Office of Inspector General

Information Technology Vulnerability Audit, 2023

A23-04

September 2023

FEDERAL MARITIME COMMISSION

FEDERAL MARITIME COMMISSION
Washington, DC 20573

September 28, 2023

Office of Inspector General

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

Please find enclosed the Office of Inspector General's (OIG) *Information Technology Vulnerability Audit* (ITVA). The OIG relied on the expertise of information security specialists from *FYRM Associates, Inc.* an approved subcontractor of *Dembo Jones P.C.* to perform this audit.

The objectives of this audit were to evaluate the FMC external and internal network segments, systems, and applications to assess the FMC's IT vulnerability assessment program and identify any critical security IT weaknesses. The scope of the ITVA included multiple FMC Network targets within the external and internal network environments.

The testing team simulated an outside attacker, gathered publicly available information about the target environment, and attempted to gain unauthorized access to FMC systems within the scope of testing. The simulated external attack scenario did not lead to unauthorized access within the testing timeframe.

The results of the OIG's ITVA audit identified multiple vulnerabilities in FMC IT systems and applications. [redacted] Eight recommendations are provided to address four findings. FMC management agreed with all eight 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,

Jon Hatfield
Inspector General

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

Table of Contents

REPORT HIGHLIGHTS

Federal Maritime Commission
Office of Inspector General (OIG)

REPORT HIGHLIGHTS

The OIG Recommends the FMC Enhance Policies and Procedures to Ensure the Confidentiality, Integrity, and Availability of Information Systems and Data in Support of the Agency's Mission

(Audit A23-04, September 2023)

Why We Did This Audit

The Federal Information Security Modernization Act of 2014 (FISMA 2014) requires Federal agencies to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency. As part of the FISMA requirements, Federal agencies must meet the minimum-security requirements by selecting the appropriate security controls and assurance requirements as described in National Institute of Standards and Technology Special Publication 800-53, "Recommended Security Controls for Federal Information Systems".

Background

The FMC is highly dependent on IT systems and electronic data to carry out agency operations and to process, maintain, and report essential information. Therefore, the security of these systems and data is vital to ensure the confidentiality, integrity, and availability of FMC systems and information. Risks to the FMC's IT systems can include insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, and new and more destructive attacks.

What We Found

The scope of our testing encompassed the FMC's IT systems and IT security. More specifically, our testing included security testing of multiple FMC Network targets within the external (Internet-facing) and internal network environments. Our testing was for the period June 20, 2023 through September 7, 2023. Specific details for the targets and target environment were provided by FMC personnel to the testing team prior to the commencement of testing.

The OIG employed two testing scenarios that were intended to provide real world examples of what a knowledgeable and motivated hacker could achieve if focused on the FMC.

- Red Team External Attack - The testing team simulated an outside attacker, gathered publicly available information about the target environment, and attempted to gain unauthorized access to FMC systems within the scope of testing.
- Red Team Internal Attack - The testing team simulated both a malicious insider and an outside attacker that had gained access to an internal system (for example, via phishing against an authorized user), gathered information about the target environment, and attempted to gain unauthorized access to FMC systems within the scope of testing.

Multiple vulnerabilities were identified in FMC IT systems and applications. [redacted] Eight (8) recommendations are provided to address four (4) findings.

Findings

1. Insufficient software management.
2. Default authentication credentials are utilized.
3. Insufficient configuration management.
4. Flaws in custom-developed application functionality.

INFORMATION TECHNOLOGY VULNERABILITY AUDIT, 2023

PURPOSE

Dembo Jones, PC, CPAs & Advisors (Dembo, Contractor), and their approved subcontractor FYRM Associates, Inc. (FYRM, Contractor), on behalf of the Federal Maritime Commission (FMC), Office of the Inspector General (OIG), conducted an independent audit of the FMC's information technology (IT) vulnerability assessment program to identify any critical IT security weaknesses. This report was prepared by the contractor with guidance by the OIG.

BACKGROUND

The FMC is highly dependent on IT systems and electronic data to carry out agency operations and to process, maintain, and report essential information. Therefore, the security of these systems and data is vital to ensure the confidentiality, integrity, and availability of FMC systems and information. Risks to the FMC's IT systems can include insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, and new and more destructive attacks.

The FMC Network is designed to facilitate the services and resources needed to support FMC operations and FMC's end user community. Further, the purpose of the FMC Network is to provide FMC employees and/or contractors access to the FMC domain, E-mail account management, interconnection(s) between all FMC end users and the Internet, as well as provide access to agency applications.

Prior to testing, the FMC, the OIG, and Contractors (the "parties") developed a Rules of Engagement (ROE) that outlined details of the testing objectives, scope, and methodology by defining targets, time frame, rules, reporting, points of contact, and additional aspects of the engagement. The ROE was utilized to ensure testing procedures were performed in a manner that was transparent to all parties and minimized the potential for negative operational impact.

OBJECTIVES, 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 full version of this report contains information that is not appropriate for public release under applicable law. To create the public version of the report, the Office of Inspector General redacted (blacked out) portions of the full report.

Scope

The scope of our testing encompassed the FMC's IT systems and IT security. More specifically, our testing included covert security testing of multiple FMC Network targets[1] within the external (Internet-facing) and internal network environments. Our testing was for the period June 20, 2023 through September 7, 2023. Specific details for the targets and target environment were provided by FMC personnel to the testing team prior to the commencement of testing. The following information was requested from FMC to expedite testing:

- Internet protocol (IP) address ranges for in-scope network segments (external and internal);
- Uniform Resource Locators (URLs) or other relevant information for specific target applications; and
- IP addresses, URLs, and other relevant information for systems requiring special attention during testing (e.g., systems that could become unresponsive in response to specific tests).

