FEDERAL MARITIME COMMISSION

OFFICE OF INSPECTOR GENERAL

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

Fiscal Year 2025

Report No. A25-03

FEDERAL MARITIME COMMISSION
Washington, DC 20573

September 19, 2025

Office of Inspector General

Dear Commissioners Dye, Maffei, and Vekich:

Please find attached the Office of Inspector General's (OIG) report for the *Fiscal Year (FY) 2025 Audit of the FMC's Compliance with the Federal Information Security Modernization Act (FISMA)*. The OIG relied on the expertise of information security auditors from the certified public accounting firm Harper, Rains, Knight & Company, P.A. (HRK) to perform the audit.

The objective of this performance audit was to assess the effectiveness of the FMC's information security program and practices for FY 2025. 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's information security program to be consistently implemented and ***effective***. Further, FMC resolved six prior year audit recommendations and made progress towards implementing the other two open audit recommendations. In addition, we followed up on recommendations issued during the FMC's 2023 Information Technology Vulnerability Audit and found that FMC resolved seven audit recommendations and made progress towards implementing the final open audit recommendation. The FY 2025 audit did not result in any new findings. FMC management agreed with all remaining 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,

/s/
Jon Hatfield
Inspector General

Attachment

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

Harper, Rains, Knight & Company

PERFORMANCE AUDIT REPORT

FEDERAL MARITIME COMMISSION
FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 (FISMA)

FOR THE FISCAL YEAR ENDING
SEPTEMBER 30, 2025

Harper, Rains, Knight & Company, P.A.
1425 K ST NW, Suite 1120
Washington, DC 20005
202-558-5163
www.hrkcpa.com

Harper, Rains, Knight & Company

TABLE OF CONTENTS

Harper, Rains, Knight & Company

INDEPENDENT AUDITORS' PERFORMANCE AUDIT REPORT ON THE FEDERAL MARITIME COMMISSION'S COMPLIANCE WITH FEDERAL INFORMATION SECURITY MODERNIZATION ACT FOR FISCAL YEAR 2025

Jonathan Hatfield
Inspector General
Federal Maritime Commission

This report presents the results of our independent performance audit of the Federal Maritime Commission's (FMC) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires Federal agencies, including FMC, to have an annual independent evaluation performed of their information security programs and practices to determine the effectiveness of such programs and practices, and to report the results of the evaluation to the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). The FMC Office of Inspector General (OIG) contracted with Harper, Rains, Knight & Company, PA (HRK) to conduct a performance audit of FMC's information security program and practices for Fiscal Year (FY) 2025.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). 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 objective of this performance audit was to assess the effectiveness of the FMC's information security program and practices for FY 2025. As part of our audit, we responded to the core metrics and supplemental metrics identified in the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics (IG Metrics) and* the associated *FY 2025 Inspector General FISMA Metrics Evaluator's Guide.* We assessed the maturity levels to be consistently implemented and overall effective. The FMC is a small, independent federal agency. As such, in some instances, the FMC generally does not have the resources, or in some cases the need, to implement the extent of controls described at a level equal to or greater than "managed and measurable." We also considered applicable OMB policy and guidelines, National Institute of Standards and Technology's (NIST) standards and guidelines, and the NIST *Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework).*

We determined that FMC has established and maintained a consistently implemented information security program, consistent with applicable FISMA requirements, OMB policy and guidance, DHS guidance, and NIST standards and guidelines. The FY 2025 audit did not result in any new findings. However, two findings remain open from the FY 2024 FISMA audit. We identified the following open findings where the FMC Office of Information Technology's (OIT) information security program can better protect the confidentiality, integrity, and availability of its information and information systems:

- *FMC Has Not Met Event Logging Tiers in Accordance with OMB M-21-31; and*
- *Lack of Business Impact Analysis Policy, Results, and Incorporation into Contingency Planning Efforts.*

Addressing these open prior year findings will strengthen the FMC's information security program and practices and contribute to ongoing efforts to maintain reasonable assurance of adequate security over information resources.

