FEDERAL MARITIME COMMISSION

OFFICE OF INSPECTOR GENERAL

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

Fiscal Year 2023

Report No. A23-03

FEDERAL MARITIME COMMISSION
Washington, DC 20573

July 28, 2023

Office of Inspector General

Dear Chairman Maffei and Commissioners Dye, Sola, Bentzel, and Vekich:

Please find enclosed the Office of Inspector General's (OIG) report for the *Fiscal Year 2023 Audit of the FMC's Compliance with the Federal Information Security Modernization Act (FISMA)*. The OIG relied on the expertise of an information security evaluator from *Dembo Jones P.C.* for assistance on this mandated review.

The objectives of this independent audit of the FMC's information security program were to evaluate the FMC's security posture by assessing compliance with the FISMA. More specifically, the purpose of the audit was to identify areas for improvement in the FMC's information security policies, procedures, and practices.

The results of the OIG's FISMA audit found the FMC resolved one of the prior year audit recommendations and made progress towards implementing the other audit recommendation. In addition, this year's audit includes three new audit recommendations for weaknesses that existed during FY 2023. FMC management agreed with all three recommendations.

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

Respectfully submitted,

Jon Hatfield
Inspector General

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

TABLE OF CONTENTS

Contents

PURPOSE

Dembo Jones (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.

BACKGROUND

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies in the executive branch to develop, document, and implement an information security program to provide information security for the information and information systems that support the operations and assets for the agency.[1] 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 review performed on their information security programs and practices and to report the results to OMB. FISMA states that the independent review 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.

[1] The Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

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, 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 Information Systems and Organizations, Revision 5.[2] For example, testing covered system security plans, access controls, risk assessments, personnel security, contingency planning, identification / authentication and auditing. Because of recent changes in FISMA guidance, our testing was for the period October 1, 2022 through July 31, 2023 for fiscal year 2023.

NIST 800-53, Rev. 5 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. To promote consistency in Inspectors General (IG) annual evaluations performed under FISMA, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in coordination with OMB, the Department of Homeland Security (DHS), and the Federal Chief Information Officers (CIO) and Chief Information Security Officers (CISO) Councils developed an evaluation guide for IGs to use in their FY 2023 FISMA evaluations. The guide provides a baseline of suggested sources of evidence and test steps/objectives that can be used by IGs as part of their FISMA evaluations. The guide is a companion document to the FY 2023 IG FISMA metrics[3] and provides guidance to IGs to assist in their FISMA evaluations. For purposes of this FISMA engagement, the scope of our testing included the controls listed in table 1 on page 3.

[2] NIST, Security and Privacy Controls for Information Systems and Organizations, SP 800-53, Revision 5 (Gaithersburg, Md.: December 2020).
[3] FY 2023 FISMA Metrics Evaluators Guide (cisa.gov).

Table 1

Family	Controls
Access Control (AC)	AC-1, AC-2, AC-5, AC-6, AC-8, AC-11, AC-12, AC-17, AC-19, AC-21
Awareness and Training (AT)	AT-1, AT-2, AT-3
Audit and Accountability (AU)	AU-2, AU-3, AU-6
Security Assessment and Authorization (CA)	CA-1, CA-2, CA-3, CA-5, CA-6, CA-7
Configuration Management (CM)	CM-2, CM-3, CM-6, CM-7, CM-8, CM-10, CM-11
Contingency Planning (CP)	CP-1, CP-2, CP-3, CP-4
Identification and Authentication (IA)	IA-1, IA-2, IA-4, IA-5, IA-7, IA-8
Incident Response (IR)	IR-4, IR-5, IR-6
Media Protection (MP)	MP-3, MP-6
Planning (PL)	PL-2, PL-4
Program Management (PM)	PM-4, PM-5, PM-6, PM-9, PM-10, PM-13, PM-14, PM-20, PM-27, PM-30, PM-31
Personnel Security (PS)	PS-1, PS-6
Physical and Environmental (PE)	PE-3
Risk Assessment (RA)	RA-1, RA-3, RA-5, RA-8, RA-9
Supply Chain Risk Management (SR)	SR-1, SR-2, SR-3, SR-5, SR-6
System and Services Acquisition (SA)	SA-4, SA-8
System and Communications Protection (SC)	SC-7, SC-8, SC-10, SC-13, SC-18, SC-28
System and Information Integrity (SI)	SI-2, SI-3, SI-4, SI-7, SI-12
Privacy Controls (PT)	PT-5, PT-6

