UNITED STATES GOVERNMENT
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: March 22, 2017

TO: Chairman

FROM: Inspector General for RM, AIGA

SUBJECT: Public Report on the Federal Communications Commission's (FCC) Fiscal Year 2016 Federal Information Security Modernization Act (FISMA) Evaluation

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, the 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, including compliance with FISMA mandates and related standards.

Kearney's attached report summarizes their detailed, sensitive FISMA Evaluation Report, issued on December 09, 2016, and results of the agency Cyberscope IG FISMA metrics submitted to the Department of Homeland Security (DHS) on November 10, 2016. Kearney evaluated the eight IG FISMA metric domains and compared the results for 2016 to those for 2015. The overall score on the FCC Cybersecurity Framework Function Scorecard was 37 out of 100. The score was computed through Cyberscope based on Kearney's assessment results and responses to the questions within Cyberscope.

Although FCC has made consistent improvements in various elements of the agency's overall security program in comparison to FY 2015 results, Kearney concluded that FCC was not in compliance with FISMA legislation, OMB guidance, and applicable NIST Special Publications as of September 30, 2016. In FY 2016, Kearney identified 12 findings and offered 39 recommendations intended to improve the effectiveness of the FCC's information security program controls. Of the 39 recommendations, 25 were repeated from the FY 2015 FISMA evaluation and 22 address information security weaknesses identified as significant deficiencies. FCC management provided a written response to the detailed FISMA Evaluation Report on December 05, 2016. We 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 Audit 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 2016
Federal Information Security Modernization Act Evaluation

for the

Federal Communications Commission

January 26, 2017

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 an annual independent evaluation of their information security program and practices and to report the evaluation results to the Office of Management and Budget (OMB). FISMA states that the independent evaluation is 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 production of its annual FISMA report to Congress. Accordingly, DHS provided agency IGs with a set of security-related metrics to address their FISMA reporting responsibilities in *FY 2016 Inspector General Federal Information Security Modernization Act Reporting Metrics, Version 1.1.3,* dated September 26, 2016.

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 metrics. The FCC IG was required to submit responses to the metrics through DHS's FISMA reporting platform, CyberScope, by November 10, 2016. Additionally, we followed up on findings reported in previous FISMA evaluations to determine whether risks have been properly mitigated. Our evaluation methodology met the Council of Inspectors General on Integrity and Efficiency (CIGIE) *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.

Evaluation Results

The FCC has improved its overall information security program since the fiscal year (FY) 2015 evaluation, most notably in establishing a formal information technology (IT) risk management and governance program. Additionally, the FCC continues to implement changes in its IT environment, including shifting additional processing to the cloud and replacing legacy systems and infrastructure. Management stated these efforts have required significant resources, delaying the full implementation of the risk management program and the Homeland Security Presidential Directive 12 (HSPD-12) mandate to use Personal Identity Verification (PIV) cards for logical access to information systems. While these changes provide the FCC with an opportunity to improve its information security posture, management must prioritize and devote sufficient resources to fully 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 2016 DHS IG FISMA metrics in comparison to FY 2015 results, highlighting areas of improvement as well as those requiring continued management attention. For domains in which DHS provides a maturity model rather than individual metric questions, the results indicate the level of maturity attained for each of the three areas.[1] The overall maturity level is the lowest of the three area levels.

Summary of FY 2016 DHS IG FISMA Responses Compared to FY 2015

2016 DHS IG FISMA Metric Domain (Security Function)	2015: # of Exceptions/ Total Metric Questions	2016: # of Exceptions/ Total Metric Questions	2016: Program Effective?	2016: Severity of Noted Exceptions
1.1 Risk Management (Identify)	9 of 16 (Risk Management 7 of 9 (POA&M)	10 of 17	No	Significant Deficiency
1.2. Contractor Systems (Identify)	5 of 7	2 of 4	No	Significant Deficiency
2.1 Configuration Management (Protect)	6 of 12	3 of 10	No	Control Deficiency
2.2 Identity and Access Management (I&AM) (Protect)	4 of 9 (I&AM) 0 of 12 (Remote Access)	10 of 15	No	Significant Deficiency
2.3 Security and Privacy Training (Protect)	0 of 7	0 of 6	Yes	N/A
3.1 Information Security Continuous Monitoring (Detect)[2]	Level 2 for People, Processes, and Technology	Level 2 for People and Processes; Level 3 for Technology	No	Significant Deficiency
4.1 Incident Response (Respond)[3]	2 of 8	Level 3 for Processes and Technology; Level 4 for People	No	Control Deficiency
5.1 Contingency Planning (Recover)	7 of 12	7 of 11	No	Control Deficiency

Note: For FY 2016, DHS combined some FY 2015 metric domains. Plan of Action and Milestones (POA&M) was included with Risk Management and Remote Access was included with Identity and Access Management.

