Office of Inspector General

Evaluation of the FMC's Compliance with the Federal Information Security Management Act FY 2016

A17-02

November 2016

FEDERAL MARITIME COMMISSION

FEDERAL MARITIME COMMISSION
Washington, DC 20573

November 8, 2016

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) 2016. 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 improvements on the agency's information technology (IT) security. However, some weaknesses remain. The OIG concluded the FMC has effectively implemented six of the nine outstanding prior year FISMA recommendations. Further, this report contains three recommendations to address three findings; however, two of the three recommendations were implemented by the agency prior to the release of this report.

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

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 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.

FISMA assigns specific responsibilities to agency heads and Inspectors General (IGs). 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, 2015 through September 30, 2016 (fiscal year 2016).

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
Security Assessment and Authorization (CA)	CA-2, CA-7
Personnel Security (PS)	PS-4, PS-5
Physical and Environmental Protection (PE)	PE-2, PE-3, PE-5, PE-6, PE-8, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15
Contingency Planning (CP)	CP-2
Configuration Management (CM)	CM-6, CM-8
Media Protection (MP)	MP-2, MP-5, MP-6
Incident Response (IR)	IR-2, IR-3, IR-4, IR-5, IR-6, IR-8
Awareness and Training (AT)	AT-2, AT-3
Identification and Authentication (IA)	IA-2, IA-5
Access Control (AC)	AC-2, AC-5, AC-7, AC-8, AC-11, AC-17, AC-18
Audit and Accountability (AU)	AU-2, AU-3, AU-4, AU-6
System and Communications Protection (SC)	SC-8
Accountability, Audit and Risk Management (AR)	AR-2

[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 Incident Response Plan

Incident response policies document how, when and who shall respond to respective incidents. Furthermore, managing the incidents should also consider the effects of breaches to Personally Identifiable Information (PII) and whether or not the United States Computer Emergency Readiness Team (US-CERT) should be contacted for consultation and/or communication. As technologies are always changing and new vulnerabilities are introduced, it is imperative that the Incident Response Plan stay current.

Condition:
Upon review of the Incident Response Plan, it was determined that the date of this Plan was from 2011, and there was no evidence of a periodic review and/or update of the plan.

It shall also be noted that this condition has been resolved prior to the close of the fiscal year, but was a weakness for the majority of the FY.

Criteria:
NIST 800-53, Revision 4, Incident Response (IR-8), training, states:
"**NIST SP 800-53 Control:** The organization:

a. Develops an incident response plan that:
    1. Provides the organization with a roadmap for implementing its incident response capability;
    2. Describes the structure and organization of the incident response capability;
    3. Provides a high-level approach for how the incident response capability fits into the overall organization;
    4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
    5. Defines reportable incidents;
    6. Provides metrics for measuring the incident response capability within the organization;
    7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
    8. Is reviewed and approved;
b. Distributes copies of the incident response plan;
c. Reviews the incident response plan [*annually]*;
d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
e. Communicates incident response plan changes; and
f. Protects the incident response plan from unauthorized disclosure and modification."

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 review and potential updates to the Incident Response Plan, it is possible that the agency is exposed to vulnerabilities to which the agency may not be able to respond effectively or in a timely manner.

Recommendation:

1. The Incident Response Plan shall be reviewed annually or whenever there are significant changes to the agency's environment. Based on these reviews, the Incident Response Plan should be updated and communicated to pertinent personnel involved in managing incidents.

Management Response:

Management agrees with this recommendation. The Commission's Incident Response Plan was revised effective September 22, 2016. Going forward, the plan will be reviewed annually or whenever significant changes occur. Management considers this recommendation closed.

02 Security Awareness Training

Security awareness training should be conducted initially (e.g. newly employed), annually and whenever there are significant changes to the agency's network. Security awareness training applies to both employees and contractors, as well as anyone else who may have direct access to the agency's data or systems. The primary intent of performing security awareness training is to ensure that those with access to agency data and systems, will have the knowledge of what are acceptable actions when handling agency data or using agency systems.

Condition:
Upon inquiry with management personnel, it was determined that contractors are not required to undergo security awareness training.

