FEDERAL MARITIME COMMISSION

OFFICE OF INSPECTOR GENERAL

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

Fiscal Year 2024

Report No. A24-02

FEDERAL MARITIME COMMISSION
Washington, DC 20573

July 31, 2024

Office of Inspector General

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

Please find attached the Office of Inspector General's (OIG) report for the *Fiscal Year (FY) 2024 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 2024. 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 two prior year audit recommendations and made progress towards implementing the other two open audit recommendations. In addition, this year's audit includes new audit recommendations to address six findings that existed during FY 2024. FMC management agreed with all the 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, 2024

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 2024

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) 2024.

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 2024. As part of our audit, we responded to the core metrics and supplemental metrics identified in the *FY 2023 -2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics (IG Metrics)*, the associated *FY 2024 Inspector General FISMA Metrics Evaluator's Guide*, and assessed the maturity levels on behalf of the FMC OIG to be consistently implemented, which we determined to be 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 FMC established and maintained a consistently implemented information security program and practices, consistent with applicable FISMA requirements, OMB policy and guidance, DHS guidance, and NIST standards and guidelines. Our report identified the following 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:

- *Unauthorized and unmanaged software was installed and executed;*
- *Supply Chain Risk Management (SCRM) – SCRM and C-SCRM policies have been developed by OIT but have not been performed;*
- *Identity and Access Management (ICAM) – Non-Privileged user able to bypass multifactor authentication (MFA) to access SharePoint;*
- *Completion of Security Awareness Training;*
- *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 identified current year and open prior year findings strengthens the FMC's information security program and practices and contributes 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.

Harper, Rains, Knight & Company, P.A.

Washington, D.C.
July 31, 2024

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 2024 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 2023-2024 IG FISMA Reporting Metrics*. The *FY 2023-2024 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.
- *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices (M-22-18)*, initiates a government-wide shift towards requiring agencies to use software developed in a secure manner. This will minimize the risks associated with running unvetted technologies on agency networks, increasing the resilience of Federal technology against cyber threats.

The IG FISMA metrics are aligned with the five function areas in the NIST Cybersecurity Framework: identify, protect, detect, respond, and recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing 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, 2023, through June 30, 2024. As part of our audit, we responded to the core metrics identified in the *FY 2023 -2024 Inspector General FISMA Reporting Metrics, the associated FY 2024 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:

- Risk Management (Identify);
- Supply Chain Risk Management (Identify);
- Configuration Management (Protect);
- Identity, Credential, 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 (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;
- Reviewed the status of recommendations in prior year FISMA audit reports;
- Completed an internal network vulnerability assessment of selected FMC systems; and
- Completed an external network penetration testing of selected FMC systems.

The independent performance audit was conducted from February 21, 2024 through July 31, 2024. It covered the period from October 1, 2023, through June 30, 2024.

Criteria

The criteria used in conducting this audit included:

- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- FY 2023 – 2024 Inspector General (IG) Federal Information Security Modernization Act (FISMA) Reporting Metrics;
- FY 2024 IG FISMA Metrics Evaluator's Guide, v 4.0, April 30, 2024;
- 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) v1.1;
- 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-24-04, *Fiscal Year 2024 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 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 Functions Area for Core Metrics

Identify	Consistently Implemented	Defined
Protect	Consistently Implemented	Consistently Implemented
Detect	Consistently Implemented	Defined
Respond	Consistently Implemented	Consistently Implemented
Recover	Consistently Implemented	Managed and Measurable

Ratings in FY 2024 will focus on a calculated average approach, wherein the average of the metrics in a particular domain will be used by IGs to determine the effectiveness of individual function areas (identify, protect, detect, respond, and recover) and the overall program.

Findings and Recommendations

HRK has assessed the effectiveness of FMC information system security controls and identified weaknesses. The results of our audit identified areas in FMC's information security program that need improvement. The findings and their associated recommendations are discussed below.

Finding 1: Unauthorized and unmanaged software was installed and executed

Condition:

HRK observed, with the FMC CISO, an employee install and execute unauthorized software, including executing the Print Driver which should have been locked per the FMC CISO.

