OFFICE OF
INSPECTOR GENERAL
FEDERAL COMMUNICATIONS COMMISSION

45 L Street NE, Washington, DC 20554
www.fcc.gov/inspector-general

[PUBLIC]

Federal Communications Commission's FY 2025 Federal Information Security Modernization Act Evaluation

Report Number: 25-EVAL-04-01

December 18, 2025

TABLE OF CONTENTS

Page #

I. Evaluation Purpose

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 agency Inspector General (IG) or an IG-determined independent external evaluator must perform the independent evaluations. The FCC Office of Inspector General (FCC OIG) contracted with Kearney & Company, P.C. (defined as "Kearney," "we," and "our" in this report) to conduct FCC's fiscal year (FY) 2025 evaluation. The objective of this evaluation was to determine the effectiveness of information security policies, procedures, and practices of a representative subset of 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 FCC as the administrator of the Federal Universal Service Fund (USF). In addition, Kearney followed up on findings and recommendations reported in previous FISMA evaluations to determine whether previously identified risks were properly mitigated.

II. Background

To achieve its mission of regulating interstate and international communications, FCC must safeguard the sensitive information 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 in the *FY 2025 IG FISMA Reporting Metrics*. Specifically, DHS includes 20 core metrics, along with five supplemental metrics, which were grouped into 10 domains and organized by the six information security functions outlined in the NIST Cybersecurity Framework (CSF) 2.0 to address their FISMA reporting responsibilities in the *FY 2025 IG FISMA Reporting Metrics*. ***Exhibit 1*** presents the IG FISMA metrics structure and the corresponding six information security functions and 10 metric domains.

Exhibit 1: CSF Functions and Associated Metric Domains

CSF Function	*FY 2025 IG FISMA Metric Domain*
Govern[1]	Cybersecurity Governance
	Cybersecurity Supply Chain Risk Management
Identify	Risk and Asset 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 2025 IG FISMA Reporting Metrics

For FY 2025, DHS provided maturity models for each FISMA metric in all 10 domains and six NIST CSF Function areas. ***Exhibit 2*** presents the maturity levels within DHS's maturity model structure, from lowest to highest maturity, 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 use quantitative and qualitative metrics 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 2025 IG FISMA Reporting Metrics

Using the five maturity levels above, DHS instituted a scoring system to determine the degree of maturity of an agency's information security programs, as well as specific criteria to identify whether the agency's program in each CSF function was effective. Ratings throughout the 10

[1] CSF 2.0 introduced Govern as the sixth function and it was included in the *FY 2025 FISMA Reporting Metrics*. Furthermore, Cybersecurity Governance was added as a domain within the function, and Cybersecurity Supply Chain Risk Management, previously in the Identify function, was realigned to the Govern function.

domains are determined based on a calculated average, wherein the average of the metrics within each domain is used to determine the effectiveness of individual function areas and the overall information security program. With the calculated average scoring model, core and supplemental metrics are averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. While DHS and OMB encourage IGs to focus on the results of the core metrics and use the calculated average of the supplemental metrics as a data point to support risk-based determination of the overall program and function-level effectiveness, IGs have the discretion to determine the overall effectiveness rating and the rating for each function based on their assessment. If all the metrics are fully satisfied at the highest maturity capability, then the function is scored at Level 5: *Optimized*. DHS further stipulates that a program must achieve at least Level 4: *Managed and Measurable* to be considered effective.

Kearney evaluated the effectiveness of FCC's information security program and practices by designing procedures to assess consistency between the Commission's security controls and FISMA requirements, OMB policy guidance 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 FCC had taken appropriate corrective actions and properly mitigated the related risks. Kearney provided the results of our evaluation to the FCC OIG to use in submitting the IG responses to the DHS metrics through CyberScope by the August 1, 2025 deadline. We also issued a detailed non-public FISMA report to FCC management, which contains sensitive information about FCC's information security program. Accordingly, the FCC OIG does not intend to release that report publicly.

As required by our contract, the evaluation was conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) *Quality Standards for Inspection and Evaluation.* Our methodology included inquiries, observations, and inspection of FCC and USAC documents and records, as well as direct testing of controls.

III. Evaluation Results

As shown in ***Exhibit 3***, as of June 2025 (i.e., the end of our fieldwork), we concluded that the Commission's overall information security program was ineffective and not in compliance with FISMA legislation, OMB guidance, and applicable NIST Special Publications (SP), based on the *FY 2025 IG FISMA Reporting Metrics*. However, FCC's information security program was effective and in compliance for two of the 10 domain areas, and one of those areas reflected improvement from the Level 3 to the Level 4 maturity level from last year's evaluation.

