

OFFICE OF INSPECTOR GENERAL
Federal Communications Commission

[PUBLIC]

**FY 24 Federal Information Security
Modernization Act of 2014 (FISMA) Evaluation
for the Federal Communications Commission**

Report Number
24-EVAL-05-01

January 7, 2025



202-418-0470



www.fcc.gov/inspector-general




Federal Communications Commission
Office of Inspector General
45 L Street NE, Washington, DC 20554

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: January 7, 2025

TO: Jessica Rosenworcel, Chairwoman
Brendan Carr, Commissioner
Geoffrey Starks, Commissioner
Nathan Simington, Commissioner
Anna M. Gomez, Commissioner
Mark Stephens, Managing Director



FROM: Fara Damelin, Inspector General

SUBJECT: Public Report on the Federal Communications Commission's (FCC's) Fiscal Year 2024 Federal Information Security Modernization Act Evaluation (Report No. 24-EVAL-05-01)

In accordance with the Federal Information Security Modernization Act (FISMA), the FCC Office of Inspector General (FCC OIG) is providing an executive summary and the final public report on the FCC's Fiscal Year 2024 FISMA Evaluation. FCC OIG contracted with Kearney and Company, P.C. (Kearney) to evaluate FCC's progress in complying with the requirements of FISMA. The evaluation also assessed FCC's compliance with Department of Homeland Security reporting requirements, and applicable Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) guidance for a representative subset of FCC's information systems.

Kearney determined that the Commission's FY 2024 information security program was not in compliance with FISMA legislation, OMB guidance, and applicable NIST special publications. Five of the nine domains Kearney evaluated warrant additional management attention to address identified deficiencies:

- Risk Management,
- Supply Chain Risk Management,
- Configuration Management,
- Identity and Access Management, and
- Information Security Continuous Monitoring.

The FISMA evaluation report includes seven findings and offers 27 recommendations to improve the effectiveness of FCC's information security program controls. Of the 27 recommendations we issued, 21 are either repeats or updates from prior FISMA evaluations, and six address new deficiencies identified in FY 2024.

Kearney also identified the following related progress: In FY 2024, FCC and USAC closed six prior year recommendations and made improvements to processes within its information security program. These include modernization of FCC's IT environment through the migration of IT assets and components from the data center to cloud service providers and implementation of tools to improve its management of account creation, authentication, and administration.

In management's response, FCC concurred in principle with all seven findings and committed to resolve the associated recommendations. We appreciate the Commission's attention to these issues, which have been identified as top challenges in this year's FCC OIG report, [FCC's Top Management and Performance Challenges for FY 2025](#).

Kearney is wholly responsible for the attached public FISMA evaluation report and the conclusions expressed therein. FCC OIG monitored Kearney's performance throughout the evaluation and reviewed its report and related documentation. Our review disclosed no instances where Kearney did not comply in all material respects with Council of Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation.

Please direct any questions regarding this evaluation report to Sophie Jones, Assistant Inspector General for Audit, at (202) 418-1655 or Sophila.Jones@fcc.gov or to Robyn Williams, Deputy Assistant Inspector General for Audit, at (202) 418-7890 or Robyn.Williams@fcc.gov.

We thank management for the cooperation and assistance provided throughout this engagement.

Attachment

cc: Daniel Daly, Deputy Managing Director
Jae Seong, Chief Financial Officer
Allen Hill, Chief Information Officer
Don Tweedie, Deputy Chief Information Officer
Christopher Webber, Chief Information Security Officer

FCC OIG'S EXECUTIVE SUMMARY

Fiscal Year (FY) 2024 Federal Information Security Modernization Act of 2014 (FISMA) Evaluation for the Federal Communications Commission (FCC or Commission)

Background

FISMA requires federal agencies, including the Federal Communications Commission (FCC) to perform annual independent evaluations of their information security programs and practices and to report the evaluation results to the Office of Management and Budget (OMB). FISMA requires that the agency's Inspector General (IG) or an IG-determined independent external evaluator perform the independent evaluations.

