, budget, or time to adequately review and update the Contingency Plans, as well as deploy software products to support the network in the event of a disaster.

Risk:

In the event of a disaster, the FMC will be unprepared, as occurred in June 2011. Although data is being backed up and stored off-site, this provides for data reconstitution only and not necessarily ongoing live administration. The current setting for FMC did not allow for continuous connectivity in the event of a disaster.

Recommendation(s):

5. Ensure that the Contingency Plan has been reviewed and signed off as final. Also, ensure that OIT performs a contingency test, training, and exercise in accordance with NIST 800-34. The estimated level of effort for this recommendation is 40 hours.

Management Response:

FMC acknowledges finding # 04. FMC has met with HHS regarding the agency's disaster recovery plan as a first step in establishing a comprehensive agency-wide contingency plan. FMC anticipates implementing and testing this recommendation by the fourth quarter of FY12.

OIG Comments to Management Response:

OIG has reviewed management's response; however this response does not address all of the issues contained within the condition. For example, the Contingency Plan needs to be finalized and signed which was not reflected in management's response. This will be tested again in the next FISMA cycle, however this issue is relatively straightforward to correct and this should be remediated sooner than the anticipated timeframe.

05. Incident Response

Condition:

Incident response is concerned with identifying, managing and preventing those events that are attacks on an agency network. We inquired about incident response with IT personnel. It was revealed that there is no incident response training for IT personnel to assist in identifying harmful incidents. There is also no incident response reporting mechanisms in place to identify, document, report and manage those security related incidents that arise.

Criteria:

NIST 800-53 Recommended Security Controls for Federal Information Systems and Organizations page F-63 (IR-5) states "The organization tracks and documents information system security incidents. Supplemental Guidance: Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including,

for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports."

NIST 800-53 Recommended Security Controls for Federal Information Systems and Organizations page F-61 (IR-2) states "(1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations. (2) The organization employs automated mechanisms to provide a more thorough and realistic training environment."

Cause:

OIT indicated that it lacks the budget and staffing resources to comply.

Risk:

In the event of an incident, the FMC will likely be unprepared to isolate an exploited weakness from the FMC network because incident response training has not been provided to OIT personnel that manage the network.

Recommendation(s):

6. Ensure that IT personnel are properly trained with regard to incident response prevention, detection, and correction. The estimated level of effort for this recommendation is 40 hours per year for each OIT employee with incident response responsibilities.
7. The FMC should implement formal incident response procedures so that in the event of an incident, the appropriate responses could be taken to minimize any adverse impact to the agency. *(The OIG estimates the required level of effort for this recommendation to be 20 hours.)*.

Management Response:

FMC's information technology personnel are required to take and pass an additional security awareness test designed for IT professionals annually. FMC IT personnel are also required to annually review and be familiar with Managing Directive 2011 – 2 Incident Response, and FMC form 93 Initial Security Incident Report at the conclusion of the annual security awareness test designed for IT professionals.

OIG Comments to Management Response:

OIG agrees with management response with regard to recommendation number 7; however management has not addressed the issue of specific IT training related to Incident Response handling. This recommendation will remain open.

06. HSPD-12

Condition:

It was revealed that the FMC has not implemented the Homeland Security Presidential Directive (HSPD)-12 requirements across the agency. The FMC has provided agency employees (excluding contractors) with the PIV card but has not fully implemented all requirements.

Criteria:

NIST 800-116 Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS) section 2.2 states "HSPD-12 mandates the establishment of a government-wide standard for identity credentials to improve physical security in federally-controlled facilities. To that end, HSPD-12 requires all government employees and contractors be issued a new identity credential based on the FIPS 201 on PIV. Following FIPS 201, this credential is referred to herein as a PIV Card." This section also states: "Recommendation: The OMB Memorandum [M-08-01] requires that the credential issuance be accomplished by October 27, 2008 (or by the date specified in the implementation plan mutually agreed-upon by the agency and OMB). Agency implementation plans should be written to accomplish the goals of HSPD-12.