This report is for the purpose of concluding on the audit objective described above. Accordingly, this report is not suitable for any other purpose. We appreciate the cooperation and courtesies that FMC personnel extended to us during the execution of this performance audit.

Washington, D.C.
September 16, 2025

Background

The Office of Information Technology (OIT) is responsible for planning, developing, implementing, and maintaining FMC's Information Technology (IT) program, policies, standards and procedures. OIT promotes the application and use of information technologies and administers policies and procedures within FMC to ensure compliance with related federal laws and regulations, to include information security. The Chief Information Officer is the official responsible for carrying out the mission of the OIT, which is responsible for designing the enterprise information architecture; determining the requirements of FMC's information systems; and developing the integrated systems for nationwide use. Within the OIT is the Chief Information Security Officer (CISO) who is the official responsible for carrying out the OIT responsibilities under FISMA, including IT governance and security, and is the primary liaison to FMC's authorizing officials, systems owners, and information security officials.

Federal Information Security Modernization Act of 2014

FISMA codifies the Department of Homeland Security's role in administering the implementation of information security policies for federal Executive Branch civilian agencies, overseeing agencies' compliance with those policies, and assisting OMB in developing those policies. The legislation provides the Department authority to develop and oversee the implementation of binding operational directives to other agencies, in coordination and consistent with OMB policies and practices. FISMA also:

- Authorizes DHS to provide operational and technical assistance to other federal Executive Branch civilian agencies at the agency's request;
- Places the federal information security incident center (a function fulfilled by US-CERT) within DHS by law;
- Authorizes DHS technology deployments to other agencies' networks (upon those agencies' request);
- Directs OMB to revise policies regarding notification of individuals affected by federal agency data breaches;
- Requires agencies to report major information security incidents as well as data breaches to Congress as they occur and annually; and
- Simplifies existing FISMA reporting to eliminate inefficient or wasteful reporting while adding new reporting requirements for major information security incidents.

FISMA requires FMC to develop, document, and implement an agency-wide information security program to protect its information and information systems, including those provided or managed by another agency, contractor, or other source. FISMA also clearly places responsibility on each agency program office to develop, implement, and maintain a security program that assesses risk and provides adequate security for the operations and assets of programs and systems under its control.

Furthermore, OIG must submit to DHS the "Inspector General FISMA Reporting Metrics" that depicts the effectiveness of the agency's information security program.

Fiscal Year 2025 IG Metrics

FISMA requires each agency inspector general (IG), or an independent external auditor, to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency. OMB, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and other stakeholders worked collaboratively to develop the *FY 2025 IG FISMA Reporting Metrics*. The *FY 2025 IG FISMA Reporting Metrics* represent a continuation of the work started in FY 2022, when the IG metrics reporting process was transitioned to a multi-year cycle.

The Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements (M-22-05) encouraged agencies to shift towards a continuous assessment process for their annual independent assessment. To help facilitate this, the memo also announced that OMB and CIGIE are transitioning the IG FISMA metrics to a multi-year cycle—with a set of core metrics that must be evaluated annually and the remaining metrics that will be evaluated on a two-year cycle, beginning in FY 2023.

The core metrics represent a combination of Administration priorities and other highly valuable controls that must be evaluated annually. Specifically, these core metrics align with the Executive Order on Improving the Nation's Cybersecurity (EO 14028), and guidance from OMB to agencies to improve federal cybersecurity, including:

- *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (M-22-09),* sets forth a plan for migrating the federal government to a new cybersecurity paradigm that does not presume that any person or device inside an organization's perimeter is trusted, and focuses agencies on strengthening their capability to limit, and continuously verify, the access those people and devices have to government data.
- *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents (M-21-31),* sets detailed requirements for log management, configuration, and enterprise-level centralization. It also provides a maturity model that prioritizes the most critical software types and requirements.
- *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (M-22-01)*, directs agencies, with support from the Cybersecurity and Infrastructure Security Agency (CISA), to accelerate their adoption of robust endpoint, detection, and response (EDR) solutions, an essential component for zero trust architecture that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.
- *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices (M-23-16),* which reinforces the requirements established in M-22-18, reaffirms the importance of secure software development practices, and provides supplemental guidance on the scope of M-22-18's requirements for agencies' use of Plans of Actions and Milestones (POA&Ms) when a software provider cannot provide the required attestation, but plans to do so.