FISMA directs the National Institute of Standards and Technology (NIST) to develop risk-based standards and guidelines to assist agencies in defining security requirements for their information systems. The Department of Homeland Security (DHS) provided agency IGs with a set of security-related metrics grouped into nine domains and organized by the five information security functions outlined in the NIST Cybersecurity Framework, to address their FISMA reporting responsibilities in the FY 2024 IG FISMA Reporting Metrics.

FCC OIG's Approach

For FY 24, FCC Office of Inspector General (FCC OIG) contracted with Kearney and Company, P.C. (Kearney) to evaluate the FCC's progress in complying with the requirements of FISMA. The evaluation also assessed FCC's compliance with DHS reporting requirements, and applicable OMB and NIST guidance for a representative subset of FCC's information systems. Kearney is wholly responsible for the attached FISMA evaluation report dated December 30, 2024 and the conclusions expressed therein. FCC OIG monitored Kearney's performance throughout the evaluation and reviewed its report and related documentation. Our review disclosed no instances where Kearney did not comply in all material respects with the Council of Inspectors General on Integrity and Efficiency's (CIGIE's) Quality Standards for Inspection and Evaluation.

Objectives

The objectives of this evaluation were to: (1) determine the effectiveness of information security policies, procedures, and practices for a representative subset of

the FCC and the Universal Service Administrative Company's (USAC, one of the Commission's fund administrators) information systems; (2) assess compliance with FISMA and related information security policies, procedures, standards, and guidelines; (3) prepare FCC OIG's responses to the DHS FY 2024 Inspector General FISMA Reporting Metrics.

Results in Brief

Kearney determined that the Commission's FY 2024 information security program was not in compliance with FISMA legislation, OMB guidance, and applicable NIST special publications. Five of the nine domains Kearney evaluated warrant additional management attention to address identified deficiencies. Kearney grouped the deficiencies and instances of noncompliance from those five domains into seven findings.

Kearney also identified the following progress: In FY 2024, FCC and USAC closed six prior year recommendations and made improvements to processes within its information security program. These include modernization of FCC's IT environment through the migration of IT assets and components from the data center to cloud service providers and implementation of tools to improve its management of account creation, authentication, and administration.

Recommendations

The FISMA evaluation offers 27 recommendations to improve the effectiveness of the FCC's information security program controls. Of the 27 recommendations, 21 are either repeats or updates from prior FISMA evaluations, and six address new deficiencies identified in FY 2024.

Public Release

FCC OIG is publicly releasing this Executive Summary and a public version of this report in accordance with our obligation under FISMA to take appropriate steps to ensure the protection of information that, if disclosed, may adversely affect information security.



**Fiscal Year (FY) 2024
Federal Information Security
Modernization Act of 2014 (FISMA)
Evaluation for the
Federal Communications Commission (FCC)**

Report No. 24-EVAL-05-01

January 7, 2025

**KEARNEY &
COMPANY**

*Point of Contact:
Franz Inden, Partner
1701 Duke Street, Suite 500
Alexandria, VA 22314
703-931-5600, 703-931-3655 (fax)
franz.inden@kearneyco.com*

TABLE OF CONTENTS

	<u>Page #</u>
I. Evaluation Purpose	1
II. Background	1
III. Evaluation Results	3
IV. Recommendations	4
APPENDIX A: MANAGEMENT’S RESPONSE TO DETAILED FISMA REPORT	5
APPENDIX B: ACRONYM LIST	8

I. Evaluation Purpose

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including the Federal Communications Commission (“the FCC” or “the Commission”), to perform annual independent evaluations of their information security programs and practices and to report the evaluation results to the Office of Management and Budget (OMB). FISMA states that the agency Inspector General (IG) or an IG-determined independent external evaluator must perform the independent evaluations. The FCC Office of Inspector General (OIG) contracted with Kearney & Company, P.C. (defined as “Kearney,” “we,” and “our” in this report) to conduct the FCC’s fiscal year (FY) 2024 evaluation. The objective of this evaluation was to determine the effectiveness of information security policies, procedures, and practices of a representative subset of the FCC’s and the Universal Service Administrative Company’s (USAC) information systems, including compliance with FISMA and related information security policies, procedures, standards, and guidelines. USAC is a not-for-profit corporation designated by the FCC as the administrator of the federal universal service fund.