Specifically, the following items listed in Table 1 were provided by FMC and were considered in-scope for our testing:

Table 1: Scope information provided by FMC

Scope Information Type	Details
IP Addresses External / Internet-facing	[redacted]
IP Addresses Internal	[redacted]
Domains External and Internal	[redacted]

[1] For this engagement, a target refers to any IT system or device, such as servers and web applications, that is used by FMC to perform its mission and stores, transmits, or manages data. Such systems or devices may be the target of cyber security attacks by malicious entities.

Scope Information Type	Details
Web Applications (Base URLs)	[redacted]

The FMC major applications that were in scope for our testing are described in Table 2 below.

Table 2: In scope major applications

Application Name	Description
Form 1 ("Automated Tariff Registration System")	Allows users to add or to make changes to their tariff registrations. Form 1 uses SMTP to email customers regarding their accounts and registration forms. The Message Center is also used to track correspondence between users and the FMC.
Form 18 / FMC-18	New Ocean Transportation Intermediary license applications are the most frequently submitted application type and consist of requests for Non-vessel operating common carrier (NVOCC) authority and/or Ocean Freight Forwarder authority. The FMC requires applicants to submit an electronic FMC-18.
FMC-65	Renewal System for foreign-based unlicensed NVOCCs, also known as Foreign-registered NVOCCs or Registered NVOCCs.
BCLFileroom	Document storage supporting other applications, including FMC-18 and Ocean Transportation Intermediaries (OTIs) renewals.
eMonitoring (previously "eFile")	This is an application allowing users to file Quarterly Monitoring Reports (QMRs), Meeting Minutes, and Voluntary Service Contract Guidelines.
OTI Renewals	In accordance with the Commission's rules at 46 CFR 515.14, licensed OTIs are required every three years to update (renew) their license. All triennial updates must be submitted through the Commission's on-line Triennial License Update System.
eAgreements (previously "FMCAgreements")	This is an application allowing agreement administers to file QMRs, Meeting Minutes, and Voluntary Service Contract Guidelines.
RPI	The Regulated Persons Index (RPI) contains general information on all persons regulated by the FMC. This is a SQL server database system that contains a profile of each regulated person and a unique identifier (RPI number/Organization Number).

Application Name	Description
SERVCON	SERVCON is the Federal Maritime Commission's internet-based filing system for ocean common carrier service contracts and non-vessel-operating common carrier service arrangements (NSAs), maintained by FMC.

Methodology

The testing methodology was designed to identify potential security vulnerabilities in an efficient manner that minimized negative operational impact. The specific testing methodology and procedures for each testing scenario described below are based on the following general phases:

- System Reconnaissance - The testing team performed reconnaissance testing procedures to gather relevant technical information about the target(s) and target environment as well as defensive security systems within the target environment. This phase included the use of automated scanning tools and manual techniques. The information obtained during this phase was analyzed to complete the following steps:
    - Adjust the scope of the assessment to either include or exclude certain network segments, systems, and applications;
    - Develop a prioritized target profile to include specific primary and secondary targets;
    - Identify technical strengths and weaknesses within the target environment; and
    - Determine the appropriate testing tools, techniques, and approach to be utilized during the Vulnerability Identification phase.
- Vulnerability Identification - The testing team utilized automated scanning tools and manual testing techniques to identify vulnerabilities and weaknesses within the system environment. Automated scanning tool configurations were customized as needed based on the information obtained during the System Reconnaissance phase.
- Validation & Risk Analysis - Based on the results of the Vulnerability Identification phase, the testing team attempted to exploit certain vulnerabilities according to the Vulnerability Exploitation methodology described below. The results of the exploitation procedures and additional information obtained during the assessment were included in the analysis of risk (high, medium, low) associated with each identified vulnerability and across the scope of the assessment. For example, an unsuccessful exploitation attempt may indicate that a

vulnerability was falsely identified by scanning tools, referred to as a "false positive", for which the vulnerability would not be included in the report. A successful exploitation attempt that enables the testing team to compromise sensitive data or obtain unauthorized access to additional systems and applications may increase the risk rating since the impact was not fully known prior to the attempt.

Vulnerability Exploitation

During the Information Technology Vulnerability Audit (ITVA), the testing team attempted to exploit certain vulnerabilities identified within the target environment to validate the results obtained during the Vulnerability Identification testing phase and to assist in the analysis of risk associated with the selected vulnerabilities. During the exploitation process, the testing team attempted to perform the following actions:

- Obtain unauthorized access to systems, data, or functionality;
- Increase access privileges to the affected systems(s) containing the exploited vulnerability;
- Obtain unauthorized access to additional systems, data, or functionality beyond the affected systems(s) by utilizing existing trust relationships; and
- Identify additional vulnerabilities and weaknesses within the system environment.

The exploitation process varied based on the potential for negative operational impact, such as service disruption or unintended data changes, that may occur because of either successful or unsuccessful exploitation attempts. The testing team immediately attempted to exploit vulnerabilities that are known to not cause system instability or have other negative operational impact. Examples of such vulnerabilities include network file shares that could be viewed or modified by anyone and weak login credentials.

For exploits that may cause system instability or have other negative operational impact, the testing team performed the following steps to coordinate such exploitation attempts with all appropriate parties and personnel:

1. Create an exploitation test plan that describes details of each vulnerability, exploit to be used, affected target system(s), and expected result of successful exploitation for each selected vulnerability.
2. Discuss the exploitation test plan with FMC points of contact, system administrators, and additional personnel representing the OIG, Dembo, and FMC as needed.
3. Determine an appropriate timeframe to attempt exploitation.

