OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: January 8, 2020

TO: Chairman

FROM: Inspector General

SUBJECT: Public Report on the Federal Communications Commission's Fiscal Year 2019 Federal Information Security Management Act Evaluation (Project No. 19-EVAL-07-01)

In accordance with the Federal Information Security Management Act (FISMA), the FCC Office of Inspector General (OIG) engaged Kearney and Company, P.C. (Kearney) to evaluate the Commission's progress in complying with the requirements of FISMA. The evaluation also assesses 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 public FISMA evaluation report and the conclusions expressed therein. The OIG monitored Kearney's performance throughout the audit and reviewed their report and related documentation. Our review disclosed no instances where Kearney did not comply in all material respects with generally accepted government auditing standards.

We appreciate the collaboration and courtesies extended to us during the evaluation. If you have questions, please contact Robert McGriff, Assistant Inspector General for Audit at (202) 418-0483 or Sophila Jones, Deputy Assistant Inspector General for Audit, at (202) 418-1655.

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

Fiscal Year (FY) 2019
Federal Information Security Modernization Act of 2014 (FISMA)
Evaluation for the
Federal Communications Commission (FCC)

Report No. 19-EVAL-07-01

January 8, 2020

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) 2019 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 eight 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 2019 IG FISMA Reporting Metrics*, dated April 9, 2019. ***Exhibit*** presents the IG FISMA metrics structure and the corresponding eight metric domains.

[1] The eight FISMA IG domains are comprised of 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 2019 IG FISMA Metric Domain
Identify	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 2019 IG FISMA Reporting Metrics

For FY 2019, DHS provided maturity models[3] for each FISMA metric in all eight domains and five NIST Cybersecurity Framework Function areas. ***Exhibit*** 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 2019 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 eight 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 reporting platform, CyberScope. To achieve an effective level of information security

[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*.

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 October 31, 2019 deadline. 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

We found that the FCC took corrective actions to improve certain processes and remediate deficiencies identified in the FY 2018 FISMA evaluation. Most notably, the FCC authorized a major information system to operate, designed effective separation of duties (SoD) controls in its financial management system, and conducted tests of contingency plans for information systems residing on the FCC's network. While these efforts improved the Commission's information security posture, FCC management must fully implement their information security policies and procedures and resolve longstanding deficiencies in the FCC information security program.

Overall, we found security deficiencies and instances of noncompliance in six of the eight domains. We grouped the security deficiencies and instances of noncompliance into nine findings, which we issued in a non-public FISMA evaluation report. Kearney considered two of the nine findings to be high-risk and classified them as significant deficiencies 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***, we concluded that the FCC's information security program was ineffective and not in compliance with FISMA legislation, OMB guidance, and applicable NIST Special Publications as of August 19, 2019 (i.e., the end of our fieldwork).

[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."

Exhibit 3: FCC Security Control Effectiveness

NIST Cybersecurity Framework Function	FY 2019 IG FISMA Metric Domain	FY 2018 Maturity Level	FY 2019 Maturity Level	Effective?	Severity of Noted Exceptions
Identify	1.1 Risk Management	Level 3 – Consistently Implemented	Level 3 – Consistently Implemented	No	Control Deficiency
Protect	2.1 Configuration Management	Level 3 – Consistently Implemented	Level 3 – Consistently Implemented	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 4 – Managed and Measurable	Level 3 – Consistently Implemented	No	Control Deficiency
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 2 – Defined	Level 2 – Defined	No	Significant Deficiency
Respond	4.1 Incident Response	Level 2 – Defined	Level 2 – Defined	No	Control Deficiency
Recover	5.1 Contingency Planning	Level 2 – Defined	Level 4 – Managed and Measurable	Yes	Not Applicable