II. Background

To achieve its mission of regulating interstate and international communications, the FCC must safeguard the sensitive information it collects and manages. Ensuring the confidentiality, integrity, and availability of this information in an environment of increasingly sophisticated security threats requires a strong, agency-wide information security program.

FISMA directs the National Institute of Standards and Technology (NIST) to develop risk-based standards and guidelines to assist agencies in defining security requirements for their information systems. In addition, OMB issues information security policies and guidelines, including annual instructions to the heads of federal executive departments and agencies for meeting their reporting requirements under FISMA. The Department of Homeland Security (DHS) exercises primary responsibility within the Executive Branch for the operational aspects of federal agency cybersecurity with respect to the federal information systems that fall within the scope of FISMA. DHS’s responsibilities include overseeing agency compliance with FISMA and developing analyses for OMB to assist in the production of its annual FISMA report to Congress. Accordingly, DHS provided agency IGs with a set of security-related metrics grouped into nine domains¹ and organized by the five information security functions outlined in the NIST Cybersecurity Framework^{2,3} to address their FISMA reporting responsibilities in the *FY 2024 IG FISMA Reporting Metrics*. **Exhibit 1** presents the IG FISMA metrics structure and the corresponding nine metric domains.

¹ The nine FISMA IG domains are Risk Management, Supply Chain Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning.

² Per NIST’s *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, dated April 16, 2018: “[The five functions (i.e., Identify, Protect, Detect, Respond, and Recover)] aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.”

³ Although NIST published the *NIST Cybersecurity Framework (CSF) 2.0* on February 26, 2024, DHS organized the *FY 2024 IG FISMA Reporting Metrics*, dated February 10, 2023, around the *Framework for Improving Critical Infrastructure Cybersecurity*, dated April 16, 2018.

Exhibit 1: Cybersecurity Framework Functions and Associated Metric Domains

Cybersecurity Framework Function	FY 2024 IG FISMA Metric Domain
Identify	Risk Management
	Supply Chain Risk Management
Protect	Configuration Management
	Identity and Access Management
	Data Protection and Privacy
	Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Source: Kearney; created from the FY 2024 IG FISMA Reporting Metrics

For FY 2024, DHS provided maturity models⁴ for each FISMA metric in all nine domains and five NIST Cybersecurity Framework Function areas. **Exhibit 2** presents the maturity levels within DHS’s maturity model structure and the corresponding definition of each maturity level.

Exhibit 2: Maturity Levels and Definitions

Maturity Level	Title	Brief Definition
Level 1	Ad hoc	Program is not formalized. Activities are performed in a reactive manner.
Level 2	Defined	Program is formalized, but policies, plans, and procedures are not consistently implemented organization-wide.
Level 3	Consistently Implemented	Formalized program is consistently implemented across the agency, but measures of effectiveness are not captured and used.
Level 4	Managed and Measurable	Program activities use quantitative and qualitative metrics to measure and manage program implementation, achieve situational awareness, and control ongoing risk.
Level 5	Optimized	Program is institutionalized, repeatable, self-regenerating, and updated on a near-real-time basis based on changes in business/mission requirements and a changing threat and technology landscape.

