FEDERAL MARITIME COMMISSION

OFFICE OF INSPECTOR GENERAL

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

Fiscal Year 2020

Report No. A21-02

FINAL

TABLE OF CONTENTS

PURPOSE

Dembo Jones (contractor), on behalf of the Federal Maritime Commission (FMC), Office of Inspector General (OIG), conducted an independent audit of the quality and compliance of the FMC's information security program with applicable federal computer security laws and regulations. Dembo Jones' audit focused on FMC's information security program as required by the Federal Information Security Modernization Act (FISMA), as amended. This report was prepared by the contractor with guidance by the OIG.

BACKGROUND

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies in the executive branch to develop, document, and implement an information security program to provide information security for the information and information systems that support the operations and assets for the agency.[1] FISMA is supported by security policy promulgated through the Office of Management and Budget (OMB), and risk-based standards and guidelines published in the National Institute of Standards and Technology (NIST), Special Publication (SP) series.

FISMA assigns specific responsibilities to agency heads and Inspectors General (IGs). Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems. FISMA requires agencies to have an annual independent review performed on their information security programs and practices and to report the results to OMB. FISMA states that the independent review is to be performed by the agency IG or an independent external auditor as determined by the IG. Implementing adequate information security controls is essential to ensuring an organization can effectively meet its mission.

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 L. No. 113-283, Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub.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

SCOPE AND METHODOLOGY

We conducted this audit in accordance with generally accepted government auditing standards, issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions, based on our audit objectives.

The scope of our testing focused on the FMC General Support Systems (GSS) and Major Applications. We conducted our testing through inquiry of FMC personnel, inspection of relevant documentation, and the performance of technical security testing. More specifically, our testing covered a sample of controls as listed in NIST 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4[2]. For example, testing covered system security plans, access controls, risk assessments, personnel security, contingency planning, identification / authentication and auditing. Our testing was for the period October 1, 2019 through September 30, 2020 (fiscal year 2020).

NIST 800-53, Rev. 4, has several families and controls within those families. The number of controls will vary depending on the security categorization of the respective system (e.g. Low, Moderate, and High), as well as the control enhancements. For purposes of this FISMA engagement, the scope of our testing included the following controls:

Table 1

Family	Controls
Access Control (AC)	AC-1, AC-2, AC-5, AC-6, AC-8, AC-11, AC-12, AC-17, AC-19
Awareness and Training (AT)	AT-1, AT-2, AT-3, AT-4
Audit and Accountability (AU)	AU-2, AU-3, AU-6
Security Assessment and Authorization (CA)	CA-1, CA-2, CA-3, CA-5, CA-6, CA-7
Configuration Management (CM)	CM-1, CM-2, CM-3, CM-4, CM-6, CM-7, CM-8, CM-9, CM-10
Contingency Planning (CP)	CP-1, CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, CP-9

[2] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

Family	Controls
Identification and Authentication (IA)	IA-1, IA-2, IA-4, IA-5, IA-7, IA-8
Incident Response (IR)	IR-1, IR-4, IR-6, IR-7
Media Protection (MP)	MP-3, MP-6
Planning (PL)	PL-2, PL-4, PL-8
Program Management (PM)	PM-5, PM-7, PM-8, PM-9, PM-11
Personnel Security (PS)	PS-1, PS-2, PS-3, PS-6
Risk Assessment (RA)	RA-1, RA-2, RA-5
System and Services Acquisition (SA)	SA-3, SA-4, SA-8, SA-9
System and Communications Protection (SC)	SC-7, SC-8, SC-10, SC-13, SC-18, SC-28
System and Information Integrity (SI)	SI-2, SI-3, SI-4, SI-7

INTERNAL CONTROLS

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

CURRENT YEAR FINDING

01 Policies and Procedures

Condition:
Although the FMC has various information technology security policies and procedures, several had not been updated / reviewed in a timely manner, or they were lacking from development into a formalized policy. Specifically, the following was noted:

NIST Control	Deficiency
Risk Assessment Policy and Procedures (RA-1)	Risk policies and procedures have not been formalized, reviewed and approved.
System Development Life Cycle (SA-3)	FMC does not contain a formalized and approved Software Development Life Cycle (SDLC) policy.
Personnel Security Policy and Procedures (PS-1)	FMC's Personnel Security policy has not been updated/finalized in the last three years.
Security Assessment and Authorization Policies and Procedures (CA-1)	FMC's Security Assessment policy was last reviewed and updated in 2011.
Configuration Management Policy and Procedures (CM-1)	The Configuration Management policy was last updated in 2018, however, this policy was not signed as evidence of approval.
Configuration Management Plan (CM-9)	There is currently no Configuration Management Plan in place at the FMC.
Security Awareness and Training Policy and Procedures (AT-1)	The Security Awareness policy was last updated in 2017, however this policy was not reviewed within the last three years.
Identification and Authentication Policy and Procedures (IA-1)	Identification and Authentication policies were last reviewed and updated in 2017.
Access Control Policy and Procedures (AC-1)	Access policies were last reviewed and updated in 2017.
System and Services Acquisition Policy and Procedures (SA-1) & Acquisition Process (SA-4)	Update the Acquisition policy to ensure that it contains stipulations that require external service providers meet or exceed the NIST security requirements.

Criteria:
NIST 800-53, Revision 4, Risk Assessment Policy and Procedures (RA-1) states:
"The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
b. Reviews and updates the current:
   1. Risk assessment policy [*Assignment: organization-defined frequency*]; and
   2. Risk assessment procedures [*Assignment: organization-defined frequency*]."

NIST 800-53, Revision 4, System Development Lifecycle (SA-3) states:
"The organization:

1. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations;
2. Defines and documents information security roles and responsibilities throughout the system development life cycle;
3. Identifies individuals having information security roles and responsibilities; and
4. Integrates the organizational information security risk management process into system development life cycle activities."

NIST 800-53, Revision 4, Personnel Security Policy (PS-1) states:
"The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
b. Reviews and updates the current:
   1. Personnel security policy [Assignment: organization-defined frequency]; and
   2. Personnel security procedures [Assignment: organization-defined frequency]."

NIST 800-53, Revision 4, Security Assessment and Authorization Policy (CA-1) states:
"The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
b. Reviews and updates the current:
   1. Security assessment and authorization policy [Assignment: organization-defined frequency]; and
   2. Security assessment and authorization procedures [Assignment: organization-defined frequency]."

NIST 800-53, Revision 4, Configuration Management Policy and Procedures (CM-1) states:
"The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and

b. Reviews and updates the current:
    1. Configuration management policy [Assignment: organization-defined frequency]; and
    2. Configuration management procedures [Assignment: organization-defined frequency]."

NIST 800-53, Revision 4, Configuration Management Plan (CM-9) states:
"The organization develops, documents, and implements a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c. Defines the configuration items for the information system and places the configuration items under configuration management; and
d. Protects the configuration management plan from unauthorized disclosure and modification."

NIST 800-53, Revision 4, Security Awareness and Training Policy and Procedures (AT-1) states:
"The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
    1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
b. Reviews and updates the current:
    1. Security awareness and training policy [Assignment: organization-defined frequency]; and
    2. Security awareness and training procedures [Assignment: organization-defined frequency]."

NIST 800-53, Revision 4, Identification and Authentication Policy and Procedures (IA-1) states:
"The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
    1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
b. Reviews and updates the current:
    1. Identification and authentication policy [Assignment: organization-defined frequency]; and
    2. Identification and authentication procedures [Assignment: organization-defined frequency]."

NIST 800-53, Revision 4, Access Control Policy and Procedures (AC-1) states:
"The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
    1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:
   1. Access control policy [Assignment: organization-defined frequency]; and
   2. Access control procedures [Assignment: organization-defined frequency]."

NIST 800-53, Revision 4, System and Services Acquisition Policy and Procedures (SA-1) states:
"The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and
b. Reviews and updates the current:
   1. System and services acquisition policy [Assignment: organization-defined frequency]; and
   2. System and services acquisition procedures [Assignment: organization-defined frequency]."