"HSPD-12 explicitly requires the use of PIV Cards "in gaining physical access to federally controlled facilities and logical access to federally controlled information systems." [HSPD-12] The PIV Card employs microprocessor-based smart card technology, and is designed to be counterfeit-resistant, tamper-resistant, and interoperable across Federal government facilities. Additionally, the FIPS 201 standards suite defines the authentication mechanisms as transactions between a PIV Card and a relying party. FIPS 201 does not, however, elaborate on the uses and applications of the PIV Card. This document provides guidelines on the uses of PIV Cards with Physical Access Control Systems (PACS)."

Cause:

A lack of personnel and/or the budget to provide for agency-wide implementation of the HSPD-12 requirements.

Risk:

The HSPD-12 requirements ensure that authentication is stronger, thus decreasing unauthorized access into the network. Without implementation of the HSPD-12, the FMC deploys two-factor authentication only and is not complemented by the PIV cards. This increases the risk of unauthorized access to data and systems.

Recommendation(s):

8. Implement HSPD-12 requirements in accordance with laws and regulations. *(The OIG estimates the required level of effort for this recommendation to be 40 hours.)*

Management Response:

FMC has begun the process of implementing HSPD-12 logical access. FMC has purchased and received 260 SCR331 USB Smart Card Readers along with the Windows Active Client software and user licenses. FMC's OIT department has created an Active Directory Group Policy Object that requires smart card login. Through the testing phase, FMC has encountered several limitations and is requesting further guidance from OMB. These limitations include BlackBerry access, telework access technology and costs, and procedures for lost or stolen PIV cards. FMC has not been issuing PIV ID cards in-house due to costs and limited personnel, which limits the ability to create new, temporary or replacement cards for employees. FMC has reached out to the Federal CIO council for further guidance and was informed that as of yet, there are no Federal agencies that were successful in fully implementing HSPD-12 due to the same issues experienced by FMC. If these issues, which appear to be affecting all agencies, are resolved, FMC anticipates implementation of the logical access portion of HSPD-12 during the 4th quarter of FY12.

OIG Comments to Management Response:

OIG will retest this issue in the next FISMA cycle, as management plans to implement the OIG recommendation in FY 2012.

07. Privacy

Condition:

Through inquiry with and information provided to us by various agency personnel, we learned that the agency is not identifying:

- Systems with Personally Identifiable Information (PII) and Information in Identifiable Form (IIF).
- Systems in need a Privacy Impact Assessment (PIA).
- Which PIAs need to be posted on the FMC website?
- Information that needs to be redacted prior to posting of the PIA on the FMC website.

We found that three PIAs were required on the agency's major applications: GSS network, FMC Database (FMCDB), and SERVCON. Only the GSS Network and SERVCON had PIAs, however they are outdated. The FMCDB does not currently have a PIA. There are no PIAs posted on the FMC website.

Criteria:

Personally Identifiable Information (PII) can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific

individual, such as date and place of birth, mother's maiden name, etc. (OMB Memorandum 07-16).

To distinguish an individual is to identify an individual's **(NIST 800-122 section 2.1).**

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as Social Security Number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number
- Address information, such as street address or email address
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
- Telephone numbers, including mobile, business, and personal numbers
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scans, voice signature, facial geometry)
- Information identifying personally owned property, such as vehicle registration or identification number, and title numbers and related information
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, or employment, medical, education, or financial information).

The E-Government Act requires PIAs to be performed and updated as necessary where a system change creates new privacy risks. For example:

- Conversions - when converting paper-based records to electronic systems;
- Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;
- Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:
- Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:
- New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
- Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);
- Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:

- Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)

OMB Memorandum 03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, section II.B.2, states that:

> "The confidentiality of PII should be protected based on its risk level. This section outlines factors for determining the PII confidentiality impact level for a particular instance of PII, which is distinct from the confidentiality impact level described in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems. The PII confidentiality impact level takes into account additional PII considerations and should be used to determine if additional protections should be implemented. The PII confidentiality impact level—low, moderate, or high—indicates the potential harm that could result to the subject individuals and/or the organization if the PII were inappropriately accessed, used, or disclosed. Once the PII confidentiality impact level is selected, it should be used to supplement the provisional confidentiality impact level, which is determined from information and system categorization processes outlined in FIPS 199 and NIST Special Publication (SP) 800-60, Volumes 1 and 2: Guide for Mapping Types of Information and Information Systems to Security Categories."

