

UNITED STATES GOVERNMENT  
FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF INSPECTOR GENERAL

## MEMORANDUM

**DATE:** December 22, 2017  
**TO:** Chairman  
**FROM:** Inspector General *FOR RM, AIG4*  
**SUBJECT:** Report on the Federal Communications Commission's (FCC) Fiscal Year 2017 Federal Information Security Management Act (FISMA) Evaluation

In accordance with 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. Specifically, the evaluation assesses FCC's compliance with FISMA requirements, DHS reporting requirements, and applicable OMB and NIST guidance for a representative subset of the FCC's information systems.

The attached Kearney report combines instances of noncompliance into nine findings, and offers 24 recommendations intended to improve the effectiveness of the FCC's information security program controls. Three of the nine findings address security weaknesses identified as significant deficiencies, of which seven findings are repeated or updated from prior year FISMA evaluations. Kearney's evaluation also included an assessment of the information security practices at USAC (Universal Service Administrative Company), the administrator of the FCC Universal Service Fund. Kearney found that USAC had remediated most of its prior year FISMA findings, but one risk management program issue remains open. During the prior year, the FCC and USAC made improvements and took corrective actions on FISMA findings that led to a decrease in recommendations from 39 in the prior fiscal year to 24 for this fiscal year. And while the FCC has improved its information security program since the prior year evaluations, six of the seven domains Kearney evaluated warrant additional management attention to address deficiencies identified, and to attain a mature information security posture. FCC management provided a written response to Kearney's draft report, which is included in its entirety as an appendix to this report.

Kearney is wholly responsible for the attached final 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.

If you have any questions, please contact Robert McGriff, Assistant Inspector General for Audit at (202) 418-0483 or Sophila Jones, Deputy Assistant Inspector General for Audit, Operations, Financial and Information Technology Division.

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



**Fiscal Year (FY) 2017  
Federal Information Security  
Modernization Act of 2014 (FISMA)  
Evaluation for the  
Federal Communications Commission**

**Report No. 17-EVAL-07-01**

**December 21, 2017**



*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](mailto:Tyler.Harding@kearneyco.com)*

**TABLE OF CONTENTS**

	<b><u>Page #</u></b>
<b>I. Evaluation Purpose .....</b>	<b>1</b>
<b>II. Background .....</b>	<b>1</b>
<b>III. Evaluation Results .....</b>	<b>2</b>
<b>IV. Recommendations .....</b>	<b>4</b>
<b>V. Management Comments .....</b>	<b>4</b>
<b>APPENDIX A: MANAGEMENT’S RESPONSE TO DETAILED FISMA REPORT .....</b>	<b>5</b>
<b>APPENDIX B: ACRONYM LIST .....</b>	<b>9</b>

## **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 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 seven domains<sup>1</sup> and organized by the five information security functions outlined in the NIST Cybersecurity Framework<sup>2</sup> to address their FISMA reporting responsibilities in the *FY 2017 Inspector General Federal Information Security Modernization Act Reporting Metrics*, dated April 17, 2017.

---

<sup>1</sup> The seven FISMA IG domains are comprised of Risk Management, Configuration Management, Identity and Access Management, Security and Privacy Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning.

<sup>2</sup> Per NIST’s *Framework for Improving Critical Infrastructure Cybersecurity*, dated February 12, 2014: “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.”



The *FY 2017 IG FISMA Reporting Metrics* marked a continuation of the work that OMB, DHS, and the Council of Inspectors General on Integrity and Efficiency (CIGIE) undertook in fiscal years (FY) 2015 and 2016 to transition IG FISMA assessments to a maturity model<sup>3</sup> approach. In previous years, CIGIE, in partnership with OMB and DHS, transitioned two of the five NIST Cybersecurity Framework Function areas (i.e., Detect and Respond) to maturity models, with other function areas utilizing maturity model indicators. For 2017, DHS provided maturity models for each FISMA metric in all seven domains and five NIST Cybersecurity Framework Function areas. Additionally, 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 area are effective. Ratings throughout the seven 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 ensures that the domain ratings are scored appropriately when entered into DHS's FISMA 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*.