Source: Kearney; created from the results of the FY 2019 FCC FISMA evaluation

The FCC made improvements to processes within its information security program since the FY 2018 FISMA evaluation in the areas of Risk Management, Identity and Access Management, and, most notably, Contingency Planning. However, our assessment of the overall maturity of each metric area remained relatively consistent with the prior year. The Contingency Planning and Data Protection and Privacy domains are the two areas that changed from the prior year. As previously mentioned, the FCC's testing of contingency plans for its network and FCC-owned systems during FY 2019 resulted in an improvement in the Contingency Planning domain. We assessed the Data Protection and Privacy domain at lower maturity than the prior year because, as of the end of our evaluation fieldwork (i.e., August 2019), the FCC had failed to conduct the required test of its data breach response plan. FCC management should continue efforts to implement their information security policies and procedures with particular focus in the areas of Identity and Access Management and Information Security Continuous Monitoring.

IV. Recommendations

We issued 24 recommendations in the non-public FY 2019 FISMA evaluation report intended to improve the effectiveness of the FCC's information security program controls in the areas of Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Information Security Continuous Monitoring, and Incident Response. Our report does not include recommendations in the areas of Security Training and Contingency Planning because the FCC demonstrated effective controls in these areas. Of the 24 recommendations we issued, 15 are either repeats or updates from prior FISMA evaluations, and 9 address security deficiencies identified in FY 2019. For comparison, we issued 19 recommendations in the FY 2018 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.

V. Management Comments

On December 17, 2019, FCC management provided a written response to a draft of the non-public FY 2019 FISMA evaluation report, which we included as **APPENDIX A: MANAGEMENT'S RESPONSE TO DETAILED FISMA REPORT**. We did not subject the response to evaluation procedures, and accordingly, we do not provide conclusions on it.

The non-public FISMA report contains sensitive information concerning the FCC's information security program. Accordingly, the FCC OIG does not intend to release that report publicly.

APPENDIX A: MANAGEMENT'S RESPONSE TO DETAILED FISMA REPORT

Office of the Managing Director

M E M O R A N D U M

DATE: December 17, 2019

TO: David L. Hunt, Inspector General

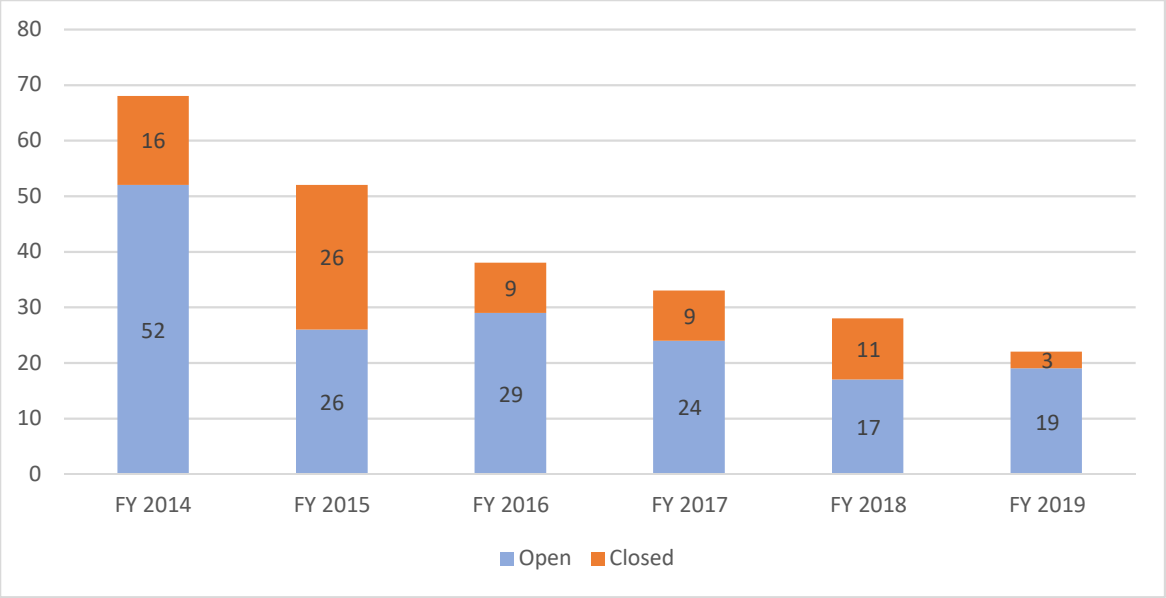
FROM: Mark Stephens, Managing Director
Francisco Salguero, Chief Information Officer
Jae Seong, Chief Financial Officer