Criteria:

NIST SP 800-53, *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-3: (*FY 2024 IG FISMA Metrics Evaluation Guide*)
To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?

P-10, Asset Identification: (*NIST SP 800-37, Rev. 2*)
Identify assets that require protection.

CA-7, Continuous Monitoring: (*NIST SP 800-53, Rev. 5*)
Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics];
b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;
c. Ongoing control assessments in accordance with the continuous monitoring strategy;
d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
e. Correlation and analysis of information generated by control assessments and monitoring;
f. Response actions to address results of the analysis of control assessment and monitoring information; and
g. Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

CM-8, System Component Inventory: (*NIST SP 800-53, Rev. 5*)

a. Develop and document an inventory of system components that:
    1. Accurately reflects the system;
    2. Includes all components within the system;
    3. Does not include duplicate accounting of components or components assigned to any other system;
    4. Is at the level of granularity deemed necessary for tracking and reporting; and
    5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and
b. Review and update the system component inventory [Assignment: organization-defined frequency].

CM-10, Software Usage Restrictions: (*NIST SP 800-53, Rev. 5*)

a. Use software and associated documentation in accordance with contract agreements and copyright laws;
b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

CM-11, User Installed Software: (*NIST SP 800-53, Rev. 5*)

a. Establish [Assignment: organization-defined policies] governing the installation of software by users;
b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; and
c. Monitor policy compliance [Assignment: organization-defined frequency].

ID.AM-02, Asset Management: (*NIST CSF*)

Inventories of software, services, and systems managed by the organization are maintained.

Cause:

FMC's software usage restrictions, which restrict applications from being installed through any process other than group policies using Managed Service Identity's (MSI's) in active directory or through Intune failed to prevent an unauthorized installation and execution of software.

Effect:

Unauthorized applications may be running in FMC's environment, creating exploitable vulnerabilities.

Recommendation:

Immediate Actions:

1. Review the installed applications on all issued laptops to ensure no unauthorized software is present.
2. Review the FMC "user" setting population to ensure each "user" is properly configured in compliance with FMC's approved GPOs.
3. Review Active Directory settings to ensure unauthorized software cannot be installed, including the Print Driver settings.

Long-Term Actions:

1. Regular software audits should be scheduled on all issued laptops to ensure compliance with FMC approved software policy.
2. Security Awareness training should be provided annually to all FMC users on the risks of downloading software.
3. Security Awareness training should be provided to all network administrators on the importance of secure configuration management on user devices.

Management's Response and Our Comments:

FMC management agrees with the recommendation(s). Management has outlined planned corrective action to address the finding(s). 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: Supply Chain Risk Management (SCRM) – SCRM and C-SCRM policies have been developed by OIT but have not been performed

Condition:

FMC OIT has developed a Supply Chain Risk Management (SCRM) standard operating procedure (SOP), however it was finalized in April of 2024 and the procedures identified in the SCRM SOP have not been performed.

Criteria:

NIST SP 800-53, Rev. 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-14: (*FY 2024 IG FISMA Metrics Evaluation Guide*) To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?

IG-Metric-15: (*FY 2024 IG FISMA Metrics Evaluation Guide*) To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems? (800-53 rev 5 SR-11, 11 (1), and 11(2)?

SA-4, Acquisition Process: (*NIST SP 800-53, Rev. 5*) Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [organization defined contract language]] in the acquisition contract for the system, system component, or system service: Security and privacy functional requirements; Strength of mechanism requirements; Security and privacy assurance requirements; Controls needed to satisfy the security and privacy requirements; Security and privacy documentation requirements; Requirements for protecting security and privacy documentation; Description of the system development environment and environment in which the system is intended to operate; Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and Acceptance criteria.

SR-1, Policy and Procedures

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] supply chain risk management 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 supply chain risk management policy and the associated supply chain risk management controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and
c. Review and update the current supply chain risk management:
    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].

