FEDERAL MARITIME COMMISSION

OFFICE OF INSPECTOR GENERAL

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

Fiscal Year 2022

Report No. A23-01

FEDERAL MARITIME COMMISSION
Washington, DC 20573

October 7, 2022

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 2022 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 PC* for assistance on this mandated audit.

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 both of the prior year audit recommendations. In addition, this year's audit includes two audit recommendations related to new government-wide information security policy requirements. FMC management agreed with both 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 Parker Skaats at (202) 523-0535 or pskaats@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 1
BACKGROUND 1
SCOPE AND METHODOLOGY 1
INTERNAL CONTROLS 3
CURRENT YEAR FINDINGS 4
1 Supply Chain 4
2 System Security and Privacy Plan 6
STATUS OF PRIOR YEAR RECOMMENDATIONS 8
APPENDIX A 9
APPENDIX B 11

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.

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

[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).

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 Federal Information Systems and Organizations, Revision 52. 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, 2021 through September 30, 2022 (fiscal year 2022).

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 the Federal Information Security Modernization Act of 2014 (FISMA), the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in coordination with the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and the Federal Chief Information Officers and Chief Information Security Officers (CISO) councils developed an evaluation guide for IGs to use in their FY 2022 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 2022 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 portions of the controls in Table 1 that follows.

[2] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 5 (Gaithersburg, Md.: September 2020, includes updates as of December 10, 2020).
[3] FY22 Core IG Metrics Implementation Analysis and Guidelines (cisa.gov).

Table 1

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

01 Supply Chain

Condition:

Information technology security policies and procedures had not been updated to reflect the latest standards and controls, as detailed in the NIST 800-53 Rev. 5 standard. The supply chain policy was not in place for the fiscal year.

Revision 5 of NIST publication 800-53 represents a multi-year effort to develop the next generation of security and privacy controls. Among the most significant changes to the publication include the establishment of a new supply chain risk management control family. The dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, present an increasing level of risk to an organization. Supply chain-related events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code. These events can have a significant impact on the confidentiality, integrity, or availability of a system and its information and, therefore, can also adversely impact organizational operations

Criteria:

NIST 800-53 Rev. 5, SR-3 Supply Chain Controls and Processes Control:

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [*Assignment: organization-defined system or system component*] in coordination with [*Assignment: organization-defined supply chain personnel*];

b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain related events: [*Assignment: organization-defined supply chain controls*]; and

c. Document the selected and implemented supply chain processes and controls in [*Selection: security and privacy plans; supply chain risk management plan*; [*Assignment: organization defined document*]].

Cause:

The FMC is a small agency with limited impact from supply chain issues, therefore, other priorities took precedence during the current fiscal year. The supply chain policy will be developed in fiscal year 2023.

Effect:

Without an appropriate supply chain policy in place, there is the risk that the FMC will be unprepared for and unable to respond expeditiously in the event that supply chain issues affect the FMC.

Recommendation:

The FMC should develop and approve a finalized supply chain policy that adheres to the NIST 800-53 Rev. 5 requirements.

Management Response:

Management agrees with this recommendation and will address this finding by creating a standalone supply chain policy or by updating Commission Order 112, *Acquisitions*. The Office of Information Technology will take the lead and work with the Office of Management Services to determine which approach best meets the requirement. It is anticipated that this will be completed by the end of the second quarter of 2023.

02 System Security and Privacy Plan

Condition:

The System Security and Privacy Plan had not been updated to reflect the latest standards and controls, as detailed in the NIST 800-53 Rev. 5.

Criteria:

NIST 800-53 Rev. 5, PL-2 System Security and Privacy Plans Control:

a. Develop security and privacy plans for the system that:

1. Are consistent with the organization's enterprise architecture;

2. Explicitly define the constituent system components;

3. Describe the operational context of the system in terms of mission and business processes;

4. Identify the individuals that fulfill system roles and responsibilities;

5. Identify the information types processed, stored, and transmitted by the system;

6. Provide the security categorization of the system, including supporting rationale;

7. Describe any specific threats to the system that are of concern to the organization;

8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;

9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;

10. Provide an overview of the security and privacy requirements for the system;

11. Identify any relevant control baselines or overlays, if applicable;

12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;

13. Include risk determinations for security and privacy architecture and design decisions;

14. Include security-and privacy related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups];

15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];

c. Review the plans [Assignment: organization-defined frequency];

d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and

e. Protect the plans from unauthorized disclosure and modification.

Cause:

The FMC had resource constraints, which prohibited the system security and privacy plan from being updated.

Effect:

Without updating the system security and privacy plan to the latest NIST 800-53 (Rev. 5); there is the increased risk that new or changed controls (contained within NIST 800-53 Rev. 5) will not be deployed thereby exposing the FMC to the risk of exploitation.

Recommendation:

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.

Management Response:

Management agrees with this recommendation. System security plans (SSPs) for the Commission's General Service System and two major applications (FMCDB and SERVCON) are reviewed annually as part of the FISMA audit. As in the past, a review table will be added to these documents to be signed after annual review by the CIO and the CISO. The Certification and Accreditation (C&A) packages for the FMC GSS, FMCDB, and SERVCON systems were reviewed and approved by the CIO and Certifying Official on September 10, 2022. It is anticipated that the SSPs will be updated in the first quarter of 2023.

STATUS OF PRIOR YEAR RECOMMENDATIONS

#	Recommendation	Report	Open / Closed
1	Passwords should have a minimum password age policy setting of at least "1" day.	A22-02	**Closed**
2	The Office of Information Technology (OIT) should develop, review and update, as necessary, the following information security program policies and procedures in accordance with NIST and agency requirements: a. Risk policies and procedures. b. System Development Life Cycle (SDLC) policy. c. Personnel Security policy. d. Security Assessment policy. e. Configuration Management policy. f. Configuration Management Plan. g. Security Awareness policy. h. Identification and Authentication policy. i. Access policy.	A21-02	**Closed** a. Closed b. Closed c. Closed[4] d. Closed e. Closed f. Closed g. Closed[4] h. Closed[4] i. Closed

[4] This deficiency was closed during the prior year audit.

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.	✓

Standards for Internal Control in the Federal Government **Relevant Green Book Principles**	**Audit Procedures** **(coverage)**
13. Management should externally communicate the necessary quality information 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:** September 28, 2022

FROM : Managing Director

SUBJECT : Audit of the FMC's Compliance with the Federal Information Security Modernization Act, Fiscal Year 2022 (Audit A 23-01)

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 all prior year recommendations have been closed.

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 agrees with this recommendation and will address this finding by creating a standalone supply chain policy or by updating Commission Order 112, *Acquisitions*. The Office of Information Technology will take the lead and work with the Office of Management Services to determine which approach best meets the requirement. It is anticipated that this will be completed by the end of the second quarter of 2023.

Recommendation 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.

Comment: Management agrees with this recommendation. System security plans (SSPs) for the Commission's General Service System and two major applications (FMCDB and SERVCON) are reviewed annually as part of the FISMA audit. As in the past, a review table will be added to these documents to be signed after annual review by the CIO and the CISO. The Certification and Accreditation (C&A) packages for the FMC GSS, FMCDB, and SERVCON systems were reviewed and approved by Edward Anthony, CIO and Certifying Official on September 10, 2022 (copy attached). It is anticipated that the SSPs will be updated in the first quarter of 2023.

LUCILLE MARVIN

Digitally signed by LUCILLE MARVIN
Date: 2022.09.29 11:50:11 -04'00'

Lucille L. Marvin

cc: Office of the Chairman