SUBJECT: Management's Response to the Fiscal Year 2019 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) 2019 Federal Information Security Modernization Act (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 2019 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 declining number of open FISMA finding conditions from year to year in *Exhibit 1* below. The Commission's information technology (IT) team continued to work throughout FY 2019 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 2018 FISMA evaluation in the areas of: Risk Management (i.e., authorizing information systems), Identity and Access Management (i.e., designing effective Separation of Duties controls within Genesis), and, most notably, Contingency Planning (i.e., conducting tests of information system contingency plans). 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 2019 evaluation.

Exhibit 1: FCC FISMA FINDING CONDITIONS FROM FY 2014 to FY 2019



In FY 2019, the FCC Acting 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 Acting CIO and CISO have built upon work completed in prior fiscal years to reduce the Commission's overall number of open FISMA finding conditions by 63% from FY 2014 to FY 2019, including a reduction of three finding conditions from FY 2018 to FY 2019. The Commission will continue to work diligently to resolve the remaining open findings.

In FY 2019, the FCC's IT resources were prioritized to respond to the Government Accountability Office's (GAO) on-going evaluation of the FCC's Electronic Comment Filing System. The FCC has been able to remediate 63% of GAO's recommendations from that study as of the date of this letter. Some of the recommendations that were remediated will likewise help in remediating FISMA findings and will also help in strengthening the FCC's cybersecurity posture.

The FCC would like to note that the FCC's IT team and the FCC's Office of Inspector General continue to resolve details on remediation of recommendations in the areas of configuration management, incident response, and monitoring of external service provider.

Steps Forward

The FY 2019 FISMA evaluation report identifies two findings as significant deficiencies in IT security. Those two findings are related to Information Security Continuous Monitoring (ISCM) and Identity and Access Management (IAM). 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 vulnerability-management plan and continue to modernize the FCC's legacy applications.
- Refine the current process of provisioning and managing user access to the FCC's information systems. Evaluate potential options for the implementation of the requirements of Homeland Security Presidential Directive 12 (HSPD-12) for Personal Identity Verification (PIV) cards for logical access to the FCC's facilities and systems.
- Focus on corrective actions related to identity and access management to remediate the findings noted in the FY 2019 FISMA evaluation report.
- Continue to evaluate risks and potential corrective actions related to Risk Management and Configuration Management domains.
- 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.

Finally, we would like to address the finding that the Commission failed to timely conduct an annual breach response plan table-top exercise, as required by OMB guidance[5] and the FCC Privacy Act Manual. We note that the Commission completed this exercise in October 2019, consistent with the FCC Privacy Act Manual requirement that it do so "at least once annually." We recognize the view of the auditors that the exercise should have been completed by September 2019, and acknowledge that competing priorities delayed the former FCC Senior Agency Official for Privacy (SAOP) from conducting a breach response plan table-top exercise prior to that date. The Commission plans to conduct its next table-top exercise in calendar year 2020.

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 2019 audit findings while continuing to enhance the cybersecurity posture of the Commission.

[5] OMB Memorandum M-17-12, Jan. 3, 2017, *Preparing for and Responding to a Breach of Personally Identifiable Information*, at 35.

Respectfully submitted,

Mark Stephens
Managing Director
Office of Managing Director

Francisco Salguero
Chief Information Officer
Office of Managing Director

Jae Seong
Chief Financial 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
SoD	Separation of Duties
USAC	Universal Service Administrative Company