The IG FISMA metrics are aligned with the six function areas in the NIST Cybersecurity Framework 2.0: govern, identify, protect, detect, respond, and recover. The Cybersecurity

Framework provides agencies with a common structure for managing and reducing their cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks.

Objective, Scope, and Methodology

The objective of this performance audit was to assess the effectiveness of the FMC's information security program and practices for the period October 1, 2024, through June 30, 2025. As part of our audit, we responded to the core metrics identified in the *FY 2025 Inspector General FISMA Reporting Metrics, the associated FY 2025 Inspector General FISMA Metrics Evaluator's Guide*, and assessed the maturity levels on behalf of the FMC OIG. We also considered applicable OMB policy and guidelines, National Institute of Standards and Technology's (NIST) standards and guidelines, and the NIST *Cybersecurity Framework.*

To address our audit objective, we assessed the overall effectiveness of the FMC information security program and practices in accordance with Inspector General reporting requirements:

- Cybersecurity Governance (Govern);
- Cybersecurity Supply Chain Risk Management (Govern);
- Risk and Asset Management (Identify);
- Configuration Management (Protect);
- Identity and Access Management (Protect);
- Data Protection and Privacy (Protect);
- Security Training (Protect);
- Information Security Continuous Monitoring (Detect);
- Incident Response (Respond); and
- Contingency Planning (Recover).

We conducted this audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We performed procedures to determine the status of recommendations from prior FISMA audits and the OIG's 2023 Information Technology Vulnerability Audit (ITVA), (see ***Appendix A***).

We reviewed FMC's general FISMA compliance efforts in the specific areas defined in DHS' guidance and the corresponding reporting instructions. We considered the internal control structure for FMC's systems in planning our audit procedures. Accordingly, we obtained an understanding of the internal controls over FMC's systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. Our understanding of these systems' internal controls was used to evaluate the degree to which the appropriate internal controls were designed and implemented. When appropriate, we conducted tests using judgmental sampling to determine the extent to which established controls and procedures are functioning as required.

To accomplish our audit objective, we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA;
- Reviewed documentation related to FMC's information security program, such as security policies and procedures, system security plans, and risk assessments;
- Tested system processes to determine the adequacy and effectiveness of selected controls; and
- Reviewed the status of recommendations in prior year FISMA and related audit reports.

The independent performance audit was conducted from February 24, 2025 through July 31, 2025. It covered the period from October 1, 2024, through June 30, 2025.

Criteria

The criteria used in conducting this audit included:

- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- FY 2025 Inspector General (IG) Federal Information Security Modernization Act (FISMA) Reporting Metrics;
- FY 2025 IG FISMA Metrics Evaluator's Guide, v 1.0, May 5, 2025;
- NIST SP 800-12, Rev. 1, *An Introduction to Computer Security*: *The NIST Handbook*;
- NIST SP 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*;
- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*;
- NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*;
- NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A system Life Cycle Approach for Security and Privacy;*
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*;
- NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations;*
- NIST *Framework for Improving Critical Infrastructure Cybersecurity* v1.1;
- NIST *Cybersecurity Framework* (CSF) v2.0;
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*;
- OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*;
- OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*;
- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*;
- OMB Memorandum M-21-30, *Protecting Critical Software through Enhanced Security Measures*;
- OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*;

- OMB Memorandum M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*;
- OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*;
- OMB Memorandum M-22-09, *Moving the U.S. Government to Zero Trust Cybersecurity Principles*;
- OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*;
- OMB Memorandum M-23-16, Update to Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices;*
- OMB Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements;*
- Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*;
- DHS CISA Binding Operational Directives (BODs) and Emergency Directives (EDs);
- Federal Cybersecurity Workforce Assessment Act of 2015;
- Federal Identity, Credential, and Access Management Roadmap Implementation Guidance;
- Federal Information Processing Standard (FIPS) Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors;* and
- Other criteria as appropriate.