Cause:

This is the result of there being a lack of personnel to prepare and manage the privacy requirements, and a lack of clear understanding of when a PIA is required.

Recommendation:

9. A system inventory should be maintained and from this listing, the following should be performed:

    - Identify which of those systems have PII and IIF. The estimated level of effort for this recommendation is 4 hours.
    - Identify which of those systems need a PIA. The estimated level of effort for this recommendation is 2 hours.
    - Identify which of those PIAs need to be posted on the FMC website. The estimated level of effort for this recommendation is 1 hour.
    - Identify information that needs to be redacted prior to posting of the PIA on the FMC website. The estimated level of effort for this recommendation is 4 hours.

Management Response:

FMC concurs with the findings of the Office of the Inspector General and will employ the recommendations above by the 3rd quarter of FY12.

OIG Comments to Management Response:

OIG has reviewed management response and will be tested in the next FISMA cycle.

08. Access Rights

Condition:

We reviewed the complexity settings (e.g. date of last logon) of the FMC servers as well as inquired with various IT personnel. The following was noted:

- There are no reviews of user access to ensure that those users who are terminated, transferred, or promoted have their access rights reviewed and updated accordingly.
- Six users that are external to the agency have access to FMC data and their activity has not been reviewed.
    - Three of the six users have not logged on since 2008 and their access was not deactivated.
    - One of the six has not logged in for more than six months and also has not been deactivated.
    - Two users have logged on within three months.

Criteria:

FMC Inactive Account Policy OIT-P04 states the following:

Section 1 states "Purpose. The purpose of this policy is to ensure that user accounts exist only for authorized users and FMC OIT staff is required to regularly identify, disable, and purge inactive accounts in a timely and coordinated manner."

Section 5 states "Policy. a. On a monthly basis, the OIT Network Engineer (NE) will identify and immediately disable inactive Windows LAN accounts."

Section 6 states "Responsibilities. a. OIT. OIT is responsible for: (i) Disabling inactive accounts, (ii) Distributing information received regarding inactive accounts to the OIT Network Engineer, (iii) Providing an email to office/bureau heads, COTRs, and the CIO identifying disabled accounts with necessary next steps."

NIST 800-53 Recommended Security Controls for Federal Information Systems and Organizations page F-4 (AC-2) states "The information system automatically disables inactive accounts after [Assignment: organization-defined time period]. (4) The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals. (5) The organization: (a) Requires that users log out when [Assignment: organization defined time-period of expected inactivity and/or description of when to log out]."

Cause:

Check out processes weaknesses and lax monitoring procedures regarding account changes needed for those employees changing positions.

Risk:

Without appropriate reviews of the user access rights, users will inadvertently possess rights that exceed their authorizations. This creates a situation whereby exploitation can occur. Furthermore, if a user has not logged on after a period of inactivity and still has an active account, this can also be used for exploitation by another user.

Recommendation(s):

10. Ensure that IT incorporates the agency's checkout process for terminated employees into its access procedures and updates access permissions for those employees who are promoted or move (i.e., change assignments) within the agency. This will ensure that IT changes the user access settings appropriately. IT should also review access rights on a quarterly basis and work with other Commission bureaus and offices to identify and assess non-FMC personnel access needs for other users such as those users that are external to the agency. (*The estimated level of effort for this recommendation is 3 hours every time a person's position has changed, e.g. terminated, promoted, etc.).*

Management Response:

FMC currently employs a checkout procedure for terminated employees. FMC will implement a quarterly access rights review for all internal and external accounts, which access the FMC network. FMC will implement an employee access rights review anytime an employee is promoted, transferred, or terminated. Further, the user accounts, which are external to the agency, identified during the audit have since been deactivated.

