FEDERAL MARITIME COMMISSION

OFFICE OF INSPECTOR GENERAL

Evaluation of the FMC's Compliance with the Federal Information Security Management Act FY 2018

Report No. A19-02

FINAL

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 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, 2017 through September 30, 2018 (fiscal year 2018).

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, AC-17
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-5, CA-7, CA-8
Configuration Management (CM)	CM-8, CM-9, CM-10, CM-11
Contingency Planning (CP)	CP-3, CP-4
Identification and Authentication (IA)	IA-5, IA-8
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-3, PS-4, PS-5, PS-6
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 Incident Response

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-throughs 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 because of the incident.

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

- There was no testing of the current incident response environment.

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

Cause:
Due to a lack of personnel, budget, or time constraints, FMC did not adequately document and/or assess all of the incident response controls in NIST 800-53, Revision 4.

Effect:
Without formalized and yearly testing 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:

1. Conduct incident response prevention, detection and correction testing on an annual basis.

Management Response:
Management agrees with this recommendation and the Office of Information Technology will conduct and document incident response testing annually beginning in FY 2019.

02 Acquisitions and Contracts

NIST guidance provides for the establishment of specific clauses that should be contained within contracts to ensure that agency data is adhering to standards that meet or exceed the various NIST requirements.

Condition:
A sample of one contract was obtained and reviewed and it was determined that there were no references in the contract relating to the following:

- Security functional requirements
- Security strength requirements
- Security assurance requirements

It also did not provide requirements for the developer of the system to provide a description of the functional properties of the security controls to be employed.

Criteria:
NIST 800-53, Revision 4, Acquisition Process (SA-4) states:

1. "The organization includes the following requirements, descriptions, and criteria, either explicitly or by reference, in information system acquisition contracts based on applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

a. Security functional requirements;
b. Security strength requirements;
c. Security assurance requirements;
d. Security-related documentation requirements;
e. Description of the information system development environment and environment in which the system is intended to operate; and
f. Acceptance criteria."

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.

Effect:
Without appropriate clauses in agency contracts, there is the risk that the FMC will enter into contracts where the data will not be protected in accordance with NIST or at least meet the minimum standards within NIST.

Recommendation:

2. 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.

Management Response:
Management agrees with this recommendation and will ensure that, going forward, all contracts that affect the management of data include all of the provisions stated within NIST 800-53, Rev. 4, as revised, for the SA-4 acquisition process control. OMS will do so by providing requirements to the ISSO for vetting purposes prior to contract award.

03 Rules of Behavior

Condition:
Upon review of a sampled set of users for their evidence of accepting the Rules of Behavior, the following was noted:

- The Rules of Behavior that is required for all employees and contractors did not include the provisions for social media, networking sites, posting information on commercial websites, and sharing of information.

Note: As of September 2018, the Rules of Behavior have been updated to include social media, posting on public websites and networking. Therefore, this part of the deficiency is closed as of the fiscal year-end, but was a weakness for the majority of the FY. FMC is working to ensure that all employees sign the updated Rules of Behavior.

Criteria:
<u>NIST 800-53, Revision 4, Rules of Behavior (PL-4) states:</u>

“The organization:

a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
c. Reviews and updates the rules of behavior [*Assignment: organization-defined frequency*]; and
d. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.”

Further,
“The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.”

Cause:
Due to a lack of personnel, budget, or time constraints, FMC did not adequately include all provisions within their Rules of Behavior in accordance with NIST 800-53, Revision 4.

Effect:
Without ensuring that the Rules of Behavior includes stipulations for social media, posting on networking sites, and sharing of information; there is the increased risk that employees and contractors will be unaware of their roles and responsibilities. Without knowledge of their roles and responsibilities, it further increases the risk that the agency will be exposed to unforeseen risks through the sharing, posting or dissemination of data which can be used for subsequent exploitation.

Recommendations:

3. Revise the Rules of Behavior to include social media/networking sites and posting organizational information on public websites.
4. Ensure all employees and contractors sign the revised Rules of Behavior as evidence of their acceptance.

Management Response:
Management agreed with this recommendation, and the Commission’s Rules of Behavior were updated in September 2018 to include social media, posting on public websites and networking. Management is aware that this was a weakness for the greater part of the fiscal year, however this deficiency is now considered closed.

Management agrees with this recommendation and will require that all employees acknowledge, by the end of the first quarter of FY 2019, that they have read and agree to abide by the Commission’s revised Rules of Behavior. Management understands the employee acknowledgement may be in the form of an email from the involved employee. Additionally, going forward, the new Rules of Behavior will be added to the Commission’s security awareness test policy acknowledgement page.