Source: Kearney; created from the FY 2024 IG FISMA Reporting Metrics

Using the five maturity levels above, DHS instituted a scoring system to determine the degree of maturity of an agency’s information security programs, as well as specific criteria to identify whether the agency’s program in each Cybersecurity Framework function was effective. Ratings throughout the nine domains are determined based on a calculated average, wherein the average of the metrics within each domain is used to determine the effectiveness of individual function areas and the overall information security program. With the calculated average scoring model,

⁴ The FISMA maturity models include five levels of program maturity. From lowest to highest, the levels are: 1: *Ad Hoc*; 2: *Defined*; 3: *Consistently Implemented*; 4: *Managed and Measurable*; and 5: *Optimized*.

core and supplemental metrics are averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. While DHS and OMB encourage IGs to focus on the results of the core metrics and use the calculated average of the supplemental metrics as a data point to support risk-based determination of the overall program and function-level effectiveness, IGs have the discretion to determine the overall effectiveness rating and the rating for each function based on their assessment. If all the metrics are met, then the function is scored at Level 5: *Optimized*. DHS further stipulates that a program must achieve at least Level 4: Managed and Measurable to be considered effective.

We evaluated the effectiveness of the FCC's information security program and practices by designing procedures to assess consistency between the Commission's security controls and FISMA requirements, OMB policy guidance and applicable NIST standards, and guidelines in the areas covered by the DHS metrics. Additionally, we followed up on findings reported in previous FISMA evaluations to determine whether the FCC had taken appropriate corrective actions and properly mitigated the related risks. We provided the results of our evaluation to the FCC OIG to use in submitting the IG responses to the DHS metrics through CyberScope by the July 31, 2024, deadline. We also issued a detailed non-public FISMA report to FCC management, which contains sensitive information about FCC's information security program. Accordingly, the FCC OIG does not intend to release that report publicly.

Our evaluation methodology met the Council of Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* and included inquiries, observations, and inspection of FCC and USAC documents and records, as well as direct testing of controls.

III. Evaluation Results

The FCC made improvements to processes within its information security program since the FY 2023 FISMA evaluation and continues to work toward an effective maturity level for its information security program. While there were improvements, Kearney's assessment of the overall maturity of each metric area remained relatively consistent with the prior year.

Overall, we found deficiencies and instances of noncompliance in five of the nine domains. We grouped the deficiencies and instances of noncompliance from those five domains into seven findings, which we issued in a non-public FISMA evaluation report. The deficiencies identified during the FY 2024 FISMA evaluation require the attention of agency leadership and immediate or near-immediate corrective actions. As shown in *Exhibit 3*, the FCC's information security program was effective and in compliance with FISMA legislation, OMB guidance, and applicable NIST Special Publications for one of the five function areas, as of July 2024 (i.e., the end of our fieldwork).

Therefore, we concluded that the Commission's overall information security program was ineffective and not in compliance, based on the *FY 2024 IG FISMA Reporting Metrics*, ultimately scoring agencies at the Function level.

Exhibit 3: FCC Security Control Effectiveness

NIST Cybersecurity Framework Function	FY 2024 IG FISMA Metric Domain	FY 2023 Maturity Level	FY 2024 Maturity Level	Effective?
Identify	1.1 Risk Management	Level 3 – Consistently Implemented	Level 2 – Defined	No
Identify	1.2 Supply Chain Risk Management	Level 2 – Defined	Level 2 – Defined	No
Protect	2.1 Configuration Management	Level 2 – Defined	Level 2 – Defined	No
Protect	2.2 Identity and Access Management	Level 2 – Defined	Level 2 – Defined	No
Protect	2.3 Data Protection and Privacy	Level 3 – Consistently Implemented	Level 3 – Consistently Implemented	No
Protect	2.4 Security Training	Level 4 – Managed and Measurable	Level 3 – Consistently Implemented	No
Detect	3.1 Information Security Continuous Monitoring	Level 2 – Defined	Level 2 – Defined	No
Respond	4.1 Incident Response	Level 3 – Consistently Implemented	Level 3 – Consistently Implemented	No
Recover	5.1 Contingency Planning	Level 4 – Managed and Measurable	Level 4 – Managed and Measurable	Yes

