Office of Inspector General

Evaluation of the FMC's Compliance with the Federal Information Security Management Act FY 2015

A16-02

November 2015

FEDERAL MARITIME COMMISSION

FEDERAL MARITIME COMMISSION
Washington, DC 20573

November 12, 2015

Office of Inspector General

Dear Chairman Cordero and Commissioners:

I am pleased to provide the attached Office of Inspector General (OIG) report on the status of information security at the Federal Maritime Commission (FMC) for fiscal year (FY) 2015. The OIG relied on the expertise of an information security evaluator from *Your Internal Controls LLC*, for assistance on this mandated review.

The objectives of this independent evaluation of the FMC's information security program were to evaluate its security posture by assessing compliance with the Federal Information Security Management Act (FISMA), as amended, and related information security policies, procedures, standards, and guidelines. The scope of this evaluation focused on the FMC General Support Systems (GSS) and Major Applications.

The agency continues to make progress addressing outstanding deficiencies from prior year FISMA evaluations. Specifically, five of the eight outstanding recommendations reported in last year's FISMA report have been implemented by the agency. This year's report includes six new recommendations to address five findings.

The OIG would like to thank FMC staff; especially the Office of Information Technology (OIT), for their assistance in helping the OIG meet our evaluation objectives. If you have any questions, please contact me at (202) 523-5863 or jhatfield@fmc.gov.

Respectfully submitted,

Jon Hatfield
Inspector General

Attachment

cc:	Office of the Managing Director
	Office of the General Counsel
	Office of Information Technology

FEDERAL MARITIME COMMISSION

OFFICE OF INSPECTOR GENERAL

Evaluation of the FMC's Compliance with the Federal Information Security Management Act FY 2015

TABLE OF CONTENTS

PURPOSE

Your Internal Controls (contractor), on behalf of the Federal Maritime Commission (FMC), Office of Inspector General (OIG), conducted an independent evaluation of the quality and compliance of the FMC's 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), as amended. This report was prepared by the contractor with guidance by the Office of Inspector General.

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). FISMA 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 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. We conducted our testing through inquiry of FMC personnel, observation of activities, inspection of relevant documentation, and the performance of technical security testing. More specifically, our testing covered a sample of controls as listed in NIST 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Revision 4. For example, testing covered system security plans, access controls, risk assessments, personnel security, contingency planning, identification / authentication and auditing. Our testing was for the period October 1, 2014 through September 30, 2015 (fiscal year 2015).

NIST 800-53, Rev. 4[1], has several families and controls within those families. The number of controls will vary depending on the categorization of the respective system (e.g. Low, Moderate, and High), as well as the control enhancements. For purposes of this FISMA engagement, the scope of our testing included the following controls:

Family	Controls
Risk Assessment (RA)	RA-5
Planning (PL)	PL-2, PL-4
System and Services Acquisition (SA)	SA-4, SA-9
Security Assessment and Authorization (CA)	CA-2, CA-3, CA-7, CA-8
Personnel Security (PS)	PS-4, PS-5, PS-7
Contingency Planning (CP)	CP-2, CP-3, CP-4, CP-6
Configuration Management (CM)	CM-3
Maintenance (MA)	MA-2
System and Information Integrity (SI)	SI-3, SI-5
Incident Response (IR)	IR-2, IR-3, IR-6
Awareness and Training (AT)	AT-2, AT-3
Identification and Authentication (IA)	IA-4
Access Control (AC)	AC-2, AC-7, AC-11, AC-21, AC-22
Audit and Accountability (AU)	AU-2, AU-3, AU-4

[1] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

CURRENT YEAR FINDINGS

01 Timely Remediation of Vulnerabilities

The agency's Office of Information Technology (OIT) is responsible for performing scans of the agency's information systems to identify and remediate vulnerabilities. Vulnerability scanning includes, for example: (i) scanning for missing and/or out of date patches; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Remediation is the correction of a vulnerability or eliminating a threat.