We evaluated the effectiveness of the FCC's information security program and practices by designing 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 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, 2017 deadline. Our evaluation methodology met CIGIE'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 had improved its overall information security program since the FY 2016 FISMA evaluation, most notably in the areas of risk management and governance, oversight of contractors, and continuous monitoring of information systems and security functions. Additionally, the FCC continued to implement changes in its information technology (IT) environment, including shifting additional processing to the cloud and replacing legacy systems and infrastructure. Management stated those efforts required significant resources, which resulted in delays to improvements in other areas, such as the full implementation of the Homeland Security Presidential Directive 12 (HSPD-12) mandate to use Personal Identity Verification (PIV) cards for logical access to information systems. While these ongoing efforts provide the FCC with an opportunity to improve its information security posture, FCC management must fully implement their information security policies and procedures and resolve longstanding weaknesses in the FCC information security program and systems.

<sup>3</sup> 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*.



Overall, we found security weaknesses and instances of noncompliance in six of the seven domains. We grouped the security weaknesses and instances of noncompliance into nine findings, which we issued in the non-public FISMA evaluation report. Kearney considered three of the nine findings to be high-risk and classified them as significant deficiencies based on the definition from OMB Memorandum M-14-04.<sup>4</sup> Significant deficiencies require the attention of agency leadership and immediate or near-immediate corrective actions. As shown in *Exhibit 1* below, 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 (SP) as of September 15, 2017 (i.e., the end of our fieldwork).

***Exhibit 1: Summary of FY 2017 DHS IG FISMA Metric Responses***

NIST Cybersecurity Framework Function	FY 2017 DHS IG FISMA Metric Domain	Security Control Maturity	Effective?	Severity of Noted Exceptions
Identify	1.1 Risk Management	Level 3: <i>Consistently Implemented</i>	No	Significant Deficiency
Protect	2.1 Configuration Management	Level 3: <i>Consistently Implemented</i>	No	Control Deficiency
Protect	2.2 Identity and Access Management	Level 2: <i>Defined</i>	No	Significant Deficiency
Protect	2.3 Security and Privacy Training	Level 4: <i>Managed and Measurable</i>	Yes	Control Deficiency
Detect	3.1 Information Security Continuous Monitoring	Level 2: <i>Defined</i>	No	Significant Deficiency
Respond	4.1 Incident Response	Level 2: <i>Defined</i>	No	Control Deficiency
Recover	5.1 Contingency Planning	Level 3: <i>Consistently Implemented</i>	No	Control Deficiency

Source: Generated by Kearney based upon the results of testing.

Due to the changes to the IG metrics described in the **Background** section, the FY 2017 metrics were not comparable to the FY 2016 metrics. Although Kearney generally noted that the FCC made progress since FY 2016, FCC management should continue to focus on certain security control areas, particularly Risk Management, Identity and Access Management, and Information Security Continuous Monitoring.

<sup>4</sup> 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.”

#### **IV. Recommendations**

We issued 24 recommendations in the non-public FY 2017 FISMA evaluation report in an effort to improve the effectiveness of the FCC's information security program controls in the areas of Risk Management, Configuration Management, Identity and Access Management, Information Security Continuous Monitoring, Incident Response, and Contingency Planning. Our report does not include Security and Privacy Training recommendations, as the FCC demonstrated effective controls in this area. Of the 24 recommendations we issued, 18 are either repeats or updates from the FY 2016 FISMA evaluation, and 14 address security weaknesses identified as significant deficiencies. For comparison, we issued 39 recommendations in the FY 2016 FISMA evaluation report.