4. Execute the exploitation test plan and perform necessary clean up procedures following successful exploitation.

Evidence of successful exploits were obtained by the testing team and maintained along with all other test data and evidence obtained during the audit. All test files, temporary user accounts, and other byproducts of exploitation procedures were documented prior to completing the exploitation process. None of these artifacts were removed either due to inability or uncertainty of performing a safe removal with no impact to the affected systems.

Testing Scenarios

The ITVA included the following scenarios that are intended to provide real world examples of what a knowledgeable and motivated hacker could achieve if focused on the FMC.

- Red Team External Attack - The testing team simulated an outside attacker, gathered publicly available information about the target environment, and attempted to gain unauthorized access to FMC systems within the scope of testing. If access was obtained[2], then the testing team would have attempted to pivot and gain unauthorized access to additional systems, including those not directly accessible via the Internet.
- Red Team Internal Attack - The testing team simulated both a malicious insider and an outside attacker that has gained access to an internal system (for example, via phishing against an authorized user), gathered information about the target environment, and attempted to gain unauthorized access to FMC systems within the scope of testing.

RESULTS

Red Team External Simulated Attack

During the Red Team External Attack testing scenario, we performed a combination of manual and automated testing to evaluate the current security posture of the in-scope Internet-facing IT environment, including any accessible servers, web applications, other services, and network infrastructure.

[2] The issues identified during testing for the External Attack scenario did not lead to unauthorized access within the testing timeframe.

External Vulnerabilities

During the Red Team External Attack testing scenario, we identified four (4) types of vulnerabilities, which included two (2) Medium risk and two (2) Low risk, totaling sixteen (16) instances of these vulnerabilities across systems within the in-scope environment. [redacted]

Table 3: External Vulnerabilities

Control Area	Vulnerability Name	Risk Rating
[redacted]	[redacted]	Medium
		Medium
[redacted]		Low
		Low

Details for the identified vulnerabilities were provided to FMC to request feedback and to facilitate remediation and risk mitigation efforts.

External Simulated Attack Vectors

Based on the results of the Red Team External Attack testing scenario, we did not identify vulnerabilities that could be exploited to immediately obtain unauthorized access to additional systems or data without targeting users, potentially causing service disruption, or requiring significant effort to create custom exploit code. [redacted]

Red Team Internal Simulated Attack

During the Red Team Internal Attack testing scenario, we performed a combination of manual and automated testing to evaluate the current security posture of the in-scope systems, web applications, and network infrastructure. For the web applications, we performed both unauthenticated and authenticated testing utilizing test accounts with varying levels of access to simulate FMC personnel and their external client personnel.

As part of the authenticated web application testing and with support from FMC, we created two test (fake) organizations within the application suite, beginning with "Automated Tariff Registration System" (Form 1), to minimize the likelihood that our testing may impact other organizations already defined within the environment. An additional test account for each test organization was created to facilitate the process and our testing. A summary of these accounts and organizations is listed in Table 4 and Table 5 below.

Table 4: External client test account and organization 1

Field	Value
Username	[redacted]
Email	
Company Name	
Comments	

Table 5: External client test account and organization 2

Field	Value
Username	[redacted]
Email	
Company Name	
Comments	

We performed a limited subset of authentication testing against the web applications due to testing being conducted within the production environment (a sufficient non-production environment was not available) and additional coordination time to create the test accounts and organizations.

Internal Vulnerabilities

During the Red Team Internal Attack testing scenario, we separately reported vulnerabilities identified during the unauthenticated network-based testing from those identified during the unauthenticated and authenticated web application testing. For the network-based testing, we identified twenty-two (22) types of vulnerabilities--seven (7) High risk, seven (7) Medium risk, seven (7) Low risk, and one (1) Informational risk--with a total of eight hundred six (806) instances across systems within the in-scope environment. [redacted]

Table 6: Internal Network-Based Vulnerabilities

Control Area	Vulnerability Name	Risk Rating
[redacted]	[redacted]	High
[redacted]	[redacted]	High
[redacted]	[redacted]	High
[redacted]	[redacted]	High
[redacted]	[redacted]	High
[redacted]	[redacted]	High
[redacted]	[redacted]	High
[redacted]	[redacted]	Medium
[redacted]	[redacted]	Medium
[redacted]	[redacted]	Medium
[redacted]	[redacted]	Medium
[redacted]	[redacted]	Medium
[redacted]	[redacted]	Medium
[redacted]	[redacted]	Medium
[redacted]	[redacted]	Low
[redacted]	[redacted]	Low
[redacted]	[redacted]	Low
[redacted]	[redacted]	Low
[redacted]	[redacted]	Low
[redacted]	[redacted]	Low
[redacted]	[redacted]	Low
[redacted]	[redacted]	Informational

For the application testing, we identified five (5) types of vulnerabilities--one (1) High risk, two (2) Medium risk, and two (2) Low risk--with a total of sixty-three (63) instances across the applications within the in-scope environment. [redacted]

