FEDERAL MARITIME COMMISSION

OFFICE OF INSPECTOR GENERAL

Audit of the FMC's Compliance with the Federal Information Security Modernization Act

Fiscal Year 2019

Report No. A20-03

FINAL

TABLE OF CONTENTS

PURPOSE 1
BACKGROUND 1
SCOPE AND METHODOLOGY 1
CURRENT YEAR FINDINGS 3
STATUS OF PRIOR YEAR RECOMMENDATIONS 7
MANAGEMENT RESPONSE 8

PURPOSE

Dembo Jones, P.C. (contractor), on behalf of the Federal Maritime Commission (FMC), Office of Inspector General (OIG), conducted an independent audit of the quality and compliance of the FMC's information security program with applicable federal computer security laws and regulations. Dembo Jones' audit focused on FMC's information security program as required by the Federal Information Security Modernization Act (FISMA), as amended. This report was prepared by the contractor with guidance by the OIG. Mr. Jack Heyman, CISA, CAP, CIPP, CPA, CGFM, led the project for Dembo Jones, P.C.

BACKGROUND

The Federal Information Security Modernization Act of 2014 (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

We conducted this audit in accordance with generally accepted government auditing standards, issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions, based on our audit objectives.

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, 2018 through September 30, 2019 (fiscal year 2019).

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-11
Awareness and Training (AT)	AT-1, AT-2, AT-3, AT-4
Audit and Accountability (AU)	AU-2, AU-3, AU-4, AU-6
Security Assessment and Authorization (CA)	CA-7
Configuration Management (CM)	CM-8, CM-9
Contingency Planning (CP)	CP-3, CP-4, CP-9
Identification and Authentication (IA)	IA-5
Incident Response (IR)	IR-2, IR-3
Physical and Environmental Protection (PE)	PE-3, PE-4, PE-6
Planning (PL)	PL-4
Personnel Security (PS)	PS-2, PS-3, PS-4, PS-5
Risk Assessment (RA)	RA-5
System and Services Acquisition (SA)	SA-1, SA-4
System and Communications Protection (SC)	SC-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 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:
In the sample we selected for review, there was one High vulnerability identified in the scan results, which was not remediated in a timely manner (more than one month). FMC's organization-defined frequency is as follows:

Scans are conducted at least monthly and remediation is denoted below:

- Critical – within 10 days
- High – within 30 days
- Medium – within 60 days
- Low – ad hoc

Criteria:
NIST 800-53, Revision 4, Risk Assessment (RA-5) states:

1. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported;
2. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and
    3. Measuring vulnerability impact;
3. Analyzes vulnerability scan reports and results from security control assessments;
4. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and
5. Shares information obtained from the vulnerability scanning process and security control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

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 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. FMC should remediate vulnerabilities in a timely manner consistent with agency policy and guidance from the Department of Homeland Security.

Management Response:

Management agrees with this recommendation and will ensure that, going forward, legitimate vulnerabilities are remediated in a timely manner per established NIST and DHS guidelines.

2 Access Authorization Management

Condition:
The FMC is not currently assigning risk designations to all organizational positions. Each employee and contractor should be given a position risk designation so that this can be used when approving their access authorizations. Employees and contractors with a higher risk designation may require a more frequent review of their access rights. These employees and contractors may be more scrutinized when approving rights as well. For these reasons, it is imperative for all employees and contractors to have been assessed in terms of their position risk designation.

Note:
As of September 30th, 2019, this deficiency is considered closed. The deficiency is being reported because it was open for most of the fiscal year, however this was remediated at year-end.

Criteria:
NIST 800-53, Revision 4, Personnel Security (PS-2) states:
"The organization:
a. Assigns a risk designation to all organizational positions;
b. Establishes screening criteria for individuals filling those positions; and
c. Reviews and updates position risk designations [Annually]."

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 assigning a risk designation to all personnel, there is the risk that employees and/or contractors will have access provisions which are not commensurate with their risk designation, thereby posing a risk to the agency.

Recommendation(s):

2. All employees and contractors should be assigned a risk designation, which shall then be used when assigning computer network access provisions/privileges.

Management Response:

Management agrees with this recommendation, and all employees and contractors have been assigned risk designations. As of September 30, 2019, this deficiency is considered closed.

3 Access Authorization Management

Condition:
Upon review of a sampled set of users for their access authorizations (assessment of access rights being proposed for employees and contractors when they are reviewed and approved), the following was noted:

- There was no evidence to conclude that an ***annual*** recertification of users' access rights is being performed for non-Administrator contractors; and Administrator users (contractors) are not being reviewed on a ***semi-annual*** basis.

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."

"Requires approvals by [*Assignment: organization-defined personnel or roles*] for requests to create information system accounts."

"Reviews accounts for compliance with account management requirements [Admin users on a semi-annual basis, and regular end-users on an annual basis]."

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, there is the risk that users will be authorized network access 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):

3. All contractors should be recertified on an annual basis for regular end-users, and semi-annually for administrator users.

Management Response:

Management agrees with this recommendation and, going forward, will ensure that all contractors are recertified not less frequently than on an annual basis.

STATUS OF PRIOR YEAR RECOMMENDATIONS

#	Recommendation	Report	Open / Closed
1	OIT should ensure that all separated users have their access disabled within 5 business days of being terminated from the agency.	Report A18-02 (#1)	Closed
2	Conduct incident response prevention, detection and correction testing on an annual basis.	Report A19-02 (#1)	Closed
3	Ensure all contracts that affect the management of data include all of the provisions stated within NIST 800-53, Rev. 4 for the SA-4 control.	Report A19-02 (#2)	Closed
4	Revise the Rules of Behavior to include social media/networking sites and posting organizational information on public websites.	Report A19-02 (#3)	Closed
5	Ensure all employees and contractors sign the revised Rules of Behavior as evidence of their acceptance.	Report A19-02 (#4)	Closed
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 A19-02 (#5)	Closed

UNITED STATES GOVERNMENT FEDERAL MARITIME COMMISSION

Memorandum

TO : Inspector General **DATE**: October 15, 2019

FROM : Managing Director

SUBJECT : Audit of the FMC's Compliance with the Federal Information Security Modernization Act, FY 2019

I have reviewed the findings and recommendations contained in the subject audit. Management values the Inspector General's efforts in reviewing the quality and compliance of the Commission's information security program with applicable federal computer security laws and regulations. We appreciate the recommendations for improvement in this important effort, and note that all recommendations from prior years have been closed.

Recommendation #1: FMC should remediate vulnerabilities in a timely manner consistent with agency policy and guidance from the Department of Homeland Security.

Comment: Management agrees with this recommendation and will ensure that, going forward, legitimate vulnerabilities are remediated in a timely manner per established NIST and OHS guidelines.

Recommendation #2: All employees and contractors should be assigned a risk designation, which shall then be used when assigning computer network access provisions/privileges.

Comment: Management agrees with this recommendation, and all employees and contractors have been assigned risk designations. As of September 30, 2019, this deficiency is considered closed.

Recommendation #3: All contractors should be recertified on an annual basis for regular end users, and semi-annually for administrator users.

Comment: Management agrees with this recommendation and, going forward, will ensure that all contractors are recertified not less frequently than on an annual basis.

Karen V. Gregory

cc: Office of the Chairman