In many cases, we noted that the FCC was already in the process of implementing policies and procedures to strengthen security controls in several areas during our evaluation. Going forward, Kearney recommends that the FCC 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 November 27, 2017, FCC management provided a written response to a draft of the non-public FY 2017 FISMA evaluation report, which we included as **Appendix A**. 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: November 27, 2017

TO: David L. Hunt, Inspector General

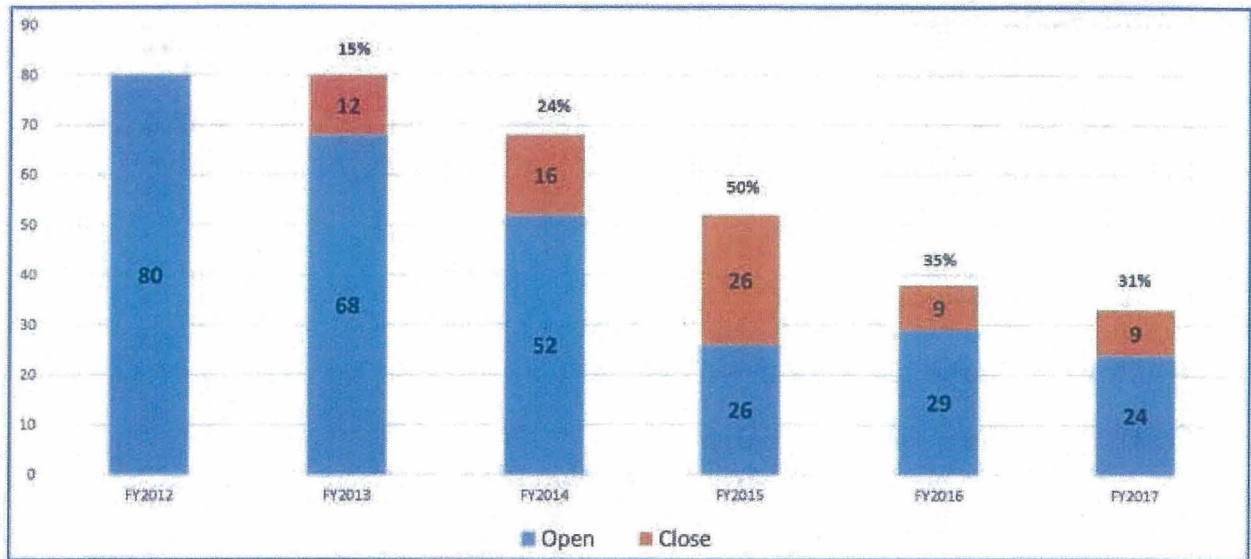
FROM: Mark Stephens, Managing Director  
Christine Calvosa, Acting Chief Information Officer  
Kathleen Heuer, Chief Financial Officer

SUBJECT: Management's Response to Independent Evaluation Report on Federal Information Security Management Act (FISMA) for Fiscal Year 2017

Thank you for the opportunity to review and comment on the draft report entitled *Fiscal Year (FY) 2017 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 2017 evaluation. The results of this year's evaluation are due to the commitment and professionalism demonstrated by both of our offices as well as independent evaluation team. During the entire evaluation, the Commission worked closely with your office and the independent evaluation team to provide necessary and timely information 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 findings from year to year in the chart below. The Commission's information technology (IT) team worked diligently throughout FY 2017 to make improvements and to resolve findings from previous years. The auditors recognized the FCC has improved its overall information security program and its compliance with FISMA and related guidance. The information security program was evaluated at between "Defined" and "Consistently Implemented", which should translate into a "Medium" score on the FISMA reporting metrics.

*FCC FISMA FINDING NUMBERS FROM FY 2012 to FY 2017*



In FY 2017, the FCC made significant progress in remediating prior-year findings associated with its oversight over the Universal Service Administration Company (USAC). Specifically, the FCC's Chief Information Officer (CIO) provided a memo to USAC leadership re-affirming USAC's requirements to comply with FISMA. Likewise, USAC leadership reciprocated and acknowledged their need to comply. In the proceeding weeks, the FCC IT team and USAC began holding bi-weekly meetings to work towards strengthening USAC's information security program.