Table 7: Internal Application Vulnerabilities

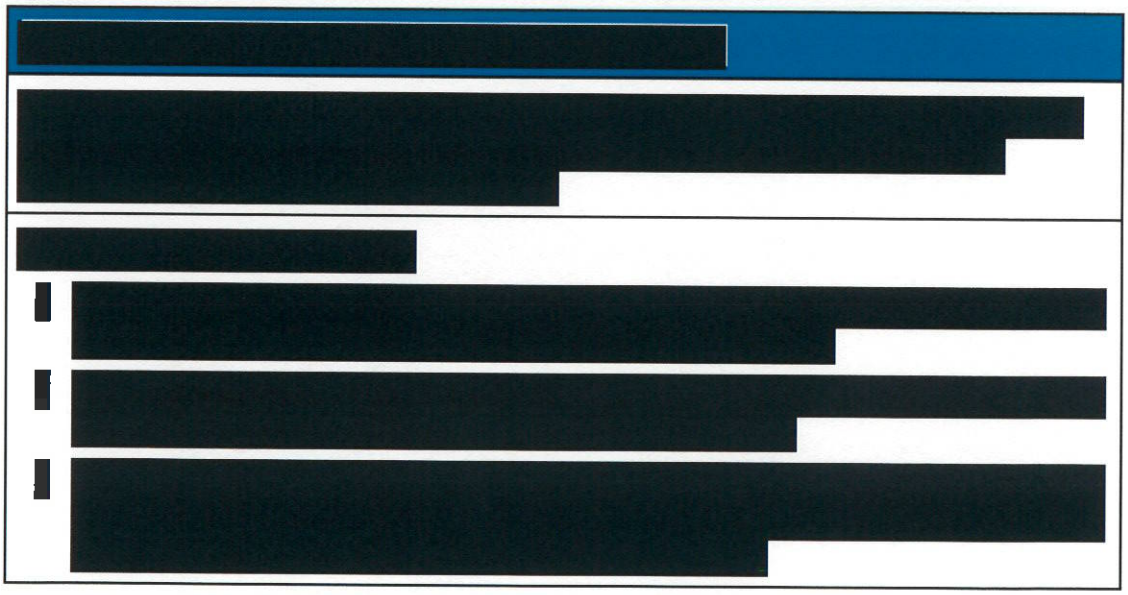
Control Area	Vulnerability Name	Risk Rating
[redacted]	[redacted]	High
	[redacted]	Medium
		Medium
		Low
		Low

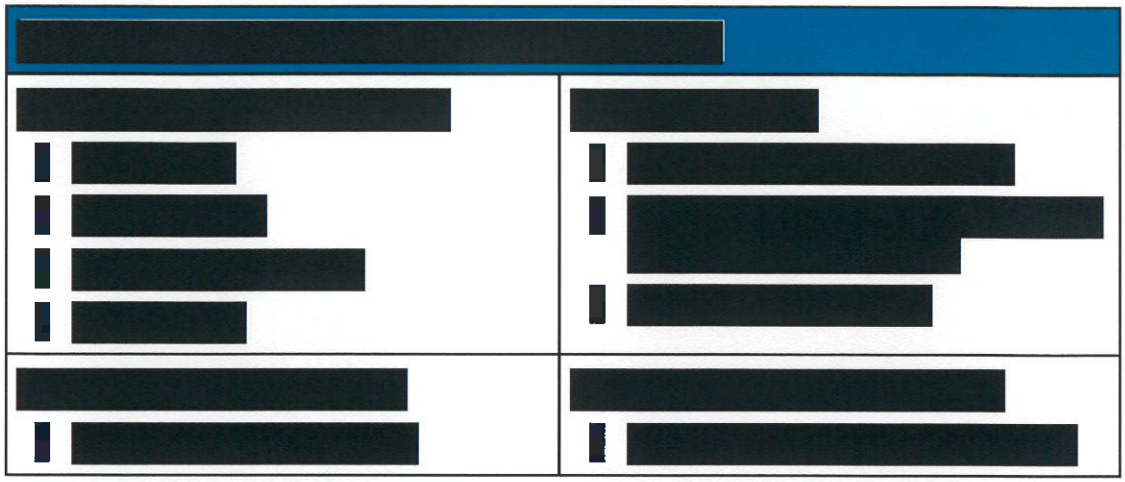
Details for the identified vulnerabilities were provided to FMC to request feedback and to facilitate remediation and risk mitigation efforts.