OIG Comments to Management Response:

OIG has not reviewed subsequent actions to ascertain if this finding has been resolved. This will be tested in the next FISMA cycle.

09. Security Awareness

Condition:

Review of the security awareness training records we identified eight of approximately 120 staff (7 percent) employees that have not taken the required Security Awareness Training. Further, the agency is not enforcing its recently issued Management Directive requiring loss of network privileges when training isn't taken.

Criteria:

FMC Management Directive 2011-4 IT Security for Personnel, section 5 states "If an employee or contractor does not take the required training within the requested timeframe, upon their next login to 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." Also stated was "Each employee and contractor shall receive a mandatory annual cyber security awareness briefing, which may be delivered in an auditorium lecture, videotape, or CBT format."

NIST 800-50 Building an Information Technology Security Awareness and Training Program page ES-3 states "Federal agencies and organizations cannot protect the confidentiality, integrity, and availability of information in today's highly networked systems environment without ensuring that all people involved in using and managing IT:

- Understand their roles and responsibilities related to the organizational mission;
- Understand the organization's IT security policy, procedures, and practices; and
- Have at least adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible.

In the IT community, it is generally understood by the IT security professional community that people are one of the weakest links in attempts to secure systems and networks. The "people factor" - not technology - is key to providing an adequate and appropriate level of security. If people are the key, but are also a weak link, more and better attention must be paid to this "asset." A robust and enterprise wide awareness and training program is paramount to ensuring that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them."

Cause:

The cause is primarily a lack of importance perceived by agency personnel and management support. Security Awareness training must be perceived as important and mandatory. Training must not be perceived as an option.

Risk:

Without appropriate security awareness training, employees may conduct agency business in ways that are not conducive to best security practices. This could result in lost or shared passwords or other vulnerabilities. Personnel need to be made aware of their responsibilities with government data and the impact on the agency as a whole if data is compromised.

Recommendation(s):

11. Ensure that all agency personnel take Security Awareness Training every year in accordance with NIST 800-50 and comply with IT Security for Personnel MD 2011-4. (*The OIG estimates the level of effort to implement this recommendation at 10 hours to*

update the Security Awareness training each year and 2 hours for each employee to take the training).

Management Response:

All Commission personnel have taken Security Awareness Training this year, and will be required to continue to do so in the future, in accordance with FMC Management Directive 2011-4 IT Security for Personnel.

OIG Comments to Management Response:

The OIG has obtained evidence that indicated that the remaining personnel have now taken the security awareness training. This issue is considered closed.

10. Password Complexity Settings

Condition:

We reviewed various password complexity settings on servers supporting the FMC applications and noted the following:

- Password complexity was set to "disabled" and not set for agency users. This means that agency users are not required to have passwords that meet complexity requirements such as alpha-numeric, special character, maximum length and password reuse.

Criteria:

FMC Password Policy OIT-P01 states the following:

Section 1, Purpose, states "The purpose of this policy is to establish a standard for creating strong passwords, protecting passwords and frequently changing passwords."

Section 2 states "This policy applies to all FMC Systems and Applications and includes all FMC employees, contractors, and others who are responsible for an account on an FMC system or network."

Section 5, Policy, states:

a. All user-level passwords (e.g. email, desktop, etc.) must be changed at least every 90 days.
b. All user passwords must be changed anytime a system or application manager leaves the FMC or has a change in duties where privileged access is no longer needed.
c. Passwords should be communicated to intended recipients in a secure manner.
d. The administrator will assign a temporary password at account creation or when staff computer upgrades occur. Forced change will occur at first login.

e. All passwords will be stored in a secured manner.
f. Batch jobs and scripts must not store/contain passwords in plain text.
g. All accounts will lock after 4 consecutive failed login attempts.
h. Remote access into the FMC infrastructure must occur in a secure manner and in accordance with the OIT Policy on Remote Access.
i. When placing systems in production, default passwords must be changed during installation and prior to system certification. This includes hardware devices and software applications.
j. All user-level and system-level passwords must conform to the strong password described in the definitions section.
k. FMC users should not use the same password for FMC accounts as for other non-FMC accounts."