Criteria:
NIST 800-53, Revision 4, Awareness and Training (AT-2), training, states:
"**NIST SP 800-53 Control:** The organization:

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

a. As part of initial training for new users;
b. When required by information system changes; and
c. Within [*5 days*] thereafter."

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 requiring contractors to undergo security awareness training, there is the risk that these individuals may access data or systems in a manner that is at risk to the agency. It is imperative that all individuals with access to agency data and systems undergo security awareness training so that they will be informed of the risks as well as their responsibilities in terms of handling agency data and accessing systems.

Recommendation:

2. Contractors should undergo formalized security awareness training within 5 days of being granted access to agency data or systems. This training should then be delivered on an annual basis or earlier if there are significant changes to the network.

Management Response:

Management agrees with this recommendation, and will ensure that within 5 days of being granted access to the agency data or systems, all FMC contractors will undergo the same security awareness training that the FMC staff are required to take.

03 Complexity Settings

A minimum password age policy determines the period of time (in days) that a password can be used before the system requires the user to change it. The minimum password age policy (one day or greater), used in conjunction with enforce password history, is helpful to prevent users from reusing their current password, thereby increasing computer security.

Condition:
Upon review of the password complexity settings, it was revealed that the minimum day password setting was set to "0".

It shall also be noted that this condition has been resolved prior to the close of the fiscal year, but was a weakness for the majority of the FY.

Criteria:
NIST 800-53, Revision 4, Identification and Authentication (IA-5), states:
"The organization manages information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators defined by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e. Changing default content of authenticators prior to information system installation;
f. *Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;*
g. Changing/refreshing authenticators;
h. Protecting authenticator content from unauthorized disclosure and modification;
i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
j. Changing authenticators for group/role accounts when membership to those accounts changes."

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 at least a minimum password setting of "1", the respective users can change their passwords at will until such time as arriving at their original password and avoiding the password expiration setting.

Recommendation:

3. Passwords should have a minimum password age policy setting of at least "1" day.

Management Response:

Management agrees with this recommendation. The password age policy has been updated, and the new policy setting the password age of two (2) days was implemented effective September 1, 2016. Management considers this recommendation closed.

STATUS OF PRIOR YEAR RECOMMENDATIONS

#	POA&M	Report	Open / Closed
1	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)	Closed
2	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: 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 policy and 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
3	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
4	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.	Report A16-02 (#1)	Closed
5	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.	Report A16-02 (#2)	Open
6	The Configuration Management Plan should be finalized and approved, and include the types of changes as well as a list of configuration items.	Report A16-02 (#3)	Closed
7	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.	Report A16-02 (#4)	Closed
8	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.	Report A16-02 (#5)	Closed
9	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.	Report A16-02 (#5)	Closed

UNITED STATES GOVERNMENT FEDERAL MARITIME COMMISSION

Memorandum

TO : Inspector General **DATE:** November 4, 2016

FROM : Managing Director

SUBJECT : Evaluation of the FMC's Compliance with FISMA, FY 2016 – Management's Response

I have reviewed the findings and recommendations contained in the subject report. Commission management values the efforts of the OIG and auditors in reviewing this critical issue for compliance and recommendations for improvement.

Recommendation #1: The Incident Response Plan shall be reviewed annually or whenever there are significant changes to the agency's environment. Based on these reviews, the Incident Response Plan should be updated and communicated to pertinent personnel involved in managing incidents.

Response: Management agrees with this recommendation. The Commission's Incident Response Plan was revised effective September 22, 2016. Going forward, the plan will be reviewed annually or whenever significant changes occur. Management considers this recommendation closed.

Recommendation #2: Contractors should undergo formalized security awareness training within 5 days of being granted access to agency data or systems. This training should then be delivered on an annual basis or earlier if there are significant changes to the network.

Response: Management agrees with this recommendation, and will ensure that within 5 days of being granted access to the agency data or systems, all FMC contractors will undergo the same security awareness training that the FMC staff are required to take.

Recommendation #3: Passwords should have a minimum password age policy setting of at least "1" day.

Response: Management agrees with this recommendation. The password age policy has been updated, and the new policy setting the password age of two (2) days was implemented effective September 1, 2016. Management considers this recommendation closed.

Please let me know if you have any questions concerning management's response.

Karen V. Gregory

cc: Office of the Chairman