FEDERAL MARITIME COMMISSION

OFFICE OF INSPECTOR GENERAL

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

Fiscal Year 2021
FINAL REPORT

Report No. A22-02

FEDERAL MARITIME COMMISSION
Washington, DC 20573

October 28, 2021

Office of Inspector General

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

Please find enclosed the Office of Inspector General's (OIG) report for the *Fiscal Year 2021 Audit of the FMC's Compliance with the Federal Information Security Modernization Act (FISMA)*. The OIG relied on the expertise of an information security evaluator from *Dembo Jones PC* for assistance on this mandated review.

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

The results of the OIG's FISMA audit found the FMC resolved one of the prior year audit recommendations and made progress towards implementing the other audit recommendation. In addition, this year's audit includes one new audit recommendation for a weakness that existed during FY 2021. FMC management reported the weakness has been addressed as of October 27, 2021.

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

Respectfully submitted,

Jon Hatfield
Inspector General

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

TABLE OF CONTENTS

Contents

PURPOSE

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

BACKGROUND

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

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

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

SCOPE AND METHODOLOGY

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

The scope of our testing focused on the FMC General Support Systems (GSS) and major applications. We conducted our testing through inquiry of FMC personnel, inspection of relevant documentation, and the performance of technical security testing. More specifically, our testing covered a sample of controls as listed in NIST 800-53, Security and Privacy Controls for 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, 2020 through September 30, 2021 (fiscal year 2021).

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, IR-8
Media Protection (MP)	MP-3, MP-6
Planning (PL)	PL-4, PL-8
Program Management (PM)	PM-5, PM-7, PM-8, PM-9, PM-11, PM-30
Personnel Security (PS)	PS-1, PS-2, PS-3, PS-6
Physical and Environmental (PE)	PE-3
Risk Assessment (RA)	RA-1, RA-2, RA-3, RA-5
Supply Chain Risk Management (SR)	SR-1, SR-3, SR-5, SR-6, SR-11
System and Services Acquisition (SA)	SA-3, SA-4, SA-8, SA-9, SA-12
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
Privacy Controls (AR, SE)	AR-4, AR-5, SE-2

INTERNAL CONTROLS

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

CURRENT YEAR FINDING

01 Complexity Settings

A minimum password age policy determines the period of time (in days) that a password can be used before the system requires the user to change it. The minimum password age policy (one day or greater), used in conjunction with the enforce password history policy, is helpful to prevent users from reusing their current password, thereby increasing computer security.

Condition:
Upon review of the password complexity settings, it was revealed that the minimum day password setting was set to “0”. Setting the number of days to “0” allows immediate password changes, which is not recommended.

Criteria:
<u>NIST 800-53, Revision 4, Identification and Authentication (IA-5), states:</u>
“The organization manages information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators defined 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/compromised or damaged authenticators, and for revoking authenticators;
e. Changing default content of authenticators prior to information system installation;
f. *<u>Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;</u>*
g. Changing/refreshing authenticators;
h. Protecting authenticator content from unauthorized disclosure and modification;
i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
j. Changing authenticators for group/role accounts when membership to those accounts changes.”

Cause:
The cause is primarily because of a lack of personnel, budget, or time constraints to adequately document and/or assess all of the controls in NIST 800-53, Revision 4.

Risk:
Without maintaining at least a minimum password setting of “1”, the respective users can change their passwords at will until such time as arriving at their original password and avoiding the password expiration setting.

Recommendation:

1. Passwords should have a minimum password age policy setting of at least “1” day.

Management Response:
Management agrees with this recommendation. The password age policy setting was changed to “1” as of October 27, 2021.

STATUS OF PRIOR YEAR RECOMMENDATIONS

#	Recommendation	Report	Open / Closed
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.	A21-02	**Open** a. Open b. Open c. Closed d. Open e. Open f. Open g. Closed h. Closed i. Open
	Management Response: Management agreed that, going forward, these policies and procedures will be reviewed every three years and updated as needed. Progress on the review and update of these nine policies and procedures is shown in Appendix B below. It is anticipated that the work in progress will be completed by the end of the 2nd quarter of FY 2022.		
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).	A21-02	**Closed**

APPENDIX A

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

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.	✓
<u>Monitoring</u>	
14. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.	✓
15. Management should remediate identified internal control deficiencies on a timely basis.	✓

APPENDIX B

UNITED STATES GOVERNMENT FEDERAL MARITIME COMMISSION

Memorandum

TO : Inspector General **DATE:** October 28, 2021

FROM : Managing Director

SUBJECT : Audit of the FMC's Compliance with the Federal Information Security Modernization Act, Fiscal Year 2021

I have reviewed the findings and recommendation 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 one prior year recommendation has been closed.

Recommendation #1: Passwords should have a minimum password age policy setting of at least "1" day.

Comment: Management agrees with this recommendation. The password age policy setting was changed to "1" as of October 27, 2021.

Prior Year Recommendation

A21-02, Audit of the FMC's Compliance with the Federal Information Security Modernization Act FY 2020

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 agreed that, going forward, these policies and procedures will be reviewed every three years and updated as needed. Progress on the review and update of these nine policies and procedures is shown in the table below. It is anticipated that the work in progress will be completed by the end of the 2nd quarter of FY 2022.

	Completed and Accepted	**Completed, Awaiting Review in FISMA FY22**	**Work in Progress**
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			✓

Lucille L.
Marvin

Digitally signed by Lucille
L. Marvin
Date: 2021.10.27
21:04:55 -04'00'

Lucille L. Marvin

cc: Office of the Chairman