[1] The maturity models include 5 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.
[2] DHS provided a maturity model for Information Security Continuous Monitoring for both FY 2015 and FY 2016.
[3] DHS provided individual metrics for Incident Response in FY 2015 and a maturity model in FY 2016.

While FCC has made progress since FY 2015, FCC management should direct priority attention to some security control areas, particularly Information Security Continuous Monitoring (ISCM), Identity and Access Management (I&AM), Risk Management, and Contractor Systems. Kearney identified these areas as containing significant deficiencies, based on the definition from OMB Memorandum M-14-04. 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 include unresolved weaknesses reported in previous FISMA evaluations. 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, 2016.

New DHS Metrics Scoring. DHS introduced the ISCM Maturity Model in 2015 and added the Incident Response Maturity Model for 2016. DHS also created "maturity model indicators" for the metrics in security domains without maturity models and a scoring system based on the metric assessment results. Kearney used the metrics and the two maturity models to assess the FCC's information security program and concluded that the FCC scored 37 points out of a possible 100 points using the DHS scoring criteria. This score will serve as a benchmark for measuring future improvements in information security. In 2016 DHS also established criteria for determining if an agency's security program was effective in each of the eight security metric domains. Based on these criteria, the FCC's security program was not effective in seven of the eight domains, as indicated in the table above.

Recommendations

Our full FY 2016 FISMA evaluation report includes 39 recommendations 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. Of the 39 recommendations, 25 are repeated from the 2015 FISMA evaluation and 22 recommendations address security weaknesses identified as significant deficiencies. The 2015 FISMA evaluation included a total of 33 recommendations. 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. However, FCC management should prioritize their implementation of the recommendations in the allocation of effort and resources. Our report does not include recommendations in the area of Security and Privacy Training as controls in this area demonstrated operating effectiveness.