SR-3, Supply Chain Controls and Processes: (*NIST SP 800-53, Rev. 5*)
a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [organization-defined system or system component] in coordination with [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: [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; [organization defined document]].

SR-5, Acquisition Strategies, Tools, and Methods: (*NIST SP 800-53, Rev. 5*) Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [organization-defined acquisition strategies, contract tools, and procurement methods].

SR-6, Supplier Assessments and Reviews: (*NIST SP 800-53, Rev. 5*) Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [organization-defined frequency].

ID.SC-2, Supply Chain Risk Management: [*NIST Cybersecurity Framework (CSF) v1.1*] Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.

ID.SC-3, Supply Chain Risk Management: [*NIST Cybersecurity Framework (CSF) v1.1*] Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.

ID.SC-4, Supply Chain Risk Management: [*NIST Cybersecurity Framework (CSF) v1.1*] Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.

Cause:

FMC has developed a SCRM policy and guide, however the overall SCRM program has not been implemented.

Effect:

The identification and prioritization of suppliers of critical or mission-essential technologies, products, and services through SCRM/C-SCRM programs is paramount to the mission/business success of organizations. An analysis of supply chain risks can help an organization identify systems or components for which additional supply chain risk mitigations are required.

Failure to adopt an organization-wide SCRM and C-SCRM strategy could impact the agency's information security program and, therefore, threatens the confidentiality, integrity, & availability of FMC's information systems.

Recommendation:

We recommend that FMC:

1. Perform the procedures and associated controls identified in the SCRM SOP. The SOP lists fourteen procedures to perform.
2. During its annual review for changes to Commission Order (CO)-112, Acquisitions, include verbiage that all IT acquisitions should follow the SCRM SOP by reference.

Management's Response and Our Comments:

FMC management agrees with the recommendation(s). Management has outlined planned corrective action to address the finding(s). 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 3: Identity and Access Management (ICAM) – Non-Privileged user able to bypass multifactor authentication (MFA) to access SharePoint

Condition:

HRK observed, with the FMC CISO, a user access FMC's SharePoint without being prompted for multifactor authentication (MFA). The FMC CISO and another user, both were prompted in accordance with FMC MFA settings.

Criteria:

NIST SP 800-53, Rev. 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-30: (*FY 2023 IG FISMA Metrics Evaluation Guide*)
To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO or web authentications) for non- privileged users to access the organization`s facilities [organization-defined entry/exit points], networks, and systems, including for remote access?

AC-17, Remote Access: (*NIST SP 800-53, Rev. 5*)
a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b. Authorize each type of remote access to the system prior to allowing such connections.

IA-2, Identification and Authentication (Organizational Users): (*NIST SP 800-53, Rev. 5*)
Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

IA-5, Authenticator Management: (*NIST SP 800-53, Rev. 5*)
Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;
b. Establishing initial authenticator content for any authenticators issued by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
e. Changing default authenticators prior to first use;
f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;
g. Protecting authenticator content from unauthorized disclosure and modification;
h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and

i. Changing authenticators for group or role accounts when membership to those accounts changes.

IA-8, Identification and Authentication (Non-Organizational Users): (*NIST SP 800-53, Rev. 5*)
Control: Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

Cause:

FMC has in place an organization-wide MFA requirement for all users to be prompted for MFA when accessing applications, such as SharePoint. However, the policy requirement was not working on one of three users we observed.

Effect:

Strong authentication mechanisms, such as multifactor authentication reduce the risk of security breaches from occurring. Strong authentication mechanisms protect the data and information on commission information systems, system components, and devices, from being accessed and exploited by unauthorized individuals.

Failure to consistently implement strong authentication mechanisms for privileged and non-privileged users could impact the agency's information security program and, therefore, threatens the confidentiality, integrity, & availability of FMC's information systems.

Recommendation:

Immediate Actions:

1. Review the settings on all issued laptops to ensure MFA requirements are in place.
2. Review the FMC user setting population to ensure each user is properly configured.

Long-Term Actions:

1. Regular configuration audits should be scheduled on all issued laptops to ensure compliance with FMC MFA requirements.
2. Periodically require FMC personnel to log out and shut down laptops to ensure all requirements are being installed correctly.
3. Security Awareness training should be provided to all network administrators on the importance of secure configuration management on user devices.