NIST 800-123 Guide to General Server Security, section 4.2.2 states "Check the Organization's Password Policy—Set account passwords appropriately. Elements that may be addressed in a password policy include the following:

– Length—a minimum length for passwords.

– Complexity—the mix of characters required. An example is requiring passwords to contain uppercase letters, lowercase letters, and non-alphabetic characters, and to not contain "dictionary" words.

– Aging—how long a password may remain unchanged. Many policies require users and administrators to change their passwords periodically. In such cases, the frequency should be determined by the enforced length and complexity of the password, the sensitivity of the information protected, and the exposure level of passwords. If aging is required, consideration should be given to enforcing a minimum aging duration to prevent users from rapidly cycling through password changes to clear out their password history and bypass reuse restrictions.

– Reuse—whether a password may be reused. Some users try to defeat a password aging requirement by changing the password to one they have used previously. If reuse is prohibited by policy, it is beneficial, if possible, to ensure that users cannot change their passwords by merely appending characters to the beginning or end of their original passwords (e.g., original password was "mysecret" that is changed to "1mysecret" or "mysecret1").

Cause:

A lack of personnel, budget, or time constraints to adequately review and implement appropriate password complexity.

Risk:

Without appropriate password complexity settings (especially for IT related personnel), users will have authentication credentials that are weak and susceptible to exploitation. Weak authentication for the IT personnel will raise the risk of spoofing a user (pretending to be someone else) and access gained can be used for adverse actions.

Recommendation(s):

12. Ensure that password complexity is set to "enabled" and applies to all personnel within the FMC agency. *(The OIG estimates the level of effort for this recommendation at 4 hours.)*

Management Response:

Finding #10 is acknowledged by the FMC. FMC realizes that by requiring complex password usage overall network security is enhanced. Currently FMC's network requires a 6 character password. FMC is currently in the process of implementing the HSPD-12 PIV two-factor authentication requirements at which point the password complexity requirement will become irrelevant. FMC is aware of the risk associated with not requiring complex passwords.

OIG Comments to Management Response:

The OIG notes that the FMC has implemented a password length requirement that is below industry and NIST-recommended standards. While the implementation of HSPD-12 will make the issue moot, the OIG believes, based on discussions with staff, that the implementation is not imminent. Substantial delays often accompany major migration and changes. Management, although not explicitly stated, also is concerned with the impact on staff having to remember longer, potentially more complex passwords. In a prior recommendation response, management stated that it plans to implement major portions of HSPD-12 by September 30, 2012. The OIG continues to believe that the agency should require all network users to have passwords that meet complexity requirements such as alpha-numeric, special character, maximum length and password reuse, until HSPD requirements are implemented.

11. Certification and Accreditation

Condition:

Obtained the latest Certification and Accreditation (C&A) packages for the General Support Systems (GSS) and Major Applications (MA) and noted the following:

1. The Network GSS C&A and the SERVCON C&A were not signed or finalized.
2. The Network GSS and SERVCON System Security Plans (SSP) were not signed or finalized.
3. The SERVCON FIPS-199 Security Categorization resulted in a "High" categorization and should have been a "Moderate" categorization.
4. The implementation status was not identified correctly. For example, Risk Assessment (RA) RA-5 states that scans are conducted, while inquiry revealed that scans were not conducted.
5. The Network GSS C&A package also included a Security Test and Evaluations (STE). The STE results identified vulnerabilities, however there was no evidence that they were remediated or corrected. The SERVCON STE had no results at all leading the OIG to conclude that tests were not performed.
6. The Network GSS contained control implementation documentation for the FMCDB system. The FMCDB should be a separate C&A package.
7. The SERVCON system meets the requirements for an e-Authentication assessment. However, this assessment was not completed for the SERVCON system.

Criteria:

NIST FIPS-199 Standards for Security Categorization of Federal Information Systems 3.0 states "The potential impact is HIGH if—

− The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals."