Management Comments

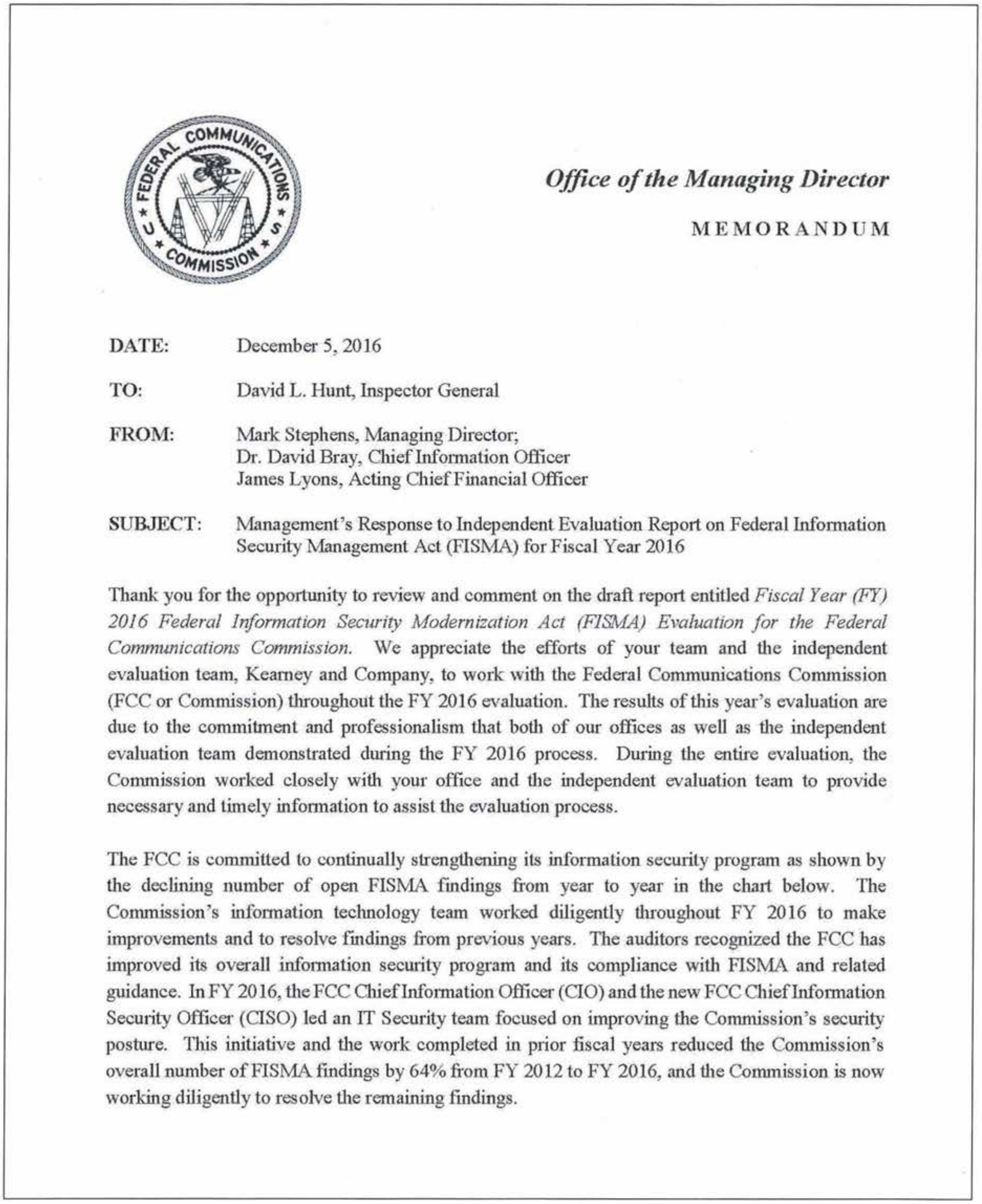
On December 05, 2016, the Office of the Managing Director provided a written response to a draft of the FISMA report, provided as Appendix A. On page 3 of the Commission's response, the Commission requested that Kearney document the agency's communications with USAC in the report. After the completion of the FISMA fieldwork and the release of the draft FISMA report, the Commission stated its efforts to engage and collaborate with USAC regarding the Commission's third party oversight. Despite the actions taken by the Commission, our evaluation continued to identify recurring information security weaknesses at USAC and noncompliance with the FISMA legislation and NIST information security guidance. We encourage the Commission to continue to expand its third party oversight efforts. Kearney prepared a detailed FISMA report that contained sensitive, non-public information for the FCC OIG and Management. The detailed FISMA report included three recommendations designed to provide adequate security for FCC data maintained by USAC. Because the detailed FISMA report contains sensitive, non-public information concerning the FCC's information security program, the FCC OIG does not intend to release the report publicly.

Sincerely,

Kearney & Company

Kearney & Company, P.C.
January 26, 2017

APPENDIX A: MANAGEMENT'S RESPONSE TO DETAILED FISMA REPORT



Office of the Managing Director

MEMORANDUM

DATE: December 5, 2016

TO: David L. Hunt, Inspector General

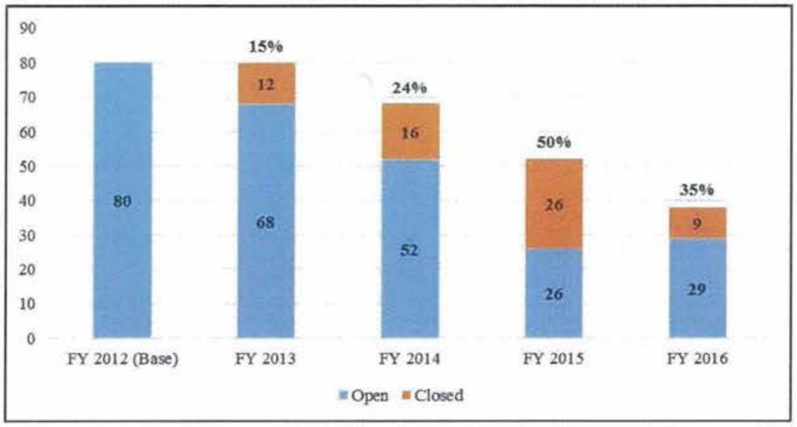
FROM: Mark Stephens, Managing Director;
Dr. David Bray, Chief Information Officer
James Lyons, Acting Chief Financial Officer