INTERNAL CONTROLS

Our audit consisted of reviewing the internal controls within the FMC's information security program in accordance with the Government Accountability Office's *Standards for Internal Control in the Federal Government*, September 2014 (Green Book). Our test procedures addressed the controls documented in Table 1 above. We developed our audit approach to address the coverage areas noted in Appendix A. This included addressing all the Green Book's internal control components (Control Environment; Risk Assessment; Control Activities; Information and Communication; and Monitoring) and a selection of the principles, based on the controls selected for this year's audit. Our test procedures included a review of various policies and procedures; assessment of risk; and testing specific system settings and configurations within the FMC's network infrastructure.

CURRENT YEAR FINDINGS

Incident Response - 01

Computer security incident response has become an important component of information technology (IT) programs. Cybersecurity-related attacks have become not only more numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.

Condition:

FMC experienced a security incident on January 11, 2023, however this incident was not reported to the United States Computer Emergency Readiness Team (US-CERT) until March 29, 2023.

Cause:

The FMC lacked preparedness in terms of determining the type of incidents to report to the US-CERT.

Criteria:

NIST Special Publication (SP) 800-61, Revision 2, Computer Security Incident Handling Guide, August 2012, Executive Summary section states:

"Organizations must create, provision, and operate a formal incident response capability. Federal law requires Federal agencies to report incidents to the United States Computer Emergency Readiness Team (US-CERT) office within the Department of Homeland Security (DHS)."

Recommendation:

All security incidents shall be reported to the US-CERT within one hour of an incident being discovered.

Management's Response:

Management agrees with this recommendation and will immediately address this finding by adhering to the requirement to report all security incidents within one hour of an incident being discovered.

Log Retention Policy - 02

Developing and approving a Log Retention Policy is critical to maintaining a strong security posture. It contains the necessary details concerning the types of logging that is performed and how long those logs should be retained. Maintaining and retaining logs are also important for an after-the-fact investigation, should one arise.

Condition:

The FMC does not currently have an approved Log Retention Policy.

Cause:

The FMC is in the process of developing several policies, one of which is the Log Retention Policy.

Criteria:

NIST Special Publication (SP) 800-92, Guide to Computer Security Log Management, September 2006, Executive Summary section states:

"A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. Many logs within an organization contain records related to computer security. These computer security logs are generated by many sources, including security software, such as antivirus software, firewalls, and intrusion detection and prevention systems; operating systems on servers, workstations, and networking equipment; and applications."

"Log management is essential to ensuring that computer security records are stored in sufficient detail for an appropriate period of time. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs are also useful when performing auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems."

NIST SP 800-61, Section 3.2.4 states:

"Create a Log Retention Policy. Information regarding an incident may be recorded in several places, such as firewall, [intrusion detection and prevention systems] (IDPS), and application logs. Creating and implementing a log retention policy that specifies how long log data should be maintained may be extremely helpful in analysis because older log entries may show reconnaissance activity or previous instances of similar attacks. Another reason for retaining logs is that incidents may not be discovered until days, weeks, or even months later. The length of time to maintain log data is dependent on several factors, including the organization's data retention policies and the volume of data."

Recommendation:

FMC should develop, document, and approve a Log Retention Policy.

Management's Response:

Management agrees with this recommendation. It is anticipated that a Log Retention Policy will be developed, approved, and implemented by the end of the 2nd quarter of 2024.

Condition:

The FMC's current Risk Assessment Policy does not meet the standard set forth in NIST SP 800-30 (Guide for Conducting Risk Assessments).

Cause:

The Office of Information Technology has a Risk Assessment Policy, but it does not incorporate all of the requirements needed to satisfy the NIST SP 800-53, section 3.16, Risk Assessment (RA-1).

Criteria:

NIST SP 800-53, section 3.16, Risk Assessment (RA-1) states:

"a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]: 1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] risk assessment policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and

c. Review and update the current risk assessment: 1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and 2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]."

Recommendation:

The FMC should develop and document an approved Risk Assessment Policy that utilizes NIST SP 800-30 (Guide for Conducting Risk Assessments) in its development.