NIST 800-37 Guide to Applying the Risk Management Framework to Federal Information Systems section 2.1 states "Assess the security controls using appropriate assessment procedures 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.

NIST 800-37 Guide to Applying the Risk Management Framework to Federal Information Systems section 2.1 states "Authorize information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable."

NIST 800-37 Guide to Applying the Risk Management Framework to Federal Information Systems section 2.3.1 states "In addition to consideration of direct management control, it may also be helpful for organizations to determine if the information resources being identified as an information system:

• Support the same mission/business objectives or functions and essentially the same operating characteristics and information security requirements; and

• Reside in the same general operating environment (or in the case of a distributed information system, reside in various locations with similar operating environments)."

NIST 800-18 Guide for Developing Security Plans for Federal Information Systems section 3.16 states "Once the information system security plan is developed, it is important to periodically assess the plan, review any change in system status, functionality, design, etc., and ensure that the plan continues to reflect the correct information about the system. This documentation and its correctness are critical for system certification activity. All plans should be reviewed and updated, if appropriate, at least annually."

According to **OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies**, e-authentication is defined as the process of establishing confidence in user identities electronically presented to an information system. OMB M-04-04 states that e-authentication "applies to all [Federal Electronic] transactions for which authentication is required, regardless of the constituency (e.g. individual user, business, or government entity)." OMB guidance provides assistance to federal agencies in determining the appropriate level of assurance for electronic transactions requiring authentication by establishing and describing four levels of identity assurance, as well as providing strategies for determining which of these levels is appropriate for the information system.

In accordance with OMB M-04-04, all federal agencies must conduct an e-authentication risk assessment on those systems that remotely authenticate users over a network for purposes of e-government and commerce to determine the required level of authentication assurance for the information system. As later clarified in OMB M-08-21, FY 2008 Reporting Instructions for FISMA and Privacy Data, an e-authentication application is an application that meets the following criteria:

- Is web-based;
- Requires authentication; and
- Extends beyond the borders of your enterprise (e.g. multi-agency, government-wide, or public facing)

If all three of these criteria are met, an e-authentication Risk Assessment is required. If any of the above criteria are not met, then an e-authentication Risk Assessment is not required.

Cause:

Agency does not have the budget or personnel resources.

Risk:

Without properly prepared C&A packages, systems will be categorized incorrectly, and the wrong controls will be selected for testing. Furthermore, documents will not be reviewed and updated as technologies and risks change. These will result in a weaker security posture for the agency as a whole and could ultimately lead to exploitation of weaknesses.

Recommendation(s):

13. The Network GSS C&A and the SERVCON C&A should be signed and finalized. *(The OIG estimates the level of effort for this recommendation at 4 hours.)*
14. The Network GSS and SERVCON System Security Plans (SSP) should be signed and finalized. *(The OIG estimates the level of effort for this recommendation at 4 hours.)*
15. The SERVCON FIPS-199 Security Categorization should be a "Moderate" categorization. *(The OIG estimates the level of effort for this recommendation at 4 hours.)*
16. All controls in the SSPs should be reviewed to ensure their implementation status is correct. The estimated level of effort for this recommendation is 40 hours.
17. Any weaknesses as a result of STEs should be corrected immediately. *(The OIG estimates the level of effort for this recommendation at 20 hours.)*
18. The FMCDB should be carved out into a separate C&A package. *(The OIG estimates the level of effort for this recommendation at 40 hours.)*
19. The SERVCON system should have an e-Authentication assessment conducted. *(The OIG estimates the level of effort for this recommendation at 2 hours.)*

Management Response:

FMC concurs with the findings of the Office of the Inspector General. FMC has remedied recommendations 13 through 16. FMC is in the process of remedying recommendations 17 through 19 and anticipates completion by the 4th quarter of FY 12.

OIG Comments to Management Response:

OIG accepts that recommendation number 15 is closed. The OIG has not received any documentation to review and test the remaining recommendation responses. This will be tested in the next FISMA cycle.