Condition:
We reviewed two vulnerability scan results over a two week period to assess the timely remediation of any high and medium vulnerabilities. Although there were no patch vulnerabilities noted from the reports, the following was the result of that review:

Week 1
High vulnerability – 1
Medium vulnerabilities – 15

Week 2
High vulnerability – 1
Medium vulnerabilities – 14

The high vulnerability from week 1 was the same vulnerability on the scan from week 2. With regard to the medium vulnerabilities, 14 of the 15 from week 1 to week 2 were the same. There was 1 medium vulnerability from week 1 that was remediated within the week timeframe.

Based on the above evaluation results, the same high and medium vulnerabilities from week 1 had not been remediated in the following week. Therefore, the high and medium vulnerabilities are not being remediated in a timely manner in order to protect the agency from known or unforeseen exposures and exploitation.

Criteria:
NIST 800-53, Revision 4, Risk Assessment (RA)-5 states:
According to NIST, the organization "remediates legitimate vulnerabilities in accordance with an organizational assessment of risk."

Cause:
The cause is primarily because of a lack of personnel, budget, or time constraints to adequately document and/or assess all of the controls in NIST 800-53, Revision 4.

Risk:
By having high and medium vulnerabilities exposed to the agency, and not remediated in a timely manner, there is the risk that adversaries can take advantage of those weaknesses and gain access to FMC's data, which ultimately may lead to a lack of integrity and/or confidentiality for the agency.

Recommendation(s):

1. All vulnerabilities should be reviewed in terms of their risk classification (e.g. high, medium, and low). Furthermore, the Office of Information Technology should establish a formalized policy for how timely deficiencies (high, medium, and low) need to be remediated. Best practices across other agencies remediate high vulnerabilities within 1 business day and medium vulnerabilities within 3-5 business days, therefore, FMC should follow best practices.

Management Response:

Management agrees that all vulnerabilities should be reviewed in terms of their risk classification and remediated accordingly. OIT will establish a policy that details an appropriate agency-specific timeline in which high and medium vulnerabilities will be remediated. It is anticipated that this finding will be remediated by the 3rd quarter of FY 2016.

02 Personnel Termination

The NIST guidance on personnel security addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements. One of the key controls is to disable information system access within an organization-defined time period upon employees' separation from the agency.

Condition:
Upon review of the users that separated from the agency during the period under review, the agency could not determine that users' access was disabled in a timely manner.

Criteria:
NIST 800-53, Revision 4, Personnel Security (PS)-4 states:
"The organization, upon termination of individual employment:

a. Disables information system access within an organization-defined time period."

Cause:
The cause is primarily because of a lack of personnel, budget, or time constraints to adequately document and/or assess all of the controls in NIST 800-53, Revision 4.

Risk:
If an agency has terminated users without having disabled their access in a timely manner, there is the risk that those users' accounts can be used for exploitation and adversarial actions against the agency.

Recommendation(s):

2. OIT should establish a formalized policy for how timely separated users' access is disabled once they have left the agency. Best practices across other agencies disable separated users within 5 business days, therefore, FMC should follow best practices.

Management Response:
Management agrees with the recommendation. OIT will establish an appropriate agency-specific policy which details the timeline for separated users' access to be disabled and to provide for the manner in which evidence of this process is captured for audit purposes. It is anticipated that OIT will develop and implement this policy during the 2nd quarter of FY 2016.

03 Configuration Management Plan

NIST guidance provides for the establishment of a configuration management plan (CMP). The CMP for the agency's information system accomplishes the following:

a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration items;
c. Defines the configuration items for the information system and places the configuration items under configuration management; and
d. Protects the configuration management plan from unauthorized disclosure and modification.

For example, a CMP describes the frequency and how to update configuration settings for the information systems.

Condition:
It was revealed that the FMC has a CMP that is not finalized. The CMP is used for documenting the types of changes being made to the agency's systems, as well as the configuration items.