Results

We assessed FMC's information security program to be consistently implemented, which we concluded was effective. The results of our independent performance audit concluded that FMC's information security program is generally compliant with the FISMA legislation and is consistent with the functional areas outlined in the NIST Cybersecurity Framework.

The summary assessment results for the FMC maturity level assessment by function areas are in ***Exhibit 1***. The five maturity model levels are *ad hoc*, *defined*, *consistently implemented*, *managed and measurable*, and *optimized.*

Exhibit 1 – FMC Overall Maturity Level Assessment by Function Area for Core Metrics

FISMA NIST Cybersecurity Framework Function Area	FY 2025 Maturity Level (Core & Supplemental Metrics)	FY 2024 Maturity Level (Core & Supplemental Metrics)
Govern	Managed and Measurable	N/A
Identify	Consistently Implemented	Consistently Implemented
Protect	Consistently Implemented	Consistently Implemented
Detect	Consistently Implemented	Consistently Implemented
Respond	Consistently Implemented	Consistently Implemented
Recover	Defined	Consistently Implemented

Ratings in FY 2025 focus on a calculated average approach, wherein the average of the metrics in a particular domain are used by IGs to determine the effectiveness of individual function areas (govern, identify, protect, detect, respond, and recover) and the overall program.

Findings and Recommendations

HRK has assessed the effectiveness of FMC information system security controls. Our FY 2025 audit report did not identify any new findings. However, two findings remain open from the FY 2024 FISMA audit. We identified the following open findings where the FMC Office of Information Technology's (OIT) information security program can better protect the confidentiality, integrity, and availability of its information and information systems.

Finding 1: FMC Has Not Met Event Logging Tiers in Accordance with OMB M-21-31 **(Prior Year Audit Finding #5)**

Condition:

FMC has not met event logging tiers of EL 3 in accordance with OMB M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents, August 27, 2021.

Criteria:

OMB M-21-31 states that recent events, including the SolarWinds incident, underscore the importance of increased government visibility before, during, and after a cybersecurity incident. Information from logs on Federal information systems (for both on-premises systems and connections hosted by third parties, such as cloud services providers (CSPs)) is invaluable in the detection, investigation, and remediation of cyber threats. The memo establishes a maturity model to guide the implementation of requirements across four Event Logging (EL) tiers, to include **EL3, Advanced Logging requirements at all criticality levels are met.**

Further, OMB M-21-31 states the following under Section II: Agency Implementation Requirements:

Agencies must immediately begin efforts to increase performance in accordance with the requirements of this memorandum. Specifically, agencies must:

- Within 60 calendar days of the date of this memorandum, assess their maturity against the maturity model in this memorandum and identify resourcing and implementation gaps associated with completing each of the requirements listed below. Agencies will provide their plans and estimates to their OMB Resource Management Office (RMO) and Office of the Federal Chief Information Officer (OFCIO) desk officer.
- Within one year of the date of this memorandum, reach EL1 maturity.
- Within 18 months of the date of this memorandum, achieve EL2 maturity.
- ***Within two years of the date of this memorandum, achieve EL3 maturity.***
- Provide, upon request and to the extent consistent with applicable law, relevant logs to the Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of

Investigation (FBI). This sharing of information is critical to defend Federal information systems.
- Share log information, as needed and appropriate, with other Federal agencies to address cybersecurity risks or incidents.

The Memorandum was dated August 27, 2021, which would require EL3 maturities by August 27, 2023.

Cause:

FMC has not achieved EL3 in accordance with OMB guidance.

Effect:

Without meeting the required maturity models for event logging, FMC may not have visibility before, during, and after a cybersecurity incident. Without the required event logs, FMC may not be able to detect, investigate, and remediate cyber threats.

Recommendation:

FMC should develop an executable plan to meet the requirements of OMB M-21-31 and ensure the plan is properly supported.

Management's Response and Our Comments:

Management agreed with the finding and recommendation. In April 2025, OIT implemented audit logging through the Azure cloud service offering. This implementation satisfies all requirements set forth by OMB M-21-31 except for the retention period. FMC's current log retention configuration is set for 90 days active. FMC anticipates configuring the Azure Sentinel cloud service offering to comply with the 12-month active, 18-month cold retention requirement. Anticipated completion time is the 2nd quarter of FY 2026.