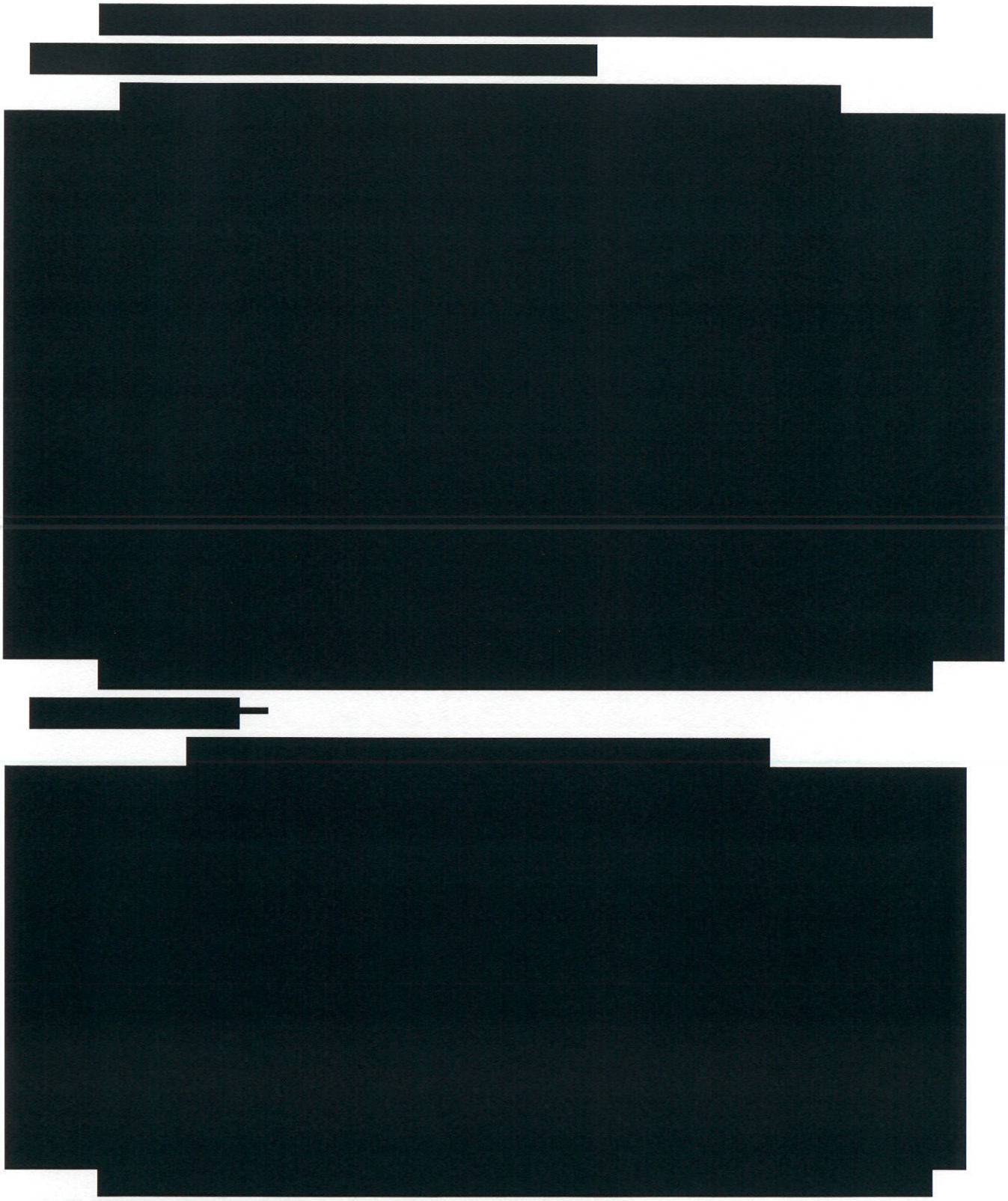
Internal Attack Vectors

Based on the results of the Red Team Internal Attack testing scenario, we identified multiple vulnerabilities that could be exploited to obtain unauthorized access to systems and data, as summarized below. Each attack vector is based on multiple vulnerabilities that were identified on various FMC systems. Each attribute described in the attack vector may apply to one or more individual instances of the identified vulnerabilities; these details were provided separately to FMC for additional information related to the individual instances.

[redacted]