Exhibit 3: FCC Security Control Effectiveness as of June 30, 2025

NIST CSF Function	FY 2025 IG FISMA Metric Domain	FY 2024 Maturity Level	FY 2025 Maturity Level	Effective?
Govern	Cybersecurity Governance	Not applicable (N/A)	Level 2: *Defined*	No
Govern	Cybersecurity Supply Chain Risk Management	Level 2: *Defined*	Level 2: *Defined*	No
Identify	Risk and Asset Management	Level 2: *Defined*	Level 2: *Defined*	No
Protect	Configuration Management	Level 2: *Defined*	Level 2: *Defined*	No
Protect	Identity and Access Management	Level 2: *Defined*	Level 2: *Defined*	No
Protect	Data Protection and Privacy	Level 3: *Consistently Implemented*	Level 3: *Consistently Implemented*	No
Protect	Security Training	Level 3: *Consistently Implemented*	Level 4: *Managed and Measurable*	Yes
Detect	Information Security Continuous Monitoring	Level 2: *Defined*	Level 2: *Defined*	No
Respond	Incident Response	Level 3: *Consistently Implemented*	Level 3: *Consistently Implemented*	No
Recover	Contingency Planning	Level 4: *Managed and Measurable*	Level 4: *Managed and Measurable*	Yes

Source: Kearney-created from the results of the FY 2025 FCC FISMA evaluation

During FY 2025, FCC continued efforts to define and implement an organization-wide information security program. For example, Kearney noted that FCC implemented corrective actions to close 13 recommendations from prior years. This includes longstanding recommendations in Identity and Access Management, related to account management for both non-privileged and privileged users. In addition, FCC implemented corrective actions related to the system inventory and developed a supply chain risk management strategy. However, additional steps remain to develop, implement, and operate an effective program.

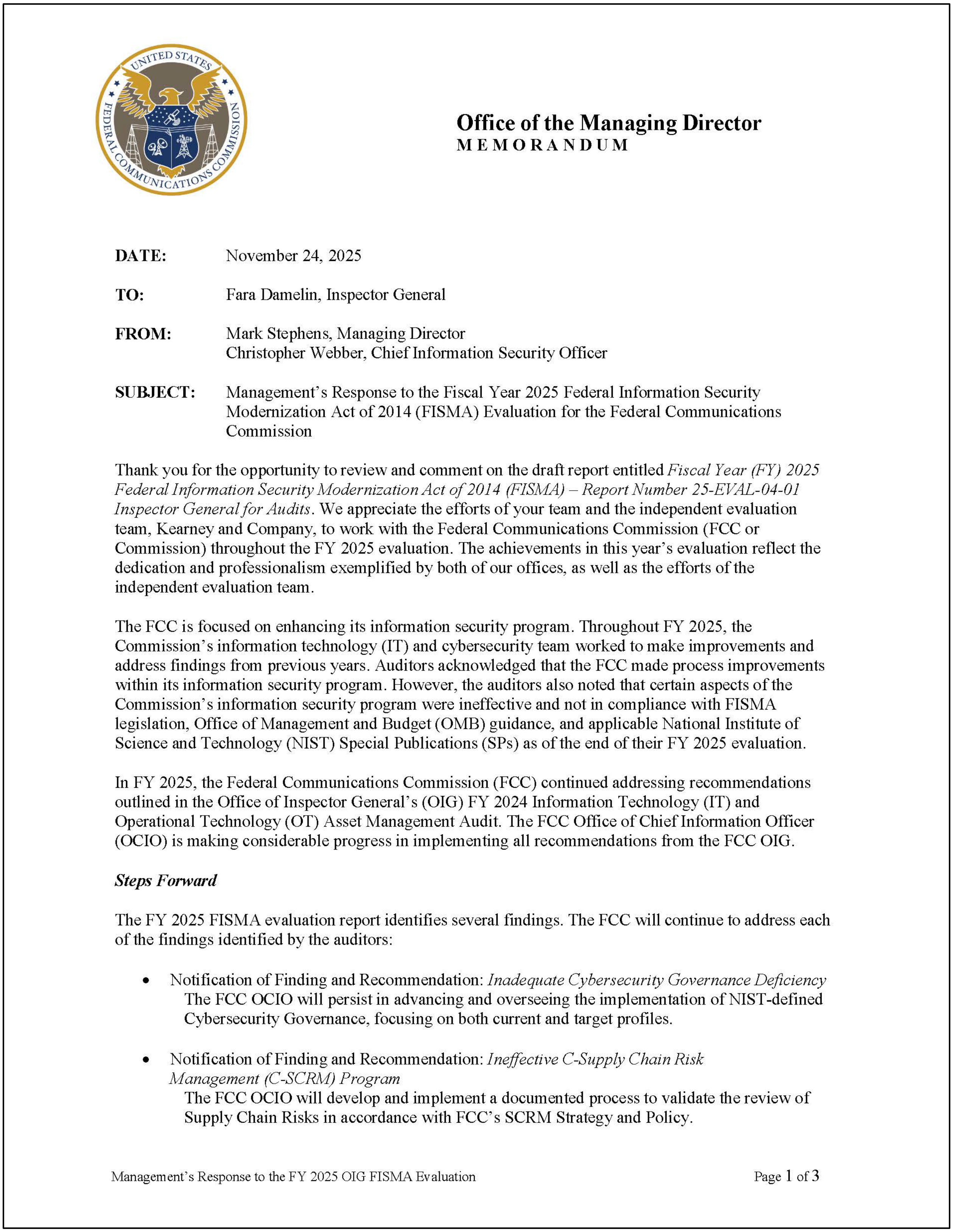
Overall, we identified deficiencies and instances of noncompliance in six of the 10 domains. Kearney grouped the deficiencies and instances of noncompliance from those six domains into nine findings, which we issued in a non-public FISMA evaluation report. The deficiencies identified during the FY 2025 FISMA evaluation require the attention of agency leadership and immediate or near-immediate corrective actions.