SUBJECT: Management's Response to Independent Evaluation Report on Federal Information Security Management Act (FISMA) for Fiscal Year 2016

Thank you for the opportunity to review and comment on the draft report entitled *Fiscal Year (FY) 2016 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 2016 evaluation. The results of this year's evaluation are due to the commitment and professionalism that both of our offices as well as the independent evaluation team demonstrated during the FY 2016 process. 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 team worked diligently throughout FY 2016 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. In FY 2016, the FCC Chief Information Officer (CIO) and the new FCC Chief Information Security Officer (CISO) led an IT Security team focused on improving the Commission's security posture. This initiative and the work completed in prior fiscal years reduced the Commission's overall number of FISMA findings by 64% from FY 2012 to FY 2016, and the Commission is now working diligently to resolve the remaining findings.

FCC FISMA FINDING NUMBERS FROM FY 2012 to FY 2016

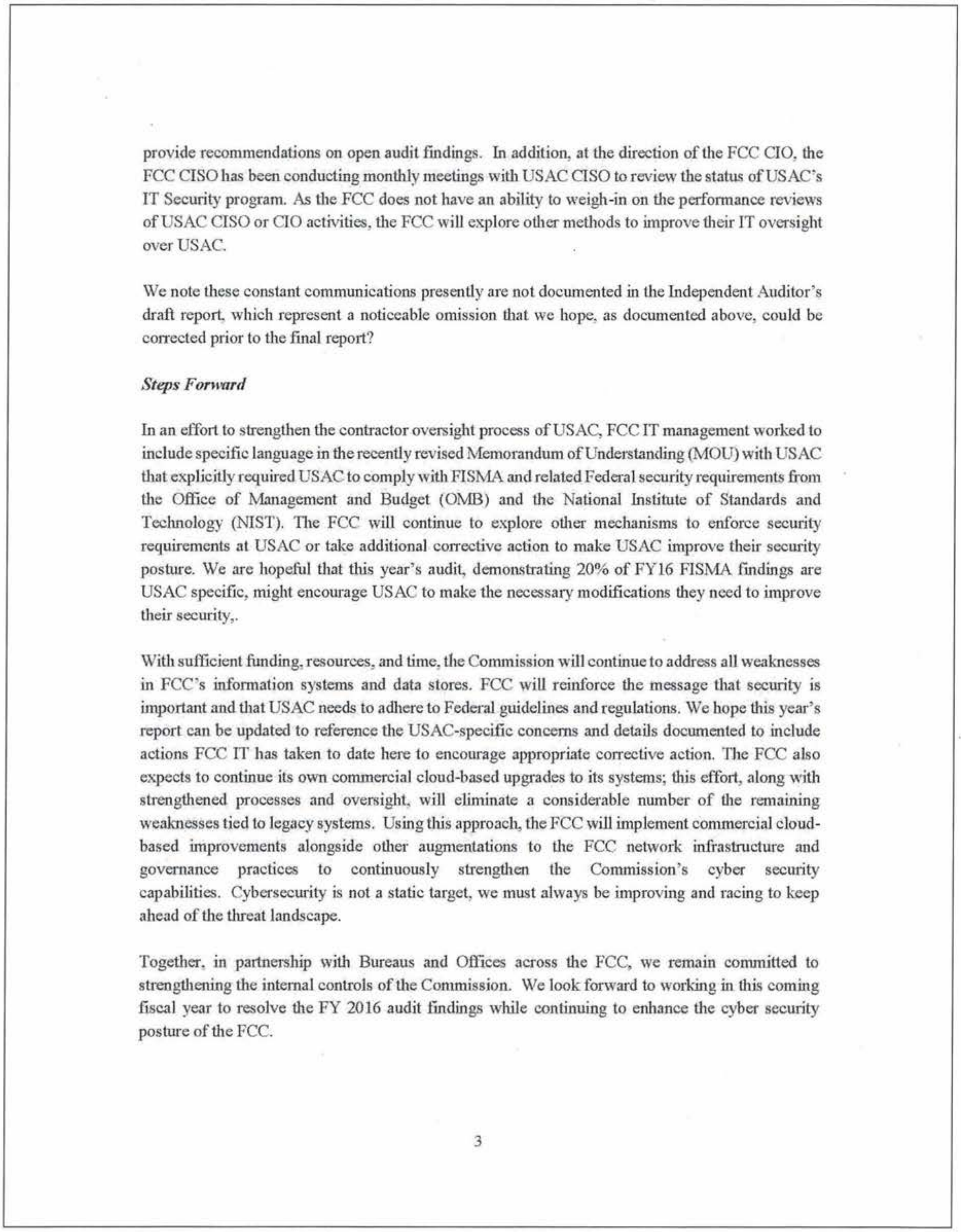


Addressing Oversight of the Universal Service Administrative Company's IT

It is important to note that 20% of the FY 2016 FISMA findings are Universal Service Administrative Company (USAC) specific. The FCC had challenges with establishing authority over contractor systems, specifically an entity like USAC which serves as the administrator of the Universal Service Fund (USF). The FCC will work to better monitor and direct the operations of USAC to address the FISMA findings found there, and we look forward to working together on this.