These planned corrective actions have not been subject to performance audit procedures, and we therefore make no conclusion on the effectiveness of the planned corrective actions. Please see Appendix B for FMC management's full response.

Finding 2: Lack of Business Impact Analysis Policy, Results, and Incorporation into Contingency Planning Efforts **(Prior Year Audit Finding #6)**

Condition:

FMC has not developed, defined, nor completed a Business Impact Analysis (BIA) to incorporate into its contingency planning efforts.

Criteria:

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, establishes controls for systems and organizations, including the minimum controls required by the provisions of FISMA to protect federal information and information systems.

IG-Metric-33: (*FY 2025 IG FISMA Metrics Evaluation Guide*)
To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts?

CP-2, Contingency Plan: (*NIST SP 800-53, Rev. 5*)

a. Develop a contingency plan for the system that:
    1. Identifies essential mission and business functions and associated contingency requirements;
    2. Provides recovery objectives, restoration priorities, and metrics;
    3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
    4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
    5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
    6. Addresses the sharing of contingency information; and
    7. Is reviewed and approved by [Assignment: organization-defined personnel or roles];
b. Distribute copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];
c. Coordinate contingency planning activities with incident handling activities;
d. Review the contingency plan for the system [Assignment: organization-defined frequency];
e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];
g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and
h. Protect the contingency plan from unauthorized disclosure and modification.

RA-9, Criticality Analysis: (*NIST SP 800-53, Rev. 5*) Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].

ID.RA-4, Risk Assessment: [*NIST Cybersecurity Framework (CSF) v2.0*] Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.

Cause:

FMC does not have a policy or procedures requiring a BIA for inclusion into its contingency planning efforts.

Effect:

Without a BIA, FMC may not prioritize, correctly, the resumption of mission and business functions.

Recommendation:

We recommend that FMC:

1. Create an overall BIA policy, procedures, and processes or incorporate a BIA policy, procedures, and processes into its existing contingency planning documents.
2. Create a Template for completing BIAs consistently across the commission following NIST SP 800-34, rev. 1, Contingency Planning Guide for Federal Information Systems, Chapter 3.
3. Incorporate the BIAs results into its overall contingency planning efforts.

Management's Response and Our Comments:

Management agreed with the finding and recommendations. OIT will coordinate with the Office of the Managing Director to facilitate the development of a BIA. The BIA will identify the potential negative impacts of disruptions to the agency, help prioritize critical functions for recovery, aid in assessing the consequences of disruptions, determine acceptable downtime, and guide the priority of system recovery and business continuity plans. Anticipated completion time is the end of the 2nd quarter of FY 2026.

These planned corrective actions have not been subject to performance audit procedures, and we therefore make no conclusion on the effectiveness of the planned corrective actions. Please see Appendix B for FMC management’s full response.

Appendix A – Status of Prior Findings

No.	Prior Year Audit Recommendations	Status
1	**Audit A23-03 FISMA Recommendation No. 2**: FMC should develop, document, and approve a Log Retention Policy.	Closed
2	**Audit A23-03 FISMA Recommendation No. 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.	Closed
3	**FY24 FISMA Performance Audit Recommendation No. 1:** FMC should ensure that unauthorized and unmanaged software cannot be installed and executed.	Closed
4	**FY24 FISMA Performance Audit Recommendation No. 2:** Implement the procedures in the SCRM SOP and during FMC's annual review for changes to Commission Order (CO)-112, Acquisitions, include verbiage that all IT acquisitions should follow the SCRM SOP by reference.	Closed
5	**FY24 FISMA Performance Audit Recommendation No. 3:** Review the settings on all issued laptops to ensure MFA requirements are in place and review the FMC user setting population to ensure each user is properly configured.	Closed
6	**FY24 FISMA Performance Audit Recommendation No. 4:** Implement a monitoring process of required trainings at FMC so that when issues like the vendor management issue arises, they can identify and address early on to ensure the required training is met.	Closed
7	**FY24 FISMA Performance Audit Recommendation No. 5:** FMC should develop an executable plan to meet the requirements of OMB M-21-31 and ensure the plan is properly supported.	Open