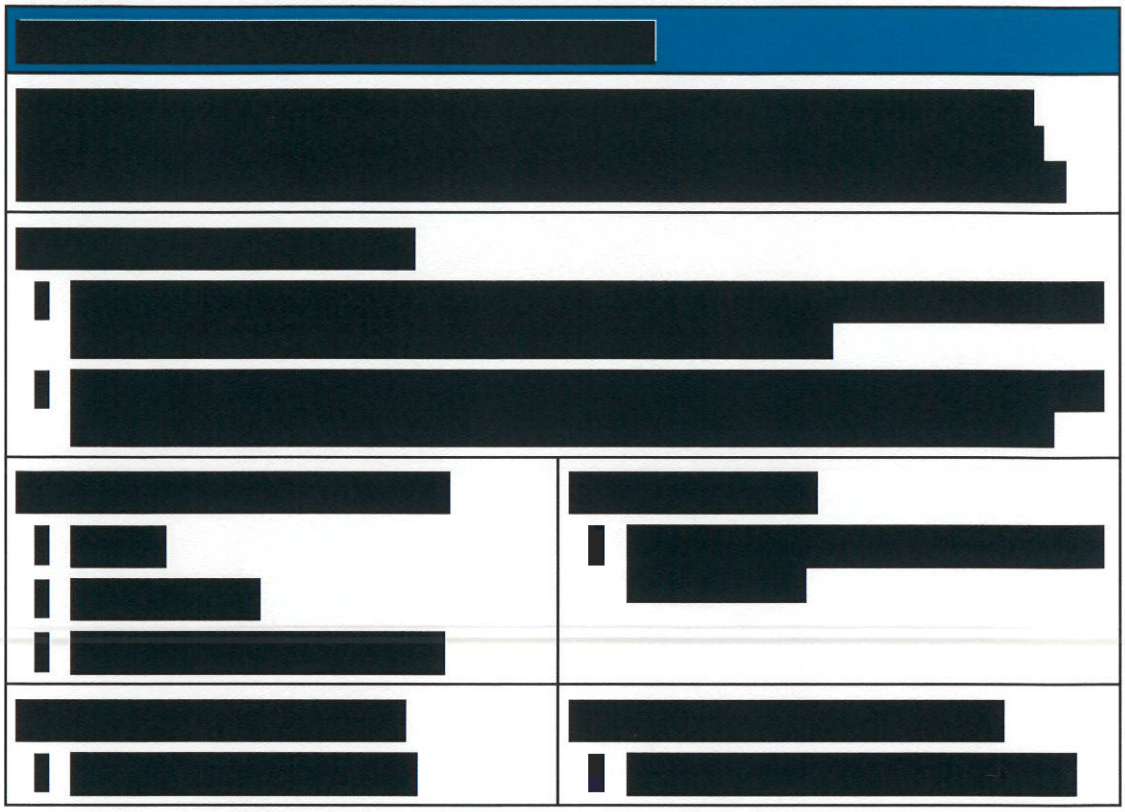




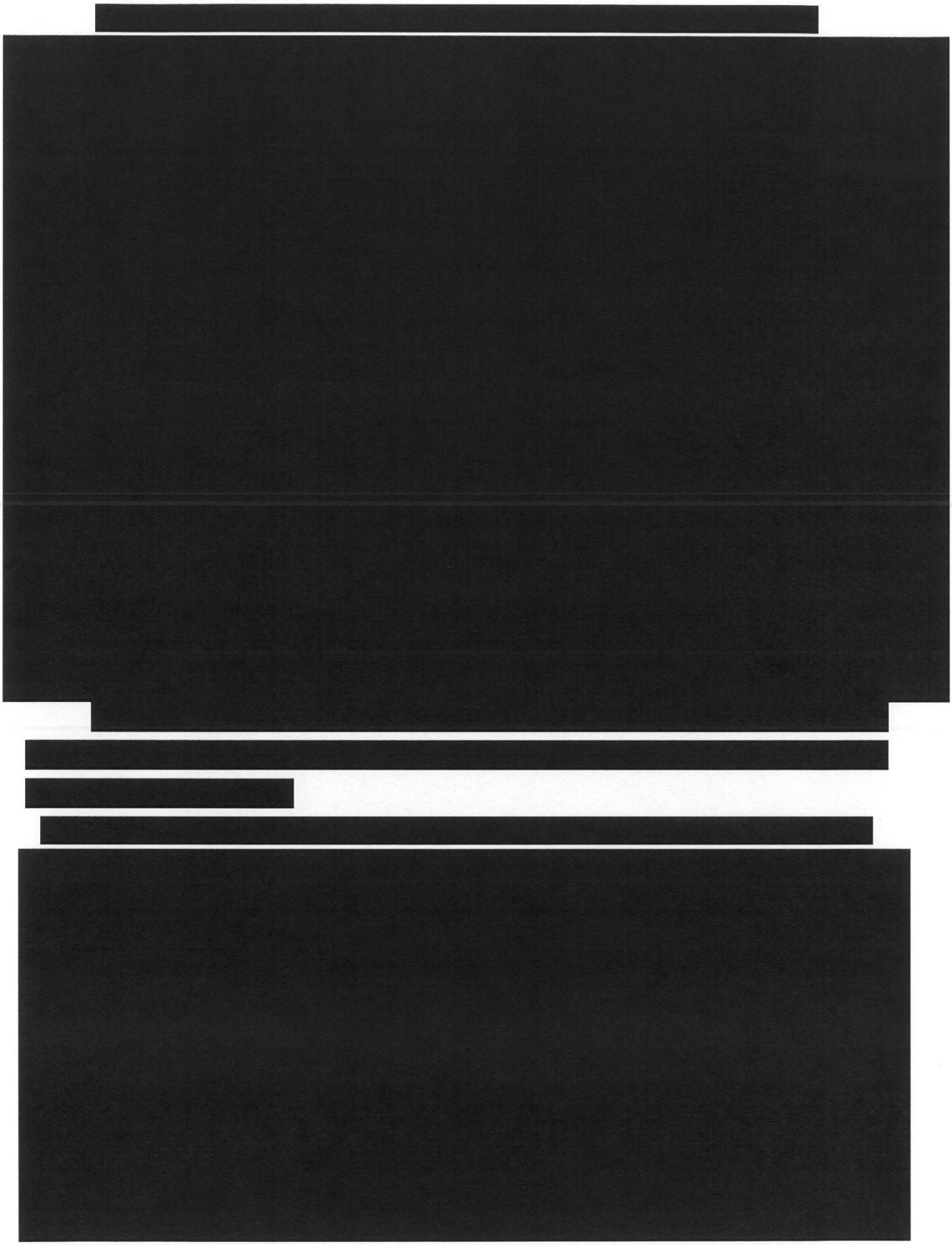


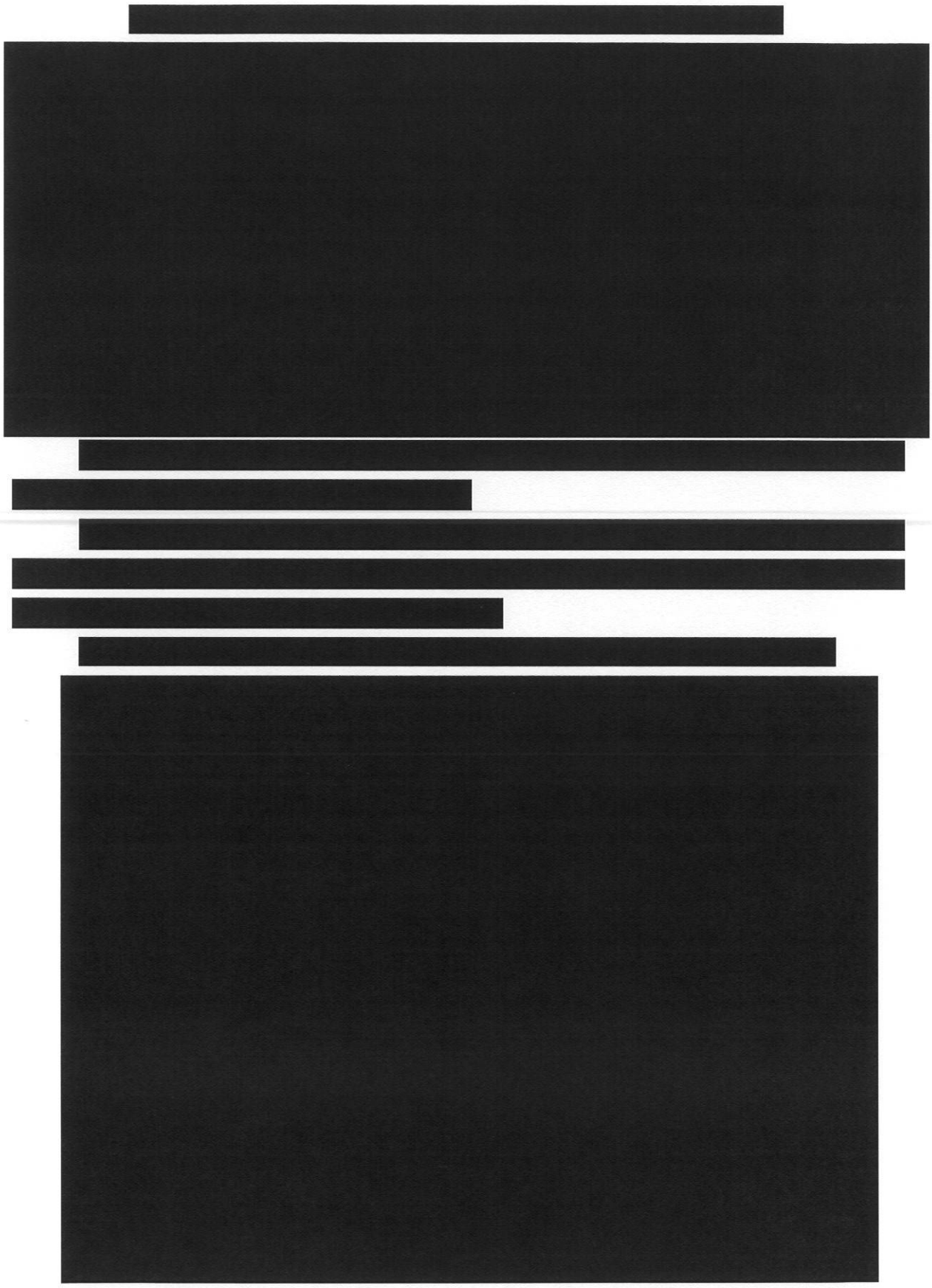
However, we did not attempt exploitation due to one or more factors, including