IV. Recommendations

Kearney issued 27 recommendations in the non-public FY 2025 FISMA evaluation report to improve the effectiveness of FCC's information security program controls in the areas of Cybersecurity Governance, Cybersecurity Supply Chain Risk Management, Risk and Asset Management, Configuration Management, Identity and Access Management, and Information Security Continuous Monitoring. Of the 27 recommendations we issued, 14 are repeats from prior FISMA evaluations, and 13 address additional deficiencies identified in FY 2025.

We noted that FCC was in the process of implementing policies and procedures to strengthen security controls in several areas during our evaluation. The Commission should continue to prioritize and implement its documented security policies and procedures, as well as establish ongoing monitoring over all six NIST CSF 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: November 24, 2025

TO: Fara Damelin, Inspector General

FROM: Mark Stephens, Managing Director
Christopher Webber, Chief Information Security Officer

SUBJECT: Management's Response to the Fiscal Year 2025 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) 2025 Federal Information Security Modernization Act of 2014 (FISMA) – Report Number 25-EVAL-04-01 Inspector General for Audits*. 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 2025 evaluation. The achievements in this year's evaluation reflect the dedication and professionalism exemplified by both of our offices, as well as the efforts of the independent evaluation team.

The FCC is focused on enhancing its information security program. Throughout FY 2025, the Commission's information technology (IT) and cybersecurity team worked to make improvements and address findings from previous years. Auditors acknowledged that the FCC made process improvements within its information security program. However, the auditors also noted that certain 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 their FY 2025 evaluation.

In FY 2025, the Federal Communications Commission (FCC) continued addressing recommendations outlined in the Office of Inspector General's (OIG) FY 2024 Information Technology (IT) and Operational Technology (OT) Asset Management Audit. The FCC Office of Chief Information Officer (OCIO) is making considerable progress in implementing all recommendations from the FCC OIG.