In FY 2017, the FCC CIO and the FCC Chief Information Security Officer (CISO) led an IT Security team focused on improving the Commission's cybersecurity posture. This initiative and the work completed in prior fiscal years reduced the Commission's overall number of FISMA findings by 70% from FY 2012 to FY 2017, with a reduction by 31% in FY 2017 alone. The Commission is now working diligently to resolve the remaining findings. The FCC IT infrastructure is currently comprised of many legacy systems, and it has become a priority to modernize these systems to reduce its operational costs as well as improve its cybersecurity posture. Along with implementing modern technologies, FCC IT has also implemented enhanced processes and procedures. Furthermore, enhanced visibility into monthly metrics of the FCC's cybersecurity posture by Commission leadership has contributed to the reduction of findings across other IT related audits.



### *Steps Forward*

The FY 2017 FISMA evaluation report identifies three significant deficiencies in IT security – Risk Management, Information Security Continuous Monitoring (ISCM), and identity and access management. With sufficient funding, resources, and time, the Commission will continue to address all weaknesses in FCC’s information systems and data stores. Specifically, FCC IT will:

- Support the FCC Risk Manager in implementing a fully integrated Enterprise Risk Management (ERM) program and will ensure that information security risks are identified at the Bureau and Office level. Further, FCC IT will assist the Bureaus and Offices in performing and documenting their individual risk assessments. Focus will be placed on completing thorough system authorizations and collaborating with IT system owners to address and remediate critical Plan of Action and Milestone (POA&M) items in a timely manner.
- Be committed to completing the implementation of its ISCM Strategy and Plan. FCC IT will reduce its system vulnerabilities through a mature patch-management process in addition to continuing its quest to modernize the FCC’s legacy applications. Enhanced and meaningful metrics will be provided on a regular basis that will provide management visibility into the cybersecurity health of the application portfolio. Actionable decisions will be reviewed and prioritized.
- Focus on refining the current process of provisioning and managing user access to its information systems. FCC IT will prioritize the implementation of an automated identity and access management solution to streamline current manual processes and minimize human error, pending the availability of resources. FCC IT will evaluate potential solutions, i.e., Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification (PIV) cards, etc., to address this deficiency.

Cybersecurity is not a static target, and we must continually strive to reduce the Commission’s exposure to threats. The FCC expects to continue its cloud-based modernization efforts, which, along with strengthened processes and oversight, will eliminate a considerable number of the remaining weaknesses associated with legacy systems. The FCC will also continue to reinforce the message to USAC that cybersecurity is paramount and they must adhere to Federal guidelines and regulations.

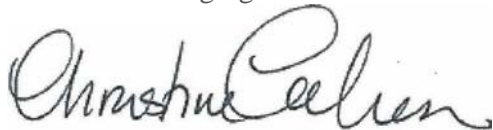
Together, in partnership with Bureaus and Offices across the Commission, we remain committed to strengthening the internal controls of the Commission. We look forward to working in this coming fiscal year to resolve the fiscal year 2017 audit findings while continuing to enhance the cybersecurity posture of the Commission.



Respectfully submitted,



Mark Stephens  
Managing Director  
Office of Managing Director



Christine Calvosa,  
Acting Chief Information Officer  
Office of Managing Director



FOR: Kathleen Heuer,  
Chief Financial Officer  
Office of Managing Director

11/27/17

**APPENDIX B: ACRONYM LIST**

<b>Acronym</b>	<b>Definition</b>
CIGIE	Council of Inspectors General on Integrity and Efficiency
Commission	Federal Communications Commission
DHS	Department of Homeland Security
FCC	Federal Communications Commission
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
HSPD-12	Homeland Security Presidential Directive 12
IG	Inspector General
IT	Information Technology
Kearney	Kearney & Company, P.C.
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
SP	Special Publication
USAC	Universal Service Administrative Company