12. Memorandums of Understanding (MOU)

Condition:

The FMC has external users from four different agencies that have access to one of its systems. Of those four agencies, two of them do not have MOUs between the external agency and FMC describing the various security requirements when accessing FMC data.

Criteria:

NIST 800-47 Security Guide for Interconnecting Information Technology Systems, section 3.5 states "Document Interconnection Agreement - document an agreement governing the interconnection and the terms under which the organizations will abide by the agreement, based on the team's review of all relevant technical, security, and administrative issues (Section 3.4 above). Two documents may be developed: an Interconnection Security Agreement (ISA) and an MOU/A."

Cause:

The cause is primarily because of lack of personnel or time constraints to adequately review MOUs and external agency needs in relation to that of the FMC.

Risk:

Without an MOU between FMC and other agencies where personnel access FMC data, the entry points into the FMC network may be exposed to weaker controls than that set by the FMC, resulting in possible exploitation of data. It is very important for the FMC to require external agencies to adhere to the same or stronger security controls when accessing FMC data from an external source.

Recommendation(s):

20. Develop an MOU for all agencies where external personnel access the FMC data.

Management Response:

Management recognizes that the MOUs need updating and will work with other agencies as needed to effect that. Primarily, updating will reflect the changes made by DOD with respect to which commands need access. Originally, MSC performed that function but it was transferred to Military Traffic Management Command (MTMC), with whom the Commission has an MOU. Subsequently, that function was transferred to U.S. Transportation Command (TRANSCOM), which subsumed the responsibilities of MTMC. Accordingly, the MOU needs updating to reflect that TRANSCOM is the agency with access to the Commission's system. Anticipated completion 2nd quarter of FY12.

OIG Comments to Management Response:

FMC will test this in the next FISMA cycle.

PRIOR YEAR FINDINGS

#	POA&M	Notes	Open / Closed
1	Formally document plans for Form-1 and Form-18 system replacements that includes, but is not limited to, explicit migration milestones and timeliness.	Evidence was obtained in the current FISMA testing that closes this finding.	Closed
2	Clearly identify the Certifying Agency, Designated Approving Authority, and system owner in the security plans and C&A documentation in accordance with NIST SP 800-37 as amended.	This was closed prior to the FISMA 2011 testing.	Closed
3	Conduct complete risk assessments on accredited FMC systems (FMC Network and SERVCON). Define accreditation boundaries. Ensure risk assessments are complete in accordance with NIST SP 800-30 as amended.	This was rolled up to FY2011 Finding #11	Open
4	Conduct control assessments in accordance with FIPS 200, NIST SP 800-53 as amended, and NIST SP 800-37 as amended.	This was rolled up to FY2011 Finding #11	Open
5	Complete the Authority to Operate letters with the correct information and titles.	This was rolled up to FY2011 Finding #11	Open
6	Correct the e-authentication risk assessment for SERVCON. SERVCON requires Level 4 authentication.	This was rolled up to FY2011 Finding #11	Open
7	As recommended in FY09, develop a POA&M process for systems that will be retained complete the POA&Ms in accordance with current OMB and NIST guidance, and maintain evidence of the closure of each item.	This year's FISMA report will be used as the final listing of outstanding POA&Ms.	Closed
8	Review and implement FMC's policies and procedures (and, if determined necessary, hardware and/or software) for the ISSO to monitor the actions of all FMC Network user, and privileged (super user) accounts such as the top tier Domain Administrator Account and the administrator accounts under the Domain Administrator Group.	This was rolled up to FY2011 Finding #8	Open
9	The FMC Network Domain Administrator user account should be changed in accordance with FMC password policy, and physically secured to restrict its access. The CIO or his designated representative should control the access and use of the password so that this password is only made available for authorized and documented network changes and/or emergencies. This would ensure accountability and avoid any potential for a single point of	This was rolled up to FY2011 Finding #8	Open