Management's Response and Our Comments:

FMC management agrees with the recommendation(s). Management has outlined planned corrective action to address the finding(s). 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 4: Completion of Security Awareness Training

Condition:

HRK sampled ten FMC employees' Security Awareness Training results and found that six of ten did not complete the training.

Criteria:

NIST SP 800-53, *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-44: (*FY 2024 IG FISMA Metrics Evaluation Guide*)
To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting.)

AT-1, Policy and Procedures: (*NIST SP 800-53, Rev. 5*)

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] awareness and training 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 awareness and training policy and the associated awareness and training controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and
c. Review and update the current awareness and training:
    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].

AT-2, Literacy Training and Awareness: (*NIST SP 800-53, Rev. 5*)

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):
    1. As part of initial training for new users and [Assignment: organization-defined frequency] thereafter; and

2. When required by system changes or following [Assignment: organization-defined events];

b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques];
c. Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

PR.AT-2, Identity Management, Authentication, and Access Control: [*NIST Cybersecurity Framework (CSF) v1.1*] Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind

Cause:

Due to a vendor misconfiguration, the 2024 Security Training campaign distributed to FMC employees was incorrectly labeled as the prior year's training. Upon inspection of the evidence, six of the ten sampled FMC employees had not completed the 2024 Security Training.

Effect:

Failure to maintain a security awareness training program to influence behavior among the FMC workforce to be security conscious and properly skilled increases cybersecurity risks to the commission.

Recommendation:

HRK recommends that FMC 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.

Management's Response and Our Comments:

FMC management agrees with the recommendation(s). Management has outlined planned corrective action to address the finding(s). 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 5: FMC Has Not Met Event Logging Tiers in Accordance with OMB M-21-31

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 systems1 (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:

FMC management agrees with the recommendation(s). Management has outlined planned corrective action to address the finding(s). 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 6: Lack of Business Impact Analysis Policy, Results, and Incorporation into Contingency Planning Efforts

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-61: (*FY 2024 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) v1.1*] 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:

FMC management agrees with the recommendation(s). Management has outlined planned corrective action to address the finding(s). 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 A23-01: FISMA Recommendation No. 1:** *The FMC should develop and approve a finalized supply chain policy that adheres to the NIST 800-53 Rev. 5 requirements.*	Closed
2	**Audit A23-03 FISMA Recommendation No. 1:** All security incidents shall be reported to the U.S.-CERT within one hour of an incident being discovered.	Closed
3	**Audit A23-03 FISMA Recommendation No. 2:** FMC should develop, document, and approve a Log Retention Policy.	Open
4	**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.	Open

Appendix B – FMC Management's Response

THIS PAGE INTENTIONALLY LEFT BLANK

UNITED STATES GOVERNMENT FEDERAL MARITIME COMMISSION

Memorandum

TO: Inspector General **DATE:** July 30, 2024

FROM: Managing Director

SUBJECT: Independent Auditors' Performance Audit Report on the Federal Maritime Commission's Compliance with Federal Information Security Modernization Act for Fiscal Year 2024

I have reviewed the findings and recommendations contained in the subject audit of the Commission's information security program and practices. The Commission values the Office of the Inspector General's efforts in this critical evaluation and appreciates the recommendations for improvement.

Recommendation #1:

Immediate Actions:

1. Review the installed applications on all issued laptops to ensure no unauthorized software is present.
2. Review the FMC "user" setting population to ensure each "user" is properly configured in compliance with FMC's approved group policy objects (GPOs).
3. Review active directory settings to ensure unauthorized software cannot be installed, including the print driver settings.

Long-Term Actions:

1. Regular software audits should be scheduled on all issued laptops to ensure compliance with FMC approved software policy.
2. Security awareness training should be provided annually to all FMC users on the risks of downloading software.
3. Security awareness training should be provided to all network administrators on the importance of secure configuration management on user devices.