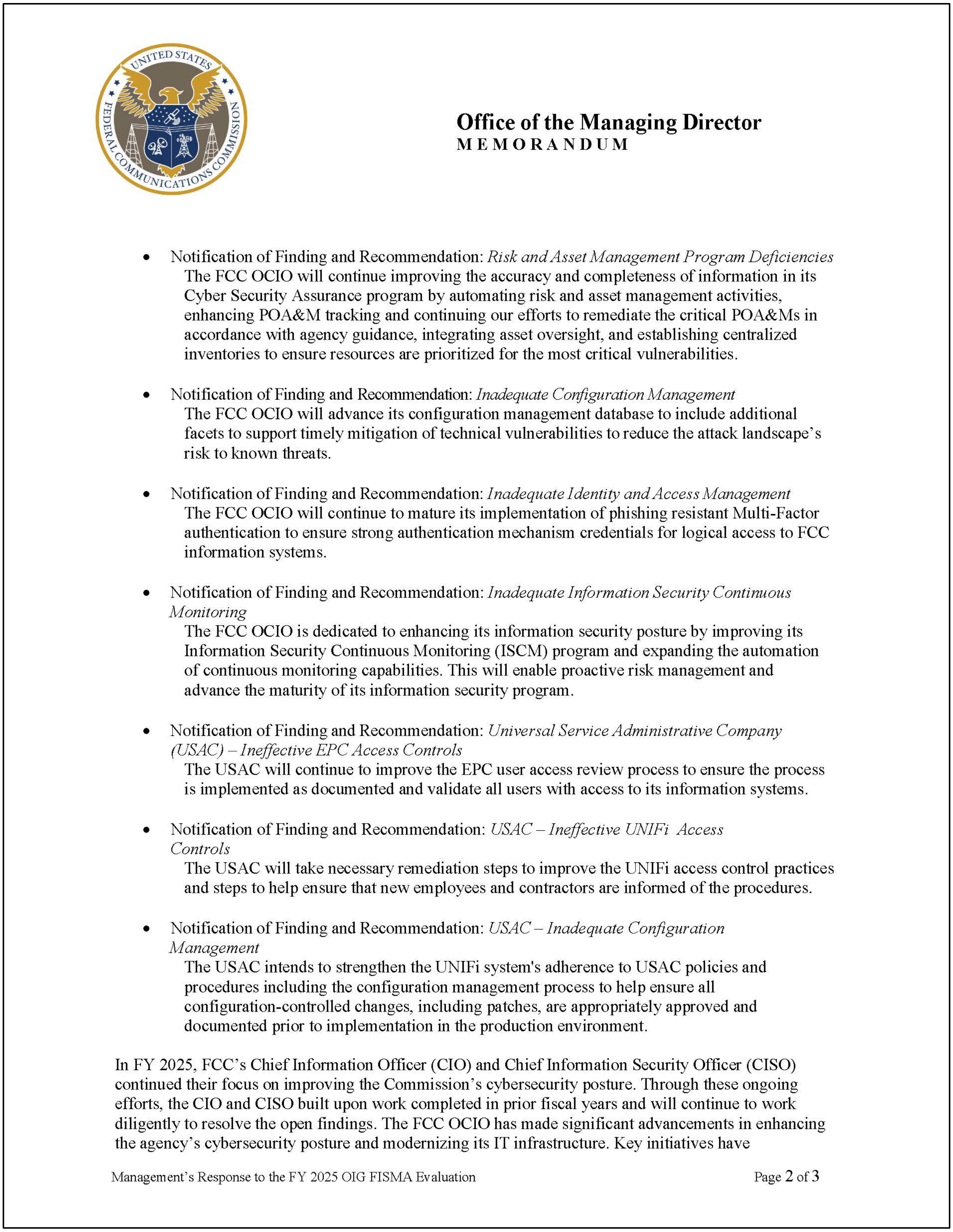
Steps Forward

The FY 2025 FISMA evaluation report identifies several findings. The FCC will continue to address each of the findings identified by the auditors:

- Notification of Finding and Recommendation: *Inadequate Cybersecurity Governance Deficiency*
  The FCC OCIO will persist in advancing and overseeing the implementation of NIST-defined Cybersecurity Governance, focusing on both current and target profiles.

- Notification of Finding and Recommendation: *Ineffective C-Supply Chain Risk Management (C-SCRM) Program*
  The FCC OCIO will develop and implement a documented process to validate the review of Supply Chain Risks in accordance with FCC's SCRM Strategy and Policy.

Management's Response to the FY 2025 OIG FISMA Evaluation Page 1 of 3



- Notification of Finding and Recommendation: *Risk and Asset Management Program Deficiencies*
  The FCC OCIO will continue improving the accuracy and completeness of information in its Cyber Security Assurance program by automating risk and asset management activities, enhancing POA&M tracking and continuing our efforts to remediate the critical POA&Ms in accordance with agency guidance, integrating asset oversight, and establishing centralized inventories to ensure resources are prioritized for the most critical vulnerabilities.

- Notification of Finding and Recommendation: *Inadequate Configuration Management*
  The FCC OCIO will advance its configuration management database to include additional facets to support timely mitigation of technical vulnerabilities to reduce the attack landscape's risk to known threats.

- Notification of Finding and Recommendation: *Inadequate Identity and Access Management*
  The FCC OCIO will continue to mature its implementation of phishing resistant Multi-Factor authentication to ensure strong authentication mechanism credentials for logical access to FCC information systems.