#	POA&M	Notes	Open / Closed
	failure. The process for handling the FMC Domain Administrator account should be documented.		
10	If regular Domain Administrator Account use is deemed necessary without employing the recommended procedures or other means that effectively enforces user accountability, FMC should: a. Document the reason for this need. b. Perform a risk assessment in accordance with NIST SP 800-30 to determine the level of risk associated with this practice. c. Develop a stand-a-alone document, or update the FMC LAN system security plan to reflect the acceptance of risk. d. The designated approval authority for the FMC LAN should accept responsibility for the risk associated with this practice in writing.	This was rolled up to FY2011 Finding #8	Open
11	Develop a contingency plan policy and procedures that address the creation, review, testing, and maintenance of contingency plans. Test contingency plans and document results in accordance with NIST SP 800-34 and NIST SP 800-53.	This was rolled up to FY2011 Finding #4	Open
12	Complete and maintain an official system inventory of all FMC systems and interfaces.	An inventory of systems are maintained and contain the necessary requirements.	Closed during the FY 2011 FISMA engagement
13	Organize the FMC inventory in a hierarchal fashion (i.e., which systems are subordinate to the GSS).	This was closed prior to the FISMA 2011 testing.	Closed
14	Define and document policies and procedures for an oversight methodology of external information system services with contractors. At the defined frequency for this process (at least once a year), FMC should meet with the contractor and, if necessary, create findings on the POA&M. A document/memo should be created each time that oversight is performed.	The FMC has numerous policies concerning system services and contractors.	Closed during the FY 2011 FISMA engagement
15	Monitor security control compliance by external service providers and maintain an inventory of the following items:	Access to the FMC data from external agencies is via the Internet with authentication	Closed

#	POA&M	Notes	Open / Closed
	* the number of contractor systems that service FMC by FIPS 199 category. * The number of contractor systems that service FMC by C&A status. * The number contractor systems that service FMC by whether annual testing occurred. * The number of contractor systems that service FMC by whether a tested contingency plan exits. * The number of agency-owned and contractor systems that service FMC assessed at e-authentication levels 3 or 4.	credentials.	
16	Maintain Authority to Operate (ATO) letters, Interconnection Security Agreements (ISA), and Memorandum of Understanding (MOU) between FMC and external service providers.	This was rolled up to FY2011 Finding #12	Open
17	Complete the SERVCON and GSS configuration management documentation to include the sections missing, as identified in the condition section, above. Additionally, confirm that the SERVCON and future configuration management plans address the following sections, in accordance with NIST SP 800-53 Revision 3: - security control, port and firewall settings. - allowable and non-allowable services. - hardware and software requirements. - patches and service packs. - establish system and application baselines and document the. deviations from the baselines.	Configuration Management and other related documentation now exists for the FMC systems.	Closed during the FY 2011 FISMA engagement
18	Implement the NIST National Checklist Program for FMC services and utilize a Security Content Automation Protocol (SCAP) scanner to verify NIST baseline security configurations for servers. Additionally, document any deviations from the baseline security configurations along with the reasons.	This was rolled up to FY2011 Finding #1	Open
19	A11-01A (1) - Develop and implement policies and procedures to require privacy impact assessments (PIA) to be completed for	This was rolled up to FY2011 Finding #7	Open

#	POA&M	Notes	Open / Closed
	each applicable information system.		
20	A11-01A (2) Remove the FMC-18 (Form-18 PIA from the publicly accessible web that incorrectly states, "A risk Assessment has been conducted and the appropriate controls have been implemented" as no authorization (formerly C&A) package was created for this system.	This was closed prior to the FISMA 2011 testing.	Closed
21	A11-01A (3) - Create a planning document for multifactor authentication that correlates with the IT capital planning and investment control process. Utilized multifactor authentication for remote authentication FMC systems to authenticate users' identities for Level 3 and Level 4 users in accordance with NIST 800-63.	This was rolled up to FY2011 Finding #6	Open
22	A11-01A (4) - Create policies and/or procedures to log, verify and reassess data extracts from database holding sensitive information after 90 days.	Policies are now in place that addresses this POA&M.	Closed
23	Evaluate FMC mobile needs and implement FIPS 140-2 encryption on mobile computers and portable devices carrying agency data.	This still remains open.	Open