OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: May 9, 2016

TO: Chairman

FROM: Inspector General for RM

SUBJECT: Federal Communications Commission's (FCC) Fiscal Year 2015 Federal Information Security Modernization Act (FISMA) Evaluation (Public Report)

In accordance with Federal Information Security Modernization Act (FISMA) of 2014, the FCC Office of Inspector General (OIG) engaged the independent certified public accounting firm of Kearney and Company, P.C. (Kearney) to evaluate the Commission's progress in complying with the requirements of FISMA. Specifically, this evaluation included testing the effectiveness of information security policies, procedures and practices of a representative subset of the FCC's and Universal Service Administrative Company's (USAC) information systems, to determine compliance with FISMA mandates and related standards.

The attached Kearney report summarizes the detailed, sensitive FISMA Evaluation Report issued on November 18, 2015 and results of the agency Cyberscope metrics submitted to the Department of Homeland Security (DHS) on November 13, 2015. Kearney summarized results of their evaluation based on the 10 reporting areas mandated by Congress in the IG FISMA metrics prepared by the DHS. The summary compares evaluation results for FY 2015 and FY 2014, and highlights areas of improvement for the agency, as well as those areas requiring continued management attention. The report also notes that FCC's security weaknesses were grouped into 12 findings for which Kearney offers thirty-three (33) recommendations.

The OIG reviewed Kearney's report and related documentation and made necessary inquiries of Kearney's representatives. Kearney concluded that FCC's information security program was not in compliance with FISMA legislation, the Office of Management and Budget guidance, and applicable NIST Special Publications as of September 30, 2015.

FCC management provided a written response to the detailed FISMA Evaluation Report on November 12, 2015. We have attached their response, in its entirety, to this report.

The OIG would like to thank FCC for its support during this evaluation. If you have questions, please contact me or Robert McGriff, Assistant Inspector General for Audits at (202) 418-0483.

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

Fiscal Year 2015
Federal Information Security Modernization Act Evaluation

for the

Federal Communications Commission

November 12, 2015

KEARNEY&
COMPANY

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

TABLE OF CONTENTS

Why We Did The Evaluation

The Federal Information Security Modernization Act of 2014 (FISMA) requires Federal agencies, including the Federal Communications Commission (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 independent evaluations are to be performed by the agency Inspector General (IG) or an IG-determined independent external auditor. The FCC IG contracted with Kearney & Company, P.C. (Kearney) to conduct the 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. The USAC is a not-for-profit corporation designated by the FCC as the administrator of federal universal service support mechanisms.

Background

To achieve the FCC's mission of regulating interstate and international communications, the Commission 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 development of its annual FISMA report to Congress. Accordingly, on June 19, 2015, DHS provided agency IGs with a set of security-related questions to address their FISMA reporting responsibilities in *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*.

We evaluated the effectiveness of the FCC's information security program and practices by designing audit procedures to assess consistency between the FCC's security controls and FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines in the areas covered by the DHS questions. The FCC is required to submit responses to the questions through DHS's FISMA reporting platform, CyberScope, by November 13, 2015. Additionally, we followed up on findings reported in previous FISMA evaluations to determine whether risks have been properly mitigated. Our evaluation methodology met the *Quality Standards for Inspection and Evaluation*, promulgated by the Council of Inspectors General on Integrity and Efficiency (CIGIE), and included inquiries, observations, and inspection of FCC and USAC documents and records, as well as direct testing of controls.

Evaluation Results

The FCC has improved its overall information security program since the fiscal year (FY) 2014 evaluation, most notably in developing policies and procedures designed to improve the security of FCC information. Additionally, the FCC is implementing major changes in its information technology (IT) environment, including the relocation of the primary FCC data center, shifting additional processing to the cloud, and replacing legacy systems and infrastructure. Management stated these efforts have required significant resources, delaying the implementation of the information security policies and procedures. While these changes provide the FCC with an opportunity to improve its information security posture, management must prioritize and devote sufficient resources to implement its information security policies and procedures and resolve longstanding weaknesses in the FCC information security program and systems. The table below presents a summary of the FY 2015 DHS IG FISMA metrics in comparison to FY 2014 results, highlighting areas of improvement as well as those requiring continued management attention.