Management's Response:

Management agrees with this recommendation. It is anticipated that the current Risk Assessment Policy will be revised using NIST SP 800-30 as a guide, and then approved and implemented by the end of the 2nd quarter of 2024.

STATUS OF PRIOR YEAR RECOMMENDATIONS

#	Recommendation	Report	Open / Closed
1	The FMC should develop and approve a finalized supply chain policy that adheres to the NIST 800-53 Rev. 5 requirements.	A23-01	**Open**
	Management Response: Management agreed with this recommendation. The Chief Information Security Officer (CISO), working with the program support contractor, created a standalone supply chain policy to implement NIST 800-53 Rev. 5 requirements. The policy is awaiting approval.		
2	The FMC should update the system security and privacy plan to include those updated controls detailed in NIST 800-53 Rev. 5. Once updated, the plan should be approved and reviewed on an annual basis.	A23-01	**Closed**

APPENDIX A

Standards for Internal Control in the Federal Government **Relevant Green Book Principles**	**Audit Procedures** **(coverage)**
Control Environment	
1. The oversight body and management should demonstrate a commitment to integrity and ethical values.	✓
2. The oversight body should oversee the entity's internal control system.	✓
3. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.	✓
4. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.	✓
Risk Assessment	
5. Management should define objectives clearly to enable the identification of risks and define risk tolerances.	✓
6. Management should identify, analyze, and respond to risks related to achieving the defined objectives.	✓
7. Management should identify, analyze, and respond to significant changes that could impact the internal control system.	✓
Control Activities	
8. Management should design control activities to achieve objectives and respond to risks.	✓
9. Management should design the entity's information system and related control activities to achieve objectives and respond to risks.	✓
10. Management should implement control activities through policies.	✓
Information and Communication	
11. Management should use quality information to achieve the entity's objectives.	✓
12. Management should internally communicate the necessary quality information to achieve the entity's objectives.	✓
13. Management should externally communicate the necessary quality information	✓

Standards for Internal Control in the Federal Government Relevant Green Book Principles	Audit Procedures (coverage)
to achieve the entity's objectives.	
Monitoring	
14. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.	✓
15. Management should remediate identified internal control deficiencies on a timely basis.	✓

APPENDIX B

UNITED STATES GOVERNMENT FEDERAL MARITIME COMMISSION

Memorandum

TO : Inspector General **DATE:** July 27, 2023

FROM : Managing Director

SUBJECT : Audit of the FMC's Compliance with the Federal Information Security Modernization Act, Fiscal Year 2023 (Audit A23-03)

I have reviewed the findings and recommendations contained in the subject audit. The Commission appreciates the Inspector General's efforts in reviewing the quality and compliance of its information security program with applicable federal computer security laws and regulations. We welcome the recommendations for improvement and note that one prior year recommendation remains open.

Current Year Recommendations:

Recommendation 1: All security incidents shall be reported to the US-CERT within one hour of an incident being discovered.

Comment: Management agrees with this recommendation and will immediately address this finding by adhering to the requirement to report all security incidents within one hour of an incident being discovered.

Recommendation 2: FMC should develop, document, and approve a Log Retention Policy.

Comment: Management agrees with this recommendation. It is anticipated that a Log Retention Policy will be developed, approved, and implemented by the end of the 2nd quarter of 2024.

Recommendation 3: The FMC should develop and document an approved Risk Assessment Policy that utilizes NIST SP 800-30 (Guide for Conducting Risk Assessments) in its development.

Comment: Management agrees with this recommendation. It is anticipated that the current Risk Assessment Policy will be revised using NIST SP 800-30 as a guide, and then approved and implemented by the end of the 2nd quarter of 2024.

Prior Year Recommendation:

Audit A23-01, Recommendation 1: The FMC should develop and approve a finalized supply chain policy that adheres to the NIST 800-53 Rev. 5 requirements.

Comment: Management agreed with this recommendation. The Chief Information Security Officer (CISO), working with the program support contractor, created a standalone supply chain policy to implement NIST 800-53 Rev. 5 requirements. The policy is awaiting approval.

LUCILLE MARVIN

Digitally signed by LUCILLE MARVIN
Date: 2023.07.26 09:36:29 -04'00'

Lucille L. Marvin

cc: Office of the Chairman
Office of Information Technology