Source: Kearney; created from the results of the FY 2024 FCC FISMA evaluation

IV. Recommendations

We issued 27 recommendations in the non-public FY 2024 FISMA evaluation report to improve the effectiveness of the FCC’s information security program controls in the areas of Risk Management, Supply Chain Risk Management, Configuration Management, Identity and Access Management, and Information Security Continuous Monitoring. Of the 27 recommendations we issued, 21 are either repeats or updates from prior FISMA evaluations, and six address deficiencies identified in FY 2024. For comparison, we issued 25 recommendations in the FY 2023 FISMA evaluation report.

We noted that the FCC was in the process of implementing policies and procedures to strengthen security controls in several areas during our evaluation. The FCC should continue to prioritize and implement its documented security policies and procedures, as well as establish ongoing monitoring over all five NIST Cybersecurity Functions to achieve an effective maturity Level 4: *Managed and Measurable* for its information security program.

APPENDIX A: MANAGEMENT'S RESPONSE TO DETAILED FISMA REPORT



Office of the Managing Director MEMORANDUM

DATE: December 31, 2024

TO: Fara Damelin, Inspector General

FROM: Mark Stephens, Managing Director
Allen Hill, Chief Information Officer

SUBJECT: Management's Response to the Fiscal Year 2024 Federal Information Security Modernization Act of 2014 (FISMA) Evaluation for the Federal Communications Commission

Thank you for the opportunity to review and comment on the draft report entitled *Fiscal Year (FY) 2024 Federal Information Security Modernization Act of 2014 (FISMA) Evaluation for the Federal Communications Commission*. We appreciate the efforts of your team and the independent evaluation team, Kearney and Company, to work with the Federal Communications Commission (FCC or Commission) throughout the FY 2024 evaluation. The results of this year's evaluation are due to the commitment and professionalism demonstrated by both of our offices as well as the independent evaluation team.

The FCC is committed to continually strengthening its information security program. The Commission's information technology (IT) and cybersecurity team continued to work throughout FY 2024 to make improvements and to resolve findings from previous years. The auditors recognized that the FCC made improvements to processes within its information security program. The FCC recognizes the auditors also concluded some aspects of the Commission's information security program were ineffective and not in compliance with FISMA legislation, Office of Management and Budget (OMB) guidance, and applicable National Institute of Science and Technology (NIST) Special Publications (SPs) as of the end of the auditors' FY 2024 evaluation.

In FY 2024, the FCC continued to remediate recommendations detailed in the Office of Inspector General's (OIG) Privacy & Data Protection Inspection of the FCC's privacy and data protection procedures. The FCC continues making significant progress implementing all the FCC OIG recommendations.

Steps Forward

The FY 2024 FISMA evaluation report identifies several findings. The FCC will continue to address each of the findings identified by the auditors:

- Continue cloud modernization with improved cybersecurity continuous monitoring will enhance real-time threat detection, ensure compliance, and strengthen the overall security posture while enabling agile, scalable operations.
- Complete the implementation of an organization-wide Supply Chain Risk Management (SCRM) strategy in accordance with federal guidance.
- Continue to evaluate risks and potential corrective actions related to Risk Management and SCRM domains.
- Continue the implementation of an adaptive and resilient security architecture for data centric protection enabling FCC to align with Zero Trust Architecture (ZTA) under EO 14028, Improving the Nation's Cybersecurity.

In FY 2024, FCC's Chief Information Officer (CIO) and Chief Information Security Officer (CISO) continued their focus on improving the Commission's cybersecurity posture. Through these ongoing efforts, the CIO and CISO built upon work completed in prior fiscal years and will continue to work diligently to resolve the open findings.