No.	Prior Year Audit Recommendations	Status
8	**FY24 FISMA Performance Audit Recommendation No. 6:** FMC should create an overall business impact analysis (BIA) policy, procedures, and processes or incorporate a BIA policy, procedures, and processes into its existing contingency planning documents. FMC should create a template for completing BIAs consistently across the Commission following NIST SP 800-34, rev. 1, Contingency Planning Guide for Federal Information Systems, Chapter 3. FMC should also incorporate the BIA results into its overall contingency planning efforts	Open

In addition to our FISMA procedures, the OIG contracted HRK to review the status of findings and recommendations from their 2023 Information Technology Vulnerability Audit (ITVA), their status is below.

No.	2023 ITVA Audit Recommendations	Status
1	**2023 ITVA Recommendation No. 1**: [redacted]	Closed
2	**2023 ITVA Recommendation No. 2:** [redacted]	Open
3	**2023 ITVA Recommendation No. 3:** [redacted]	Closed
4	**2023 ITVA Recommendation No. 4:** [redacted]	Closed
5	**2023 ITVA Recommendation No. 5:** [redacted]	Closed

No.	2023 ITVA Audit Recommendations	Status
6	**2023 ITVA Recommendation No. 6:** [redacted]	Closed
7	**2023 ITVA Recommendation No. 7:** [redacted]	Closed
8	**2023 ITVA Recommendation No. 8:** [redacted]	Closed

Appendix B – FMC Management's Response

THIS PAGE INTENTIONALLY LEFT BLANK

UNITED STATES GOVERNMENT FEDERAL MARITIME COMMISSION

Memorandum

TO: Inspector General **DATE:** September 9, 2025

FROM: Deputy Managing Director

SUBJECT: Independent Auditors' Performance Audit Report on the Federal Maritime Commission's Compliance with Federal Information Security Modernization Act for Fiscal Year 2025

I have reviewed the subject audit of the Commission's information security program and practices, and note that no new findings or recommendations were identified. The Commission values the Office of the Inspector General's efforts in this critical evaluation.

Status of Prior Years Remaining Open Recommendations

Audit No. A24-02, Audit of the FMC's Compliance with the Federal Information Security Modernization Act (FISMA) FY 2024

Recommendation #5: FMC should develop an executable plan to meet the requirements of OMB M-21-31 and ensure the plan is properly supported.

Comment: Management agreed with the finding and recommendation. In April 2025, OIT implemented audit logging through the Azure cloud service offering. This implementation satisfies all requirements set forth by OMB M-21-31 except for the retention period. FMC's current log retention configuration is set for 90 days active. FMC anticipates configuring the Azure Sentinel cloud service offering to comply with the 12-month active, 18-month cold retention requirement. Anticipated completion time is the 2nd quarter of FY 2026.

Recommendation #6:

1. Create an overall business impact analysis (BIA) policy, procedures, and processes or incorporate a BIA policy, procedures, and processes into its existing contingency planning documents.
2. Create a template for completing BIAs consistently across the Commission following NIST SP 800-34, rev. 1, Contingency Planning Guide for Federal Information Systems, Chapter 3.
3. Incorporate the BIAs results into its overall contingency planning efforts.

Comment: Management agreed with the finding and recommendations. OIT will coordinate with the Office of the Managing Director to facilitate the development of a BIA. The BIA will identify the potential negative impacts of disruptions to the agency, help

prioritize critical functions for recovery, aid in assessing the consequences of disruptions, determine acceptable downtime, and guide the priority of system recovery and business continuity plans. Anticipated completion time is the end of the 2nd quarter of FY 2026.

Audit No. A23-01, Information Technology Vulnerability Audit

Recommendation #2: [redacted]

Comment: Management agreed with this finding and recommendation. [redacted]

Cindy Hennigan

cc: Office of the Chairman
Commissioner Rebecca F. Dye
Commissioner Daniel B. Maffei
Commissioner Max M. Vekich
Office of Information Technology