Comment: Management agrees with these recommendations, and will take the following steps immediately to ensure appropriate remedial action:

- OIT will review the policy that prevents the installation of applications and device drivers to ensure that it applies to all devices.
- OIT will conduct an inventory of all applications currently on FMC-issued equipment.
- OIT will ensure that all FMC users complete the mandatory bi-annual security awareness training on schedule during the 4th quarter of FY 2024.
- OIT will ensure that all members of OIT staff complete special mandatory training designed for IT professionals on schedule during the 4th quarter of FY 2024.
- OIT will conduct continuous monitoring of all devices and software present in the FMC network environment. These reports will be reviewed weekly by the Chief Information Security Officer.

Recommendation #2: We recommend that FMC:

1. Perform the procedures and associated controls identified in the supply chain risk management standard operating procedure (SCRM SOP). The SOP lists fourteen procedures to perform.
2. During its annual review for changes to Commission Order 112, *Acquisitions*, include directive that all IT acquisitions must follow the SCRM SOP by reference.

Comment: Management agrees with these recommendations, and will take the following steps to ensure appropriate remedial action:

- OIT will ensure that the procedures outlined in the SCRM SOP are implemented and followed by the end of the 2nd quarter of FY 2025.
- During the annual review process for Commission Order 112, OIT will coordinate with the Office of the Managing Director to add the directive that all IT acquisitions should follow the SCRM SOP.

Recommendation #3:

Immediate Actions:

1. Review the settings on all issued laptops to ensure multifactor authentication (MFA) requirements are in place.
2. Review the FMC user setting population to ensure each user is properly configured.

Long-Term Actions:

1. Regular configuration audits should be scheduled on all issued laptops to ensure compliance with FMC MFA requirements.
2. Periodically require FMC personnel to log out and shut down laptops to ensure all requirements are being installed correctly.

3. Security awareness training should be provided to all network administrators on the importance of secure configuration management on user devices.

Comment: Management agrees with these recommendations, and will take the following steps to ensure appropriate remedial action by the end of the 2nd quarter of FY 2025:

- OIT will conduct a thorough review of the multi-factor authentication policy to ensure that it applies to all users who access the Microsoft O365/ SharePoint services.
- OIT has implemented certificate-based authentication for FMC-issued equipment through Intune.
- OIT will configure all FMC-issued laptops to perform a system reboot every 7 days to ensure authentication tokens are renewed.
- OIT will ensure that all members of OIT staff complete on schedule mandatory special training designed for IT professionals where the importance of secure configuration management is stressed.

Recommendation #4: HRK recommends that FMC 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.

Comment: Management agrees with this recommendation, and will take the following steps to ensure appropriate remedial action:

- OIT will work with the vendor to properly setup the training application and will initiate the security awareness training (SAT) process on a bi-annual basis for all FMC users.
- OIT will work with senior management to ensure timely completion of SAT.
- OIT will ensure that all members of OIT staff complete on schedule mandatory special training designed for IT professionals where the importance of secure configuration management is stressed.

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 agrees with these recommendations. OIT is in the process of developing a logging strategy by which the event logging 3 (EL3) logging requirement outlined in OMB M-21-31 will be met. OIT anticipates the EL3 requirement will be met by the end of the 2nd quarter of FY 2025.

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 agrees with these recommendations. OIT will coordinate with the Office of the Managing Director to facilitate the development of BIAs that provide the hierarchy of FMC applications and business systems and the recovery strategies to be implemented to ensure operational resilience and continuity of operations during and after a potential business disruption.

OIT anticipates this process will be completed by the end of the 2nd quarter of FY 2025.

Status of Prior Year Remaining Open Recommendations

Audit A23-03 FISMA

Recommendation #2: FMC should develop, document, and approve a log retention policy.

Comment: A log retention policy is currently in development and will be completed by the end of the 1st quarter of FY 2025.

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: A risk assessment policy is currently in development and will be completed by the end of the 1st quarter of FY 2025.

Lucille L. Marvin

cc: Office of the Chairman
Office of Information Technology
Office of Management Services