Summary of FY 2015 DHS IG FISMA Metrics Compared to FY 2014

2015 DHS IG FISMA Reporting Area	2014: # of DHS Exceptions/ Total DHS IG Security Metric Questions	2015: # of DHS Exceptions/ Total DHS IG Security Metric Questions	2015: Controls Effective Overall (Yes/No)	2015: Severity of Noted Exceptions
1. Continuous Monitoring Management	6 of 8	6 of 8[1]	No	Significant Deficiency
2. Configuration Management	12 of 13	6 of 12	No	Control Deficiency
3. Identity and Access Management	9 of 12	4 of 9	No	Significant Deficiency
4. Incident Response and Reporting	6 of 9	2 of 8	No	Control Deficiency
5. Risk Management	13 of 17	9 of 16	No	Significant Deficiency
6. Security Training	1 of 7	0 of 7	Yes	N/A
7. Plan of Action and Milestones (POA&M)	9 of 9	7 of 9	No	Significant Deficiency
8. Remote Access Management	6 of 13	0 of 12	Yes	N/A
9. Contingency Planning	5 of 13	7 of 12	No	Control Deficiency
10. Contractor Systems	7 of 8	5 of 7	No	Significant Deficiency

[1] For comparability purposes with the FY 2014 DHS IG FISMA metrics, Kearney responded to the eight Continuous Monitoring Management questions using *DHS IG FISMA Reporting Metrics*, dated December 18, 2014. Subsequently, on June 19, 2015, DHS issued revised reporting instructions that removed the eight security metric questions for Continuous Monitoring and replaced the questions with a maturity model for Continuous Monitoring.

Notwithstanding the progress made since FY 2014, FCC management should direct priority attention to some security control areas, particularly Continuous Monitoring Management, Identity and Access Management, Risk Management, Plan of Action and Milestones, and Contractor Systems. Kearney identified these areas as containing significant deficiencies, based on OMB's definition. Significant deficiencies require the attention of agency leadership and immediate or near-immediate corrective actions. Kearney grouped the security weaknesses discovered during the evaluation into 12 findings, many of which included weaknesses reported in previous FISMA evaluations and that remained unresolved. Based on our work performed, we concluded that the FCC's information security program was not in compliance with FISMA legislation, OMB guidance, and applicable NIST Special Publications (SP) as of September 30, 2015.

DHS introduced a new measurement technique this year in the form of an Information Security Continuous Monitoring (ISCM) Maturity Model, designed to assess the maturity of each agency's ISCM program. Kearney used the model to assess the FCC's ISCM program and concluded that it was currently at Level 2 (Defined).[2] The FCC has made progress in developing its ISCM program since its inception and should use the maturity model and other DHS resources to continue to mature its program.

Recommendations and Management Comments

Our full FY 2015 FISMA evaluation report includes 33 recommendations[3] intended to improve the effectiveness of the FCC's information security program controls in the areas of Continuous Monitoring Management, Configuration Management, Identity and Access Management, Incident Response and Reporting, Risk Management, Plan of Action and Milestones, Contingency Planning, and Contractor Systems. In many cases, the FCC was already in the process of implementing policies and procedures to strengthen security controls in these areas during our evaluation. Our report does not include recommendations in the areas of Security Training and Remote Access Management, as controls in these areas demonstrated operating effectiveness.

On November 12, 2015, the FCC's Chief Information Officer (CIO) provided a written response to a draft of the FISMA report. In the response, the CIO concurred with all 33 of the report's recommendations and described planned corrective actions that were responsive to the report's recommendations.

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

[2] In the ISCM maturity model, CIGIE has defined "Level 2 (Defined)" as "the organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organization-wide."

[3] Of the 33 recommendations, 18 recommendations are repeated from the 2014 FISMA evaluation and 19 of the 33 recommendations address security weaknesses identified as significant deficiencies.