Since 2013, FCC IT Management has worked aggressively and diligently with USAC to communicate and enforce the FISMA requirements. In December 2013, shortly after the arrival of the new FCC CIO, the FCC CIO specifically engaged an independent assessor to conduct an evaluation of USAC's IT challenges that yielded specific guidance and direction to improve their security posture. FCC conducts an independent audit of Universal Service Administrative Company internal control over financial reporting on an annual basis. This guidance and direction was shared with USAC, though as noted, USAC operates its IT autonomously with Commission oversight. In addition, the FCC established an audit follow up process with USAC to review and track USAC's corrective actions to address findings resulting from various audits in an effort to further encourage USAC to take the corrective actions through communication, diplomacy, and monitoring.

FCC IT Management has been in constant contact with USAC to encourage and support USAC's quest to improve their IT Security posture. A subset of these communications are documented in FCC IT Management's targeted communications with USAC on December 28, 2013; April 2, 2014; June 17, 2014; September 30, 2014; and June 12, 2015 specifically to review, collaborate, and



provide recommendations on open audit findings. In addition, at the direction of the FCC CIO, the FCC CISO has been conducting monthly meetings with USAC CISO to review the status of USAC's IT Security program. As the FCC does not have an ability to weigh-in on the performance reviews of USAC CISO or CIO activities, the FCC will explore other methods to improve their IT oversight over USAC.

We note these constant communications presently are not documented in the Independent Auditor's draft report, which represent a noticeable omission that we hope, as documented above, could be corrected prior to the final report?