Criteria:
<u>NIST 800-53, Revision 4, Configuration Management (CM)-9 states:</u>
"The organization develops, documents, and implements a configuration management plan for the information system."

Cause:
The cause is primarily because of a lack of personnel, budget, or time constraints to adequately document and/or assess all of the controls in NIST 800-53, Revision 4.

Risk:
Without an agency CMP, there is the risk that changes will not be made to agency systems properly, in a timely manner, and without following approved procedures. These include ensuring that changes are reviewed, tested, and approved prior to migrating from development/test to production.

Recommendation(s):

3. The Configuration Management Plan should be finalized and approved, and include the types of changes as well as a list of configuration items.

Management Response:
Management agrees with the recommendation. It is anticipated that the OIT Configuration Management Plan will be finalized and approved within OIT in the 2nd quarter of FY 2016.

04 Incident Response Training and Testing

Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or real-life simulations of known incidents. An example of an incident may be an inadvertent download of software or malware, which is subsequently introduced to the agency's network. This type of incident may not require the deployment of contingency procedures, however, it may require incident response procedures to deal with the effects of any exploitation that may occur as a result of the incident.

Condition:
Upon review of the incident response environment, the following was noted:

- There is no testing of the current incident response environment.
- There is also no training provided to the IT staff with respect to preparing for and managing incidents.

Criteria:
NIST 800-53, Revision 4, Incident Response (IR)-2, training, states:
"The organization provides incident response training to information system users consistent with assigned roles and responsibilities."

The above criteria has been deemed to include all personnel and their respective roles and responsibilities. For example, this includes IT personnel needing specific incident response training relevant to their job functions.

NIST 800-53, Revision 4, Incident Response (IR)-3, testing, states:
"The organization tests the incident response capability for the information system to determine the incident response effectiveness and documents the results."

Cause:
The cause is primarily because of a lack of personnel, budget, or time constraints to adequately document and/or assess all of the controls in NIST 800-53, Revision 4.

Risk:
Without formalized and yearly testing and training of incident response, there is the risk that when an incident occurs, the agency response will be ineffective. This may also lead to an untimely remediation of the incident thereby affecting agency data and systems. In addition, there is the risk that the OIT and other staff members will be unprepared when an incident actually does occur.

Recommendation(s):

4. Incident response prevention, detection and correction should be tested on an annual basis. Furthermore, the OIT staff members should receive incident response training on an annual basis.

Management Response:
Management agrees with the recommendation. OIT will conduct an annual incident response exercise in which OIT staff and members of the Agency Response Team (A.R.T.) will participate.

Additionally, a suitable incident response training platform will be identified for OIT staff's annual training. It is anticipated that this will be completed in the 3rd quarter of FY 2016.

05 Access Authorization Management

Access authorization management applies to the agency's employees and/or individuals deemed to have equivalent status of an employee (e.g., contractor). Management of employees' or equivalent user accounts should involve the receipt, documentation, and periodic updating of the proper authorization from the users' supervisor or other authorized individual.

Condition:
Upon review of a sampled set of users for their access authorizations, the following was noted:

- Access authorizations are not being maintained to ensure that users' rights are commensurate with what was approved.
- There was no evidence to conclude that an annual recertification of users' access rights is being performed.

Criteria:
NIST 800-53, Revision 4, Identification and Authorization (IA)-4 states:
"The organization manages information system identifiers [user accounts] by:
a. Receiving authorization from organization-defined personnel or roles to assign an individual, group, role, or device identifier." In addition, "The organization requires that the registration process to receive an individual identifier [user account] includes supervisor authorization."

NIST 800-53, Revision 4, Access Control (AC)-2 states:
"Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account."

"Authorizes access to the information system based on:
1. A valid access authorization;
2. Intended system usage; and
3. Other attributes as required by the organization or associated missions/business functions."

Further, AC-2 states the organization "Reviews accounts for compliance with account management requirements."

Cause:
The cause is primarily because of a lack of personnel, budget, or time constraints to adequately document and/or assess all of the controls in NIST 800-53, Revision 4.