04 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; and
c. Defines the configuration items for the information system and places the configuration items under configuration management.

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

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

Note: This deficiency was resolved in August of 2018, but was a weakness for the majority of the FY.

Criteria:
<u>NIST 800-53, Revision 4, Configuration Management Plan (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.

Effect:
Without an up-to-date 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:

5. 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:
The Commission's Configuration Management Plan was finalized in August 2018. Management is aware that this was a weakness for the greater part of the fiscal year, however this deficiency is now considered closed.

STATUS OF PRIOR YEAR RECOMMENDATIONS

#	POA&M	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. [***FY 2018 Testing Update***: *Upon review of the users that separated from the agency during FY 2018, the agency had two abrupt terminations. Although these terminated users' passwords were changed promptly, their accounts were not disabled for approximately five and eight months respectively.*] [***FY 2018 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 two instances noted during the FY 2018 review, OIT promptly changed the passwords on the email accounts, ensuring that separated users could not access their accounts. However, the accounts were not disabled because of the abrupt nature of their departures from the agency and the immediate need to access emails and files necessary for the agency to complete critical tasks. Going forward, disabled email accounts of departing employees will reside in an Organizational Unit (OU) within Active Directory, and any future access controlled by OIT through issuance of new access privileges. An artifact of the disablement of the account will be maintained in the Varonis DatAdvantage Active Directory log. These procedures will be implemented immediately.]	Report A18-02 (#1)	Open
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.	Report A18-02 (#2)	Closed

MANAGEMENT RESPONSE

UNITED STATES GOVERNMENT FEDERAL MARITIME COMMISSION

Memorandum

TO : Inspector General **DATE:** October 26, 2018

FROM : Managing Director

SUBJECT : Management's Response to Audit Report No. A19-02: *Evaluation of the FMC's Compliance with the Federal Information Security Management Act FY 2018*

I have reviewed the findings and recommendations contained in the subject report. Management appreciates the efforts of the OIG and auditors in reviewing the Commission's information security program for risk, compliance, and in making recommendations for improvement.

Audit Report A19-02 – Evaluation of the FMC's Compliance with the Federal Information Security Management Act, FY 2018

Recommendation #1: Conduct incident response prevention, detection and correction testing on an annual basis.

Comment: Management agrees with this recommendation and the Office of Information Technology will conduct and document incident response testing annually beginning in FY 2019.

Recommendation #2: 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.

Comment: Management agrees with this recommendation and will ensure that, going forward, all contracts that affect the management of data include all of the provisions stated within NIST 800-53, Rev. 4, as revised, for the SA-4 acquisition process control. OMS will do so by providing requirements to the ISSO for vetting purposes prior to contract award.

Recommendation #3: Revise the Rules of Behavior to include social media/networking sites and posting organizational information on public websites.

Comment: Management agreed with this recommendation, and the Commission's Rules of Behavior were updated in September 2018 to include social media, posting on public websites and networking. Management is aware that this was a weakness for the greater part of the fiscal year, however this deficiency is now considered closed.

Recommendation #4: Ensure all employees and contractors sign the revised Rules of Behavior as evidence of their acceptance.

Comment: Management agrees with this recommendation and will require that all employees acknowledge, by the end of the first quarter of FY 2019, that they have read and agree to abide by the Commission's revised Rules of Behavior. Management understands the employee acknowledgement may be in the form of an email from the involved employee. Additionally, going forward, the new Rules of Behavior will be added to the Commission's security awareness test policy acknowledgement page.

Recommendation #5: The Configuration Management Plan should be finalized and approved and include the types of changes as well as a list of configuration items.

Comment: The Commission's Configuration Management Plan was finalized in August 2018. Management is aware that this was a weakness for the greater part of the fiscal year, however this deficiency is now considered closed.

Prior Year Recommendations

Audit Report A18-02 – Evaluation of the FMC's Compliance with the Federal Information Security Management Act, FY 2017

Recommendation #1: OIT should ensure that all separated users have their access disabled within 5 business days of being terminated from the agency.

Comment: 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 two instances noted during the FY 2018 review, OIT promptly changed the passwords on the email accounts, ensuring that separated users could not access their accounts. However, the accounts were not disabled because of the abrupt nature of their departures from the agency and the immediate need to access emails and files necessary for the agency to complete critical tasks. Going forward, disabled email accounts of departing employees will reside in an Organizational Unit (OU) within Active Directory, and any future access controlled by OIT through issuance of new access privileges. An artifact of the disablement of the account will be maintained in the Varonis DatAdvantage Active Directory log. These procedures will be implemented immediately.

Should you have any questions regarding this information, please let me know.

/s/
Karen V. Gregory

cc: Office of the Chairman