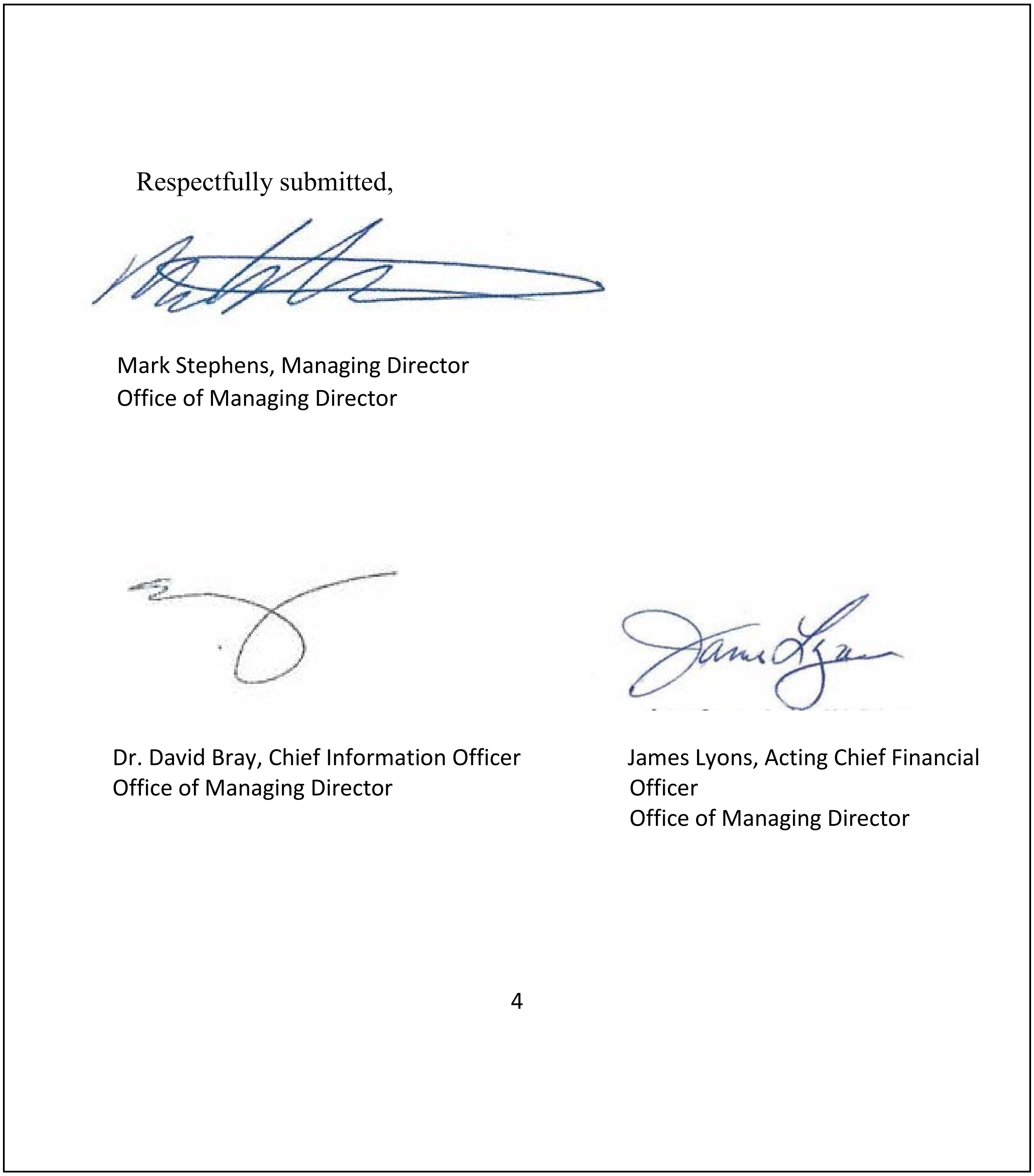
Steps Forward

In an effort to strengthen the contractor oversight process of USAC, FCC IT management worked to include specific language in the recently revised Memorandum of Understanding (MOU) with USAC that explicitly required USAC to comply with FISMA and related Federal security requirements from the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). The FCC will continue to explore other mechanisms to enforce security requirements at USAC or take additional corrective action to make USAC improve their security posture. We are hopeful that this year's audit, demonstrating 20% of FY16 FISMA findings are USAC specific, might encourage USAC to make the necessary modifications they need to improve their security,.

With sufficient funding, resources, and time, the Commission will continue to address all weaknesses in FCC's information systems and data stores. FCC will reinforce the message that security is important and that USAC needs to adhere to Federal guidelines and regulations. We hope this year's report can be updated to reference the USAC-specific concerns and details documented to include actions FCC IT has taken to date here to encourage appropriate corrective action. The FCC also expects to continue its own commercial cloud-based upgrades to its systems; this effort, along with strengthened processes and oversight, will eliminate a considerable number of the remaining weaknesses tied to legacy systems. Using this approach, the FCC will implement commercial cloud-based improvements alongside other augmentations to the FCC network infrastructure and governance practices to continuously strengthen the Commission's cyber security capabilities. Cybersecurity is not a static target, we must always be improving and racing to keep ahead of the threat landscape.

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 fiscal year to resolve the FY 2016 audit findings while continuing to enhance the cyber security posture of the FCC.

3



Respectfully submitted,

Mark Stephens, Managing Director
Office of Managing Director

Dr. David Bray, Chief Information Officer
Office of Managing Director

James Lyons, Acting Chief Financial Officer
Office of Managing Director