potential risk of service disruption and significant effort to develop a custom, non-public exploit.

[redacted]

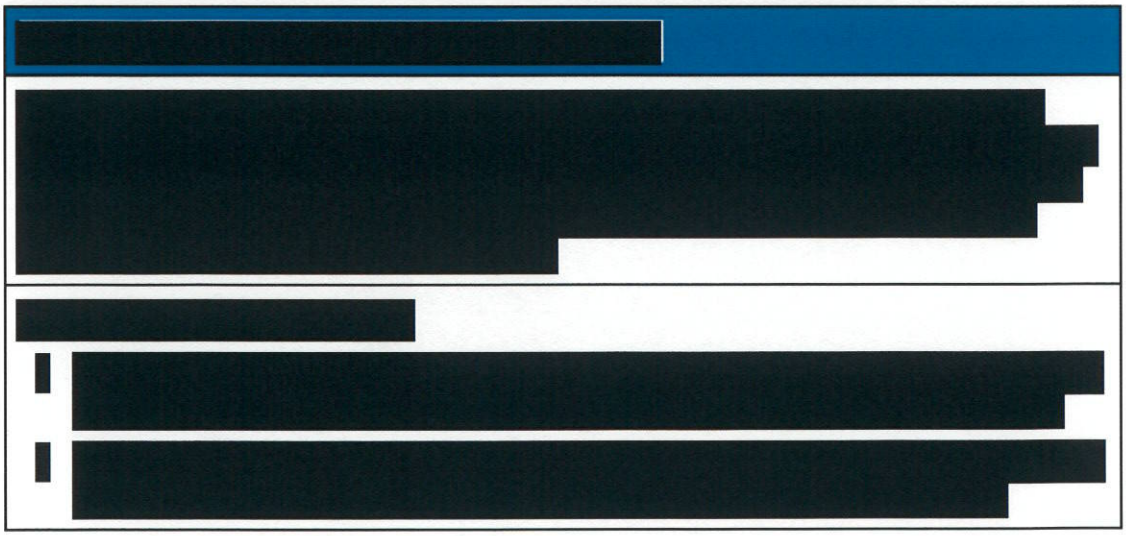


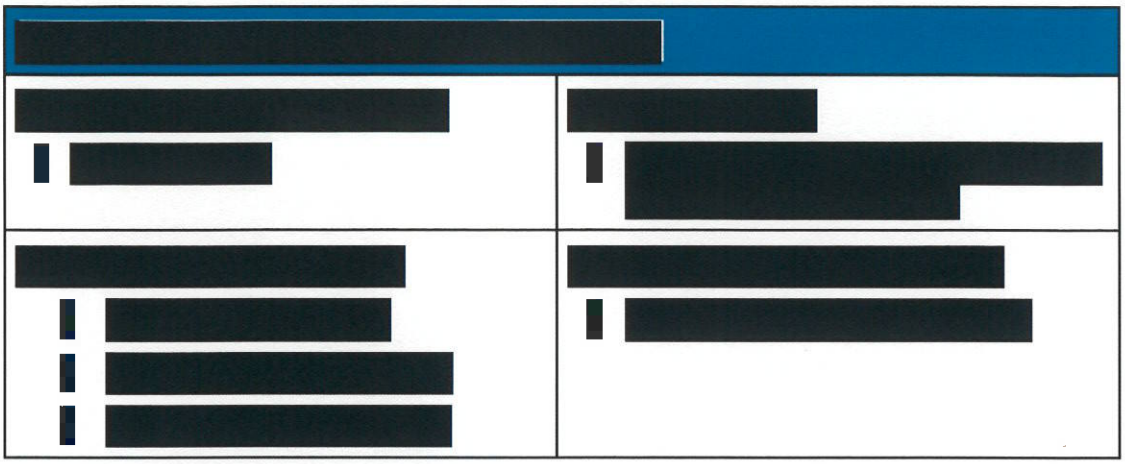
[redacted]





