UNITED STATES GOVERNMENT
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: March 13, 2023

TO: Chairwoman

FROM: Acting Inspector General Sharon R. Diskin/SJ

SUBJECT: Public Report on the Federal Communications Commission's Fiscal Year 2022 Federal Information Security Management Act Evaluation (Report No. 22-EVAL-06-01)

In accordance with the Federal Information Security Management Act (FISMA), the Office of Inspector General (OIG) is providing the final report on the Federal Communication Commission (FCC) Fiscal Year 2022 Federal Information Security Management Act Evaluation (Report No. 22-EVAL-06-01). OIG contracted with Kearney and Company, P.C. to evaluate the FCC's progress in complying with the requirements of FISMA. This evaluation is consistent with OIG's authority under the Inspector General Act of 1978, as amended, including but not limited to sections 2(1)(2) and 4(a)(1). The evaluation is not intended as a substitute for any agency regulatory compliance review or regulatory compliance audit.

The evaluation was performed in accordance with Council of the Inspectors General on Integrity and Efficiency (CIGIE) standards for inspection and evaluations (I&E). CIGIE I&E standards require that auditors plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions, based on the evaluation objectives. 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, and based on the results of the work performed, assess compliance with FISMA and related information security policies, procedures, standards, and guidelines.

Kearney found that the FCC security programs were ineffective in seven of the nine metric domains. The contractor's assessment of the overall maturity of each metric domain remained relatively consistent with the prior year. The Supply Chain Risk Management domain is the one metric domain that improved from the prior year. The FISMA evaluation report included eight findings with 21 recommendations intended to improve the effectiveness of the FCC's information security program controls. FCC management concurred with the findings.

Kearney is wholly responsible for the attached evaluation report and the conclusions expressed therein. OIG monitored Kearney's performance throughout the engagement and reviewed their report and related documentation. Our review disclosed no instances where Kearney did not comply in all material respects with CIGIE I&E standards.

We appreciate the collaboration and courtesies extended to Kearney and OIG during the evaluation. If you have questions, please contact Sophila Jones, Assistant Inspector General for Audit at (202) 418-1655, or Menjie Medina, Deputy Assistant Inspector General for Audit, at (202) 418-0949.

cc: Managing Director
Deputy Managing Director
Chief Information Officer
Deputy Chief Information Officer
Chief Information Security Officer
Chief Financial Officer
Deputy Chief Financial Officer

Fiscal Year (FY) 2022 Federal Information Security Modernization Act of 2014 (FISMA) Evaluation for the Federal Communications Commission (FCC)

Report No. 22-EVAL-06-01

March 10, 2023

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

Page #

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) 2022 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 Federal universal service support mechanisms.

II. Background

To achieve its mission of regulating interstate and international communications, the FCC must safeguard the sensitive information that 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 2022 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 comprised of 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 2022 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 2022 IG FISMA Reporting Metrics

For FY 2022, 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 are repeatable, and metrics are used 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 2022 IG FISMA Reporting Metrics

Using the maturity model levels, DHS instituted a scoring system to determine the degree of maturity of the agency's information security program, as well as specific criteria to conclude on the effectiveness of the agency's programs in each Cybersecurity Framework function. Ratings throughout the nine domains are by a simple majority, where the most frequent level (i.e., the mode) across the questions in each domain serves as the overall domain rating. OMB and DHS ensure that the domain ratings are scored appropriately when entered into DHS's FISMA

[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*.

reporting platform, CyberScope. To achieve an effective level of information security management under the maturity model concept, agencies must reach Level 4: *Managed and Measurable*. While DHS and OMB encourage IGs to utilize the automatically scored domain ratings, IGs have the discretion to determine the overall effectiveness rating and the rating for each function based on their assessment.

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 and guidelines, 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 for their use in submitting the IG responses to the DHS metrics through CyberScope by the July 31, 2022 and September 30, 2022 deadlines. We also issued a detailed report to FCC management, the non-public FISMA report, which contains sensitive information concerning the 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 2021 FISMA evaluation in the area of Supply Chain Risk Management. However, our assessment of the overall maturity of each metric area remained relatively consistent with the prior year. The FCC defined and communicated policies, procedures, and processes to ensure that Information and Communications Technologies (ICT) products, system components, systems, and services adhere to the Commission's cybersecurity and supply chain requirements, which resulted in an improvement in the Supply Chain Risk Management domain.

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 eight findings, which we issued in a non-public FISMA evaluation report. In combination, Kearney considered three of the seven findings to be high-risk and classified those areas as a significant deficiency, in aggregate, based on the definition from OMB Memorandum M-14-04.[4] Significant deficiencies 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

[4] Per OMB Memorandum M-14-04, a significant deficiency is: "a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets."

guidance, and applicable NIST Special Publications as of August 2022 (i.e., the end of our fieldwork). Therefore, we concluded that the Commission's overall information security program was ineffective and not in compliance due to the *FY 2022 IG FISMA Reporting Metrics* ultimately scoring agencies at the Function level.