The FCC OCIO has made remarkable progress in strengthening the agency's cybersecurity posture and modernizing its IT infrastructure. Key initiatives have significantly reduced vulnerabilities, enhanced security measures, and streamlined operations, demonstrating the OCIO's commitment to safeguarding the FCC's mission.

One of the most impactful achievements has been the consolidation of the FCC's network, resulting in a 91% reduction in the attack surface within the primary data center. This milestone is marked by the successful migration of 603 servers to FedRAMP-authorized cloud service providers, the decommissioning of 275 legacy servers, with ongoing progress being made migrating the remaining 88 servers in 2025. These efforts significantly hardened the FCC's network by leveraging the robust security capabilities of FedRAMP environments, which greatly reduced the attack surface and enhanced the protection of FCC data. Complementing these efforts, the FCC OCIO enhanced perimeter defenses by implementing advanced bot detection and prevention solutions, as well as web application firewalls. Together, these measures contributed to a dramatic reduction in malicious activity, with attacks decreasing from 409 million malicious requests in October 2023 to approximately 15 million in December 2024—a 96% decline—underscoring the effectiveness of these efforts in safeguarding the FCC's digital assets.

To further bolster security, the OCIO has advanced its compliance with Binding Operational Directive (BOD) 23-02 by prioritizing phishing-resistant multifactor authentication (PR-MFA). All employees and contractors are now required to use HSPD-12 PIV cards for accessing the

FCC network via Government Furnished Equipment (GFE) laptops, and remote access has been restricted. The CIO will mandate PR- MFA technologies across all FCC systems in the coming months to achieve full compliance with BOD 23-02 and to address the Identity Pillar of Zero Trust, as outlined in Executive Order 14028.

In FY2024, the FCC OCIO launched a 24/7 Virtual Security Operations Center (VSOC) to enhance agility in responding to cybersecurity threats. From July to September 2024, the VSOC effectively managed 18 email phishing incidents, 550 Security Information and Event Management (SIEM) alerts, 68 Endpoint Detection and Response (EDR) alerts, and 23 bot-related alerts. Projections for FY2025 indicate the VSOC will address an estimated 72 email phishing alerts, 220 SIEM alerts, 272 EDR alerts, and 92 bot alerts, reflecting its growing impact and capability.

The FCC OCIO values the recognition of its accomplishments by the FCC Office of Inspector General (OIG). Efforts to improve the Risk Management Framework (RMF) have included comprehensive risk and security control assessments and the development of an OMB-M-22-18 compliant software inventory, complete with vendor attestation letters. Additionally, the OCIO is committed to continuously developing, refining, and applying baseline security configurations, ensuring they remain centrally accessible for stakeholders. These efforts will continue to enhance the maturity and resilience of the FCC's cybersecurity program.

Through these initiatives, the FCC OCIO demonstrates its unwavering dedication to securing the FCC's digital environment, supporting its mission, and leading by example in the federal IT landscape. In partnership with the Bureaus and Offices across the Commission, we remain committed to collaborating with the FCC OIG to mature and strengthen the FCC's cybersecurity program. We look forward to working in this coming fiscal year to resolve the remaining FY 2024 audit findings while continuing to enhance the cybersecurity posture of the Commission.

Respectfully submitted,

**MARK
STEPHENS**

Digitally signed by MARK
STEPHENS
Date: 2025.01.07 11:20:29
-05'00'

Mark Stephens
Managing Director
Office of Managing Director

**CHRISTOPHE
R WEBBER**

Digitally signed by
CHRISTOPHER WEBBER
Date: 2025.01.07 10:22:00
-05'00'

Allen Hill
Chief Information Officer
Office of Chief Information Officer

APPENDIX B: ACRONYM LIST

Acronym	Definition
Commission	Federal Communications Commission
DHS	Department of Homeland Security
FCC	Federal Communications Commission
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IG	Inspector General
Kearney	Kearney & Company, P.C.
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
USAC	Universal Service Administrative Company