[redacted]





FINDINGS

Common Criteria

The Federal Information Security Modernization Act of 2014 (FISMA 2014) requires Federal agencies to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency. As part of the FISMA requirements, Federal agencies must meet the minimum-security requirements by selecting the appropriate security controls and assurance requirements as described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems". Criteria for the following findings reference relevant security controls defined in NIST SP 800-53, Revision 5.

FINDING 1 - Insufficient software management

Condition

[redacted]

Criteria

NIST SP 800-53 security controls:

1. RA-5, "Vulnerability Monitoring and Scanning", requires the agency to: a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and
2. SI-2, "Flaw Remediation", requires the agency to: a. Identify, report, and correct system flaws; c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and
3. SA-22, "Unsupported System Components", requires the agency to: a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.

Cause

[redacted]

Effect

[redacted]

Recommendation 1

[redacted]

Recommendation 2

[redacted]

FINDING 2 - Default authentication credentials are utilized

Condition

[redacted]

Criteria

NIST SP 800-53 security controls:

1. IA-5, "Authenticator Management", requires the agency to: Manage system authenticators by: c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; e. Changing default authenticators prior to first use;
2. RA-5, "Vulnerability Monitoring and Scanning", requires the agency to: a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and
3. SI-2, "Flaw Remediation", requires the agency to: a. Identify, report, and correct system flaws; c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates.

Cause

[redacted]

Effect

[redacted]

Recommendation 3

[redacted]

Recommendation 4

[redacted]

FINDING 3 - Insufficient configuration management

Condition

[redacted]

Criteria

NIST SP 800-53 security controls:

1. CM-6, "Configuration Settings", requires the agency to: a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration settings.

Cause

[redacted]

Effect

[redacted]

Recommendation 5

[redacted]

Recommendation 6

[redacted]

FINDING 4 - Flaws in custom-developed application functionality

Condition

[redacted]

Criteria

NIST SP 800-53 security controls:

1. SI-10, "Information Input Validation", requires the agency to: Check the validity of the following information inputs [Assignment: organization-defined information inputs to the system];
2. RA-5, "Vulnerability Monitoring and Scanning", requires the agency to: a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and
3. SI-2, "Flaw Remediation", requires the agency to: a. Identify, report, and correct system flaws; c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates.

Cause

[redacted]

Effect

[redacted]

Recommendation 7

[redacted]

Recommendation 8

[redacted]

Appendix A – Internal Controls

In planning and performing our audit, we identified internal control components and underlying internal control principles as significant to the audit objective. Specifically, we assessed the implementation of the FMC's controls to protect FMC IT systems and electronic data. However, because our review was limited to those internal control components and underlying principles that we found significant to the objective of this audit, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

Appendix B – Agency Response

TO : Inspector General **DATE:** September 26, 2023

FROM : Managing Director

SUBJECT : Audit A23-04 - Information Technology Vulnerability Audit (ITVA)

I have reviewed the findings and recommendations contained in the subject audit. Management values the Office of the Inspector General's efforts in assessing the Commission's IT vulnerability program to identify any critical security weaknesses. We appreciate the recommendations for improvement in this important effort. It is anticipated that all of the findings and recommendations made in this audit will be remediated by the Commission's application modernization project slated to begin early in FY 2024 and to be completed in FY 2026.

Finding 1 – Insufficient software management

Recommendation #1: [redacted]

Comment: Management agrees with the audit finding and recommendation. [redacted]

Recommendation #2: [redacted]

Comment: Management agrees with the audit finding and recommendation. The FMC participates in the CISA CDM program and has a robust vulnerability scanning process that covers the FMC servers and endpoints. [redacted]

Finding 2 – Default authentication credentials are utilized

Recommendation #3: [redacted]

Comment: Management agrees with the audit finding and recommendation. [redacted]

Recommendation #4: [redacted]

Comment: Management agrees with the audit finding and recommendation. [redacted]

Finding 3 – Insufficient configuration management

Recommendation #5: [redacted]

Comment: Management agrees with the audit finding and recommendation. [redacted]

Recommendation #6: [redacted]

Comment: Management agrees with the audit finding and recommendation. [redacted]

Finding 4 – Flaws in custom-developed application functionality

Recommendation #7: [redacted]

Comment: Management agrees with the audit finding and recommendation. Once completed, the application modernization process currently underway will incorporate all of the components recommended and will have a fully developed software lifecycle.

Recommendation #8: [redacted]

Comment: Management agrees with the audit finding and recommendation. The FMC participates in the CISA CDM program and does have a robust vulnerability scanning process that covers the FMC servers and endpoints. FMC also participates in the CISA Cyber Hygiene Web Application Scanning program, a service that assesses the health of our publicly accessible web applications by checking for known vulnerabilities and weak configurations. [redacted] Manual testing will be conducted on a quarterly basis to ensure the application security controls put in place remain valid and functioning as intended.

Lucille L. Marvin

cc: Office of the Chairman
Office of Information Technology