Exhibit 3: FCC Security Control Effectiveness

NIST Cybersecurity Framework Function	FY 2022 IG FISMA Metric Domain	FY 2021 Maturity Level	FY 2022 Maturity Level	Effective?	Severity of Noted Exceptions
Identify	1.1 Risk Management	Level 3 – Consistently Implemented	Level 3 – Consistently Implemented	No	Significant Deficiency
Identify	1.2 Supply Chain Risk Management	Level 1 – Ad Hoc	Level 2 - Defined	No	Control Deficiency
Protect	2.1 Configuration Management	Level 3 – Consistently Implemented	Level 2 – Defined	No	Control Deficiency
Protect	2.2 Identity and Access Management	Level 2 – Defined	Level 2 – Defined	No	Significant Deficiency
Protect	2.3 Data Protection and Privacy	Level 3 – Consistently Implemented	Level 3 – Consistently Implemented	No	Not Applicable
Protect	2.4 Security Training	Level 4 – Managed and Measurable	Level 4 – Managed and Measurable	Yes	Not Applicable
Detect	3.1 Information Security Continuous Monitoring	Level 4 – Managed and Measurable	Level 2 – Defined	No	Significant Deficiency
Respond	4.1 Incident Response	Level 4 – Managed and Measurable	Level 3 – Consistently Implemented	No	Not Applicable
Recover	5.1 Contingency Planning	Level 4 – Managed and Measurable	Level 4 – Managed and Measurable	Yes	Not Applicable

Source: Kearney; created from the results of the FY 2022 FCC FISMA evaluation

Although we assessed the FCC programs as ineffective based on the FISMA reporting metrics, the Commission has continued to improve processes within its overall information security program, improved its maturity level in one metric domain (i.e., SCRM).

IV. Recommendations

We issued 21 recommendations in the non-public FY 2022 FISMA evaluation report intended 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 21 recommendations we issued, 7 are either repeats or updates from prior FISMA evaluations, and 14 address deficiencies identified in FY 2022. For comparison, we issued 13 recommendations in the FY 2021 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: February 17, 2023

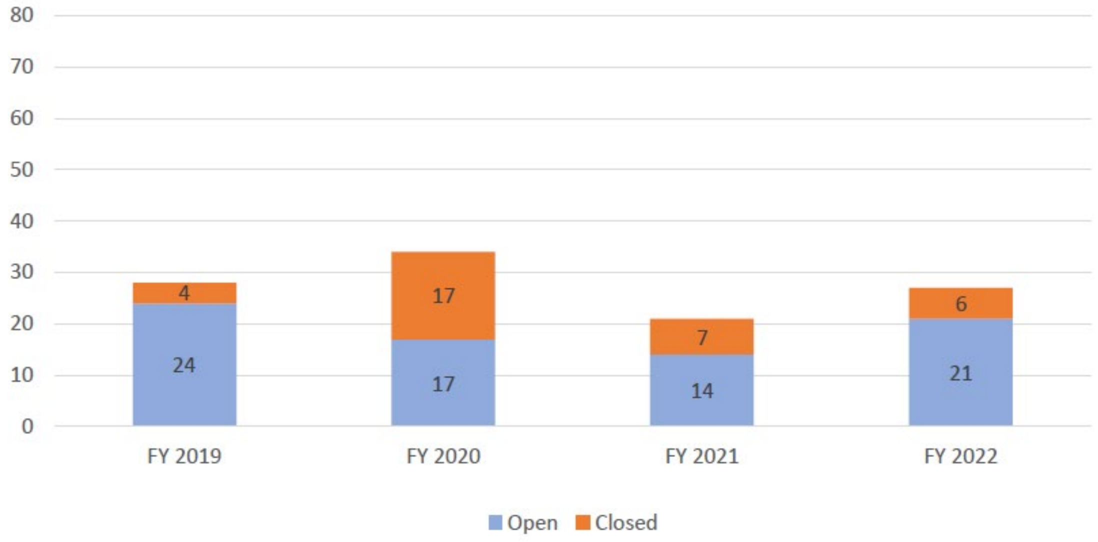
TO: Sharon Diskin, Acting Inspector General

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

SUBJECT: Management's Response to the Fiscal Year 2022 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) 2022 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 2022 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 as shown by the steady closure of FISMA recommendations from year to year in *Exhibit 1* below. The Commission's information technology (IT) team continued to work throughout FY 2022 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 2021 FISMA evaluation in the areas of: Risk Management (i.e., completing ATOs for key information systems), Data Protection and Privacy (i.e., aligning enterprise technology efforts to implement a Zero Trust Architecture), Information Security Continuous Monitoring(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 2022 evaluation.



In FY 2022, the FCC Chief Information Officer (CIO) and the FCC Deputy Chief Information Security Officer (DCISO) 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 43% of the Commission's overall number of open FISMA recommendations from FY 2021 to FY 2022. The Commission will continue to work diligently to resolve the remaining open findings.

In FY 2022, the FCC continued to remediate recommendations to the Government Accountability Office's (GAO) evaluation of the FCC's Electronic Comment Filing System. The FCC has been able to remediate 93% of GAO's recommendations from that study as of the date of this letter. Some of the recommendations that were remediated will likely help in remediating FISMA findings and will also help in strengthening the FCC's cybersecurity posture.

The FY 2022 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:

- Comply with HSPD-12 by third quarter of FY 2023. The FCC plans to enable enforcement of Personal Identity Verification (PIV) card usage for logical access to FCC resources.
- 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) 23-01 and the associated Continuous Diagnostics and Mitigation (CDM) requirements.

- Continue to evaluate risks and potential corrective actions related to Risk Management and Configuration Management domains.
- Continue to deploy tools to improve security and monitoring of activity and traffic on FCC's network.
- 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.

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 2022 audit findings while continuing to enhance the cybersecurity posture of the Commission.

Respectfully submitted,

Mark Stephens
Digitally signed by Mark Stephens
Date: 2023.02.22 12:14:23 -05'00'

Mark Stephens
Managing Director
Office of Managing Director

ALLEN HILL
Digitally signed by ALLEN HILL
Date: 2023.02.22 10:54:19 -05'00'

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
ICT	Information and Communication Technologies
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