Fiscal Year (FY) 2023
Federal Information Security Modernization Act of 2014 (FISMA) Evaluation for the Federal Communications Commission (FCC)

Report No. 23-EVAL-05-01

January 5, 2024

KEARNEY& COMPANY

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

TABLE OF CONTENTS

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) 2023 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 domains[1] and organized by the five information security functions outlined in the NIST Cybersecurity Framework[2] to address their FISMA reporting responsibilities in the *FY 2023 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.”

Exhibit 1: Cybersecurity Framework Functions and Associated Metric Domains

Cybersecurity Framework Function	FY 2023 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 2023 IG FISMA Reporting Metrics

For FY 2023, DHS provided maturity models[3] 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 2023 IG FISMA Reporting Metrics

[3] 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*.

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 are used to determine the effectiveness of individual function areas and the overall information security program. With the calculated average scoring model, 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, 2023 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

While the FCC made improvements since the FY 2022 FISMA evaluation and continues to work towards an effective maturity level for its information security program, our 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 2023 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 in one of the five function areas and in compliance with FISMA legislation, OMB guidance, and applicable NIST Special Publications as of July 2023 (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 2023 IG FISMA Reporting Metrics* ultimately scoring agencies at the Function level.

Exhibit 3: FCC Security Control Effectiveness

NIST Cybersecurity Framework Function	FY 2023 IG FISMA Metric Domain	FY 2022 Maturity Level	FY 2023 Maturity Level	Effective?
Identify	1.1 Risk Management	Level 3 – Consistently Implemented	Level 3 – Consistently Implemented	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 4 – Managed and Measurable	Yes
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 2023 FCC FISMA evaluation

IV. Recommendations

We issued 25 recommendations in the non-public FY 2023 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 25 recommendations we issued, 16 are either repeats or updates from prior FISMA evaluations, and nine address deficiencies identified in FY 2023. For comparison, we issued 21 recommendations in the FY 2022 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 7, 2023

TO: Sharon Diskin, Acting Inspector General

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

SUBJECT: Management Response to the Fiscal Year 2023 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) 2023 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 2023 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. During the entire evaluation, the Commission worked closely with your office and the independent evaluation team to provide the requested information in a timely manner to assist the evaluation process.

The FCC is committed to continually strengthening its information security program. The Commission's information technology (IT) team continued to work throughout FY 2023 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, since the FY 2022 FISMA evaluation, in the areas of: Risk Management (i.e., completing risk assessments and security control assessments for key information systems), Identity and Access Management (i.e., implementing tools to improve management of account creation, authentication and administration), Information Security Continuous Monitoring (ISCM) i.e. enhancing monthly and quarterly IT security metrics, and, Incident Response (i.e. enhancing processes for collecting, analyzing, and reporting quantitative and qualitative performance metrics). However, the FCC recognizes that the auditors also concluded that 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 2023 evaluation.

In FY 2023, the FCC Chief Information Officer (CIO) and the FCC Chief Information Security Officer (CISO) continued their focus on improving the Commission's cybersecurity posture. Through these ongoing efforts, the CIO and CISO have built upon work completed in prior fiscal years to close 24% of the Commission's overall number of open FISMA recommendations from FY 2022 to FY 2023. The Commission will continue to work diligently to resolve the remaining open findings.

In FY 2023, the FCC continued to remediate recommendations from the Government Accountability Office (GAO) evaluation of the FCC Electronic Comment Filing System (ECFS). The FCC has remediated 95% of the GAO recommendations to date. Some of the recommendations that were remediated will also assist in remediating FISMA findings and strengthening the FCC's cybersecurity posture.

Steps Forward

The FY 2023 FISMA evaluation report identifies several significant deficiencies in IT security. The Commission will continue to address each of the findings identified by the auditors. Specifically, the FCC IT team will:

- Complete the implementation of its ISCM Strategy and Plan. Reduce system vulnerabilities through an integrated risk-based vulnerability-management effort to create a more secure FCC IT environment. The FCC will implement the ISCM strategy in compliance with Binding Operational Directive (BOD) 22-01 and the associated Continuous Diagnostics and Mitigation (CDM) requirements.
- Continue to evaluate risks and potential corrective actions related to Risk Management and Supply Chain Risk Management (SCRM) domains.
- Implement an innovative Network Security Operations Center (NSOC) for effective and comprehensive security monitoring, proactively neutralizing threats and streamlining investigations.
- Continue cloud-based modernization efforts, which, along with strengthened processes and oversight, will eliminate a considerable number of the remaining weaknesses associated with legacy systems.
- Implement 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 partnership with the Bureaus and Offices across the Commission, we remain committed to strengthening the FCC's IT security controls. We look forward to working in this coming fiscal year to resolve the FY 2023 audit findings while continuing to enhance the cybersecurity posture of the Commission.

Respectfully submitted,

MARK STEPHENS Digitally signed by MARK STEPHENS Date: 2023.12.14 13:32:29 -05'00'	ALLEN HILL Digitally signed by ALLEN HILL Date: 2023.12.13 10:23:35 -05'00'
Mark Stephens Managing Director Office of Managing Director	Allen Hill Chief Information Officer Office of Managing Director

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