Risk:
Without maintaining and reviewing users' access rights on an annual basis, there is the risk that users will be authorized in excess of what they were approved for, thereby creating an environment where a user can potentially exploit FMC's systems and data.

Recommendation(s):

5. All users' rights upon initiation should have their access rights reviewed, approved (by the respective employee's immediate supervisor), and maintained for subsequent investigations and/or incident response.

6. On an annual basis, all FMC employees should have their access reviewed (by the respective employee’s immediate supervisor) to ensure it is still commensurate with their job functions.

Management Response:
Management agrees with the recommendation [5]. Currently, all users are initially granted access rights by OIT pursuant to emails from OHR (notifying OIT of the new users' arrival) and from the new employee's supervisor or department head (requesting that the new employee be given specified rights/permissions). OIT will retain these messages. Further, OIT will review the access rights of all FMC users on an annual basis. This review will be documented and maintained as an artifact. It is anticipated that this finding will be remediated in the 2nd quarter of FY 2016.

Management agrees with the recommendation [6]. Supervisors or department heads will be required to review all FMC employees' access rights on an annual basis to ensure that each employee's access remains commensurate with their job functions. This review will be documented and maintained by OIT as an artifact. It is anticipated that this finding will be remediated in the 2nd quarter of FY 2016.

STATUS OF PRIOR YEAR RECOMMENDATIONS

#	POA&M	Report	Open / Closed
1	Review all SSPs and ensure the documentation is clear and addresses each of the controls and all of their respective control objectives.	Report A15-02 (#1)	Closed
2	All controls within NIST 800-53 Revision 4 for the systems' categorization should be used as a starting point for determining the assessments and implementation of a continuous monitoring program. Then, management should determine which of those controls are critical. Those critical controls should be assessed every year. The remainder of the controls should then be divided by three and then assessed over a three-year period, whereby 1/3 of the remaining controls are assessed each year. Ideally, the controls to be assessed each year should then be done on a quarterly basis by taking the annual set of controls and assessing 1/4 each quarter.	Report A15-02 (#2)	Open FMC has developed a comprehensive continuous monitoring program, however this remains open because the plan has not been deployed yet.
3	Ensure all contractors undergo an appropriate investigation or screening prior to being granted access to any data and/or systems. Furthermore, ensure that all contractors undergo appropriate periodic reinvestigations or screening once the initial investigation is deemed to be successful. *[2015 Update: NIST 800-53, Revision 4, provides that individuals should be screened prior to authorizing access to the agency information system. First, Personnel Security (PS)-2 states: "The organization: (a) assigns a risk designation to all organizational positions; (b) establishes screening for individuals filling those positions; and (c) reviews and updates position risk designations. Further, PS-3, Personnel Screening, states: "The organization: (a) screens individuals prior to authorizing access to the information; and (b) rescreens individuals according to organization defined conditions..." NIST 800-53, Revision 4, states that personnel screening and rescreening should be based on applicable federal laws, regulations, Executive Orders, and related guidance.* *Therefore, FMC needs to review Federal requirements, and then adopt an agency appropriate process based on the Federal requirements. Once a process is adopted, the agency should implement the process to close this issue.]*	Report A15-02 (#3)	Open
4	Ensure a sufficient number of certifying officials are properly authorized and trained on the responsibilities associated with monitoring, certifying and documenting the results of employee background investigations, and reinvestigations, when warranted.	Report A15-02 (#4)	Open

#	POA&M	Report	Open / Closed
5	Take appropriate action to restart providing backup tapes to the external contractor and also test those backups by restoring from tape to ensure the data is available when needed.	Report A15-02 (#5)	Closed
6	Evaluate FMC mobile needs and implement FIPS 140-2 encryption on mobile computers and portable devices carrying agency data.	Report A2010-02 (#3)	Closed
7	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.	Report A2012-02 (#5)	Closed
8	Implement HSPD-12 in accordance with laws and regulations.	Report A2012-02 (#8)	Closed