Office of the Managing Director

MEMORANDUM

DATE: November 18, 2015

TO: David L. Hunt, Inspector General

FROM: Jon Wilkins, Managing Director
David A. Bray, Chief Information Officer
Mark Stephens, Chief Financial Officer

SUBJECT: Management Response to Federal Information Security
Management Act (FISMA) 2015 Report

Thank you for the opportunity to review and comment on the draft report entitled *Federal Information Security Management Act (FISMA) 2015 Report* detailing the results of the auditor's review of the Federal Communications Commission's (Commission or FCC) cyber security program. We appreciate the efforts of your team and the independent auditor, Kearney & Company, in support of our common goal for a safe and secure cyber-landscape.

The entire FCC team has worked hard this year since the last audit to improve our resiliency posture and FISMA assessments. While achieving perfect cyber security is not attainable given the nature of cyber threats, we at the FCC will continue to strive to do everything we can given the limitations of our legacy systems, budgetary resources, and scope as a small agency.

In FY 2015, the FCC reduced its findings by 50%, from 52 to 26. We issued a new Cyber Security Policy and achieved 99% employee and contractor Security Awareness Training completion. The FCC improved its security posture in 8 of 10 FISMA program areas evaluated. The closing of the FCC's findings from the previous audit demonstrates the Chief Information Officer's (CIO) commitment to making the FCC the most secure cyber environment possible. Given our legacy systems, budgetary resources, and scope as a small agency – management has ensured that resources have been appropriately allocated to achieve this goal.

The first step in our modernization of the FCC's historically legacy information technology (IT) infrastructure was to complete a server lift to a commercially run federal data center. The lift was successfully accomplished in September of this year, providing the FCC with a more secure environment, the agility necessary to move applications into a cloud environment, and a reduction in cost for every server decommissioned. In the work necessary to prepare for the move, more than 20% of the FCC's outdated servers were decommissioned which lowered our exposure to downtimes and breaches, improving our resiliency posture.

Prior to the server move, the FCC also moved to Office 365, the Microsoft Cloud solution, eliminating the cost of the FCC running its own overhead and providing a secure cloud environment for the FCC's e-mail and office automation efforts. Furthermore, to facilitate more secure and accessible services, the FCC implemented virtual desktop infrastructure (VDI) that enables employee and contractor remote access to FCC workstations from any location with internet access, thereby reducing the cost of the FCC having to individually patch and update individual workstations. By opting for Microsoft's Office 365 and VDI infrastructure, the FCC improved its resiliency posture versus what had been its legacy IT infrastructure.

In order to strengthen the IT organization, we made several key additions in FY 2015. Two new Deputy CIO's were put into place and a new Chief Information Security Officer (CISO) has accepted an offer to come onboard and will be in place by the end of this this month.

Of important note, the lack of clarity on the controls that FCC IT team can use in overseeing contractors led to several findings at the Universal Service Administrative Company (USAC), which serves as the administrator of the Universal Service Fund (USF). We believe that with clearer direction we will be able to better monitor and direct the operations of USAC to address the FISMA findings found there, and look forward to working together on this.

The FCC concurs with the specific findings and recommendations the auditors provided for management review. In examining these findings and recommendations and conducting a thorough analysis of the related findings, the FCC has – given the limitations of our legacy systems, budgetary resources, and scope as a small agency – provided mitigating controls for each significant deficiency or a set of management and oversight controls. We appreciate the work of the auditors and their recommendations on this topic and will certainly take them into consideration as we address our security landscape for the coming FY 2016 FISMA audit.

Together, in partnership with Bureaus and Offices across the FCC, we remain committed to strengthening the internal controls of the Commission. We look forward to working in this coming year to resolve the FY 2015 audit findings while continually enhancing the cyber security of the FCC.

Respectfully submitted,

Jon Wilkin

Jon Wilkins, Managing Director
Office of Managing Director
Federal Communications Commission

David A. Bray, Chief Information Officer
Office of Managing Director
Federal Communications Commission

Mark Stephens, Chief Financial Officer
Office of the Managing Director
Federal Communications Commission