Office of Inspector General

Evaluation of the FMC's Compliance with the Federal Information Security Management Act FY 2017

A18-02

FINAL REPORT

FEDERAL MARITIME COMMISSION

FEDERAL MARITIME COMMISSION
Washington, DC 20573

October 31, 2017

Office of Inspector General

Dear Acting Chairman Khouri and Commissioners Dye, Doyle, and Maffei:

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) 2017. 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). More specifically, the purpose of the evaluation was to identify areas for improvement in the FMC's information security policies, procedures, standards, and guidelines.

The FMC continues to make improvements on the agency's information technology (IT) security. The OIG concluded the FMC has effectively implemented all six of the prior year FISMA recommendations. Further, this report contains two recommendations to address two 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

TABLE OF CONTENTS

PURPOSE 1
BACKGROUND 1
SCOPE AND METHODOLOGY 2
CURRENT YEAR FINDINGS 3
01 Separated Users 3
02 Server Room Access 4
STATUS OF PRIOR YEAR RECOMMENDATIONS 5

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 OIG.

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, Security and Privacy 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, 2016 through September 30, 2017 (fiscal year 2017).

NIST 800-53, Rev. 4[1], has several families and controls within those families. The number of controls will vary depending on the security 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
Access Control (AC)	AC-2, AC-5, AC-7, AC-8, AC-11, AC-17, AC-18
Accountability, Audit and Risk Management (AR)	AR-2
Awareness and Training (AT)	AT-2, AT-3
Audit and Accountability (AU)	AU-2, AU-4, AU-6
Security Assessment and Authorization (CA)	CA-2, CA-3, CA-7, CA-9
Configuration Management (CM)	CM-3, CM-6, CM-8
Contingency Planning (CP)	CP-2, CP-6
Identification and Authentication (IA)	IA-2, IA-4, IA-5, IA-8
Media Protection (MP)	MP-2, MP-5, MP-6
Physical and Environmental Protection (PE)	PE-3, PE-8
Planning (PL)	PL-2
Personnel Security (PS)	PS-3, PS-4, PS-5
Risk Assessment (RA)	RA-5
System and Services Acquisition (SA)	SA-10, SA-11
System and Communications Protection (SC)	SC-8, SC-18
System and Information Integrity (SI)	SI-2, SI-3, SI-4, SI-5, SI-8

[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 Separated Users

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 did not timely disable the access for one of the sampled users that was terminated.

Criteria:
NIST 800-53, Revision 4, Personnel Termination (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 adhere to all of the controls in NIST 800-53, Revision 4.

Risk:
If an agency has terminated personnel 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:
1. The Office of Information Technology (OIT) should ensure that all separated users have their access disabled within 5 business days of being terminated from the agency.

Management Response:
Management agrees with this recommendation, and notes that there is a policy in place to disable the accounts of those separating from the FMC within 5 days – OIT disables the account of the departing employee at the time their checkout form (Form FMC-25, *Employee Clearance Statement*) is presented for OIT's sign off.

In the instance noted, one employee's access was not disabled according to the policy. This oversight occurred because the employee did not follow the normal checkout procedure. This resulted in the OIT not receiving appropriate notification to disable the employee's user account on the day of her departure. Management will review the policy and the process to ensure that access is revoked in a timely manner for all departing users in the future.

02 Server Room Access

Access to the server room, where computer hardware for the agency's systems are stored, must be protected physically.

Condition:
Upon review of the listing of those personnel with access to the server room, there was an excessive number of personnel with access to the server room. Additionally, there were also other personnel that had access to the server room that had little or no reason to gain access to the server room.

Criteria:
NIST 800-53, Revision 4, Physical Access Control (PE-3), states:

"The organization:

a. Maintains visitor access records to the facility where the information system resides; and
b. Reviews visitor access records [*Assignment: organization-defined frequency*]."

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

Risk:
Although there are controls to detect which personnel have access to the server room, and reports can be generated and reviewed; there are an excessive number of people with access to the server room. With an increased number of people having access to the server room, there is the risk of having to rely only on detective controls instead of both preventive and detective controls. Having personnel with access to the server room that do not have primary responsibilities over the server room, and failing to remove separated personnel from the access list, increases the risk that hardware supporting the agency's systems can be compromised.

Recommendation:
2. Ensure the list of all personnel with access to the server room is reviewed at least quarterly. Upon review of the listing, remove anyone's access that does not have a direct need for the server room.

Management Response:
Management agrees with this recommendation. The list of those with server room access was reviewed, and personnel who separated from the agency or whose access was determined to be non-essential were removed from the list. Moving forward, this access list will be provided for review on a quarterly basis to the Office of Information Technology by the Office of Management Services, which controls Data Watch access groups.

STATUS OF PRIOR YEAR RECOMMENDATIONS

#	POA&M	Report	Open / Closed
1	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)	Closed
2	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)	Closed
3	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)	Closed Note: Although the agency established a policy, and therefore this recommendation is closed, we found the policy has not been effectively implemented. See finding 01, Separated Users, recommendation #1.

#	POA&M	Report	Open / Closed
4	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.	Report A17-02 (#1)	Closed
5	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.	Report A17-02 (#2)	Closed
6	Passwords should have a minimum password age policy setting of at least "1" day.	Report A17-02 (#3)	Closed