NIST 800-53, Revision 4, Acquisition Process (SA-4) states:
"The organization:

a. Includes the following requirements, descriptions, and criteria, either explicitly or by reference, in information system acquisition contracts based on applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:
   1. Security functional requirements;
   2. Security strength requirements;
   3. Security assurance requirements;
   4. Security-related documentation requirements;
   5. Description of the information system development environment and environment in which the system is intended to operate; and
   6. Acceptance criteria."

Cause:
Due to time constraints, FMC did not adequately review and/or update as well ensure they have appropriate policies and procedures in accordance with NIST 800-53, Revision 4.

Effect:
Without finalized policies and procedures, there is an increased risk that IT staff will be unaware of the requirements when deploying and designing security controls.

Recommendations:

1. The Office of Information Technology (OIT) should develop, review and update, as necessary, the following information security program policies and procedures in accordance with NIST and agency requirements:

   a. Risk policies and procedures.
   b. System Development Life Cycle (SDLC) policy.
   c. Personnel Security policy.

d. Security Assessment policy.
e. Configuration Management Policy.
f. Configuration Management Plan.
g. Security Awareness policy.
h. Identification and Authentication policy.
i. Access policy.

2. The Office of Management Services (OMS) should update the Acquisition policy to ensure it contains the necessary requirements, as stated in SA-4 from NIST 800-53 (Rev. 4).

Management Response:

Recommendation #1: Management agrees with this recommendation. It is anticipated that these policies will be reviewed and updated, as necessary, by the end of the 2nd quarter of FY 2021. Going forward, the policies will be reviewed every three years and updated as needed.

Recommendation #2: Management agrees with this recommendation. Commission Order 112, *Acquisitions*, will be updated to include the necessary requirements, as stated in SA-4 from NIST 800-53 (Rev.4). It is anticipated that this will be completed by the end of the 2nd quarter of FY 2021.

STATUS OF PRIOR YEAR RECOMMENDATIONS

#	Recommendation	Report	Open / Closed
1	FMC should remediate vulnerabilities in a timely manner consistent with agency policy and guidance from the Department of Homeland Security.	Report A20-03 (#1)	Closed
2	All contractors should be recertified on an annual basis for regular end-users, and semi-annually for administrator users.	Report A20-03 (#3)	Closed

UNITED STATES GOVERNMENT FEDERAL MARITIME COMMISSION

Memorandum

TO : Inspector General **DATE:** October 29, 2020

FROM : Managing Director

SUBJECT : Audit of the FMC's Compliance with the Federal Information Security Modernization Act, Fiscal Year 2020

I have reviewed the findings and recommendations contained in the subject audit. Management appreciates the Inspector General's efforts in reviewing the quality and compliance of the Commission's information security program with applicable federal computer security laws and regulations. We welcome the recommendations for improvement, and note that all recommendations from prior years have been closed.

Recommendation #1: The Office of Information Technology (OIT) should develop, review and update, as necessary, the following information security program policies and procedures in accordance with NIST and agency requirements:

a. Risk policies and procedures
b. System Development Life Cycle (SDLC) policy
c. Personnel Security policy
d. Security Assessment policy
e. Configuration Management Policy
f. Configuration Management Plan
g. Security Awareness policy
h. Identification and Authentication policy
i. Access policy

Comment: Management agrees with this recommendation. It is anticipated that these policies will be reviewed and updated, as necessary, by the end of the 2nd quarter of FY 2021. Going forward, the policies will be reviewed every three years and updated as needed.

Recommendation #2: The Office of Management Services (OMS) should update the Acquisition policy to ensure it contains the necessary requirements, as stated in SA-4 from NIST 800-53 (Rev. 4).

Comment: Management agrees with this recommendation. Commission Order 112, *Acquisitions*, will be updated to include the necessary requirements, as stated in SA-4 from NIST 800-53 (Rev.4). It is anticipated that this will be completed by the end of the 2nd quarter of FY 2021.

KAREN GREGORY
Digitally signed by KAREN GREGORY
Date: 2020.10.29 10:16:10 -04'00'

Karen V. Gregory

cc: Office of the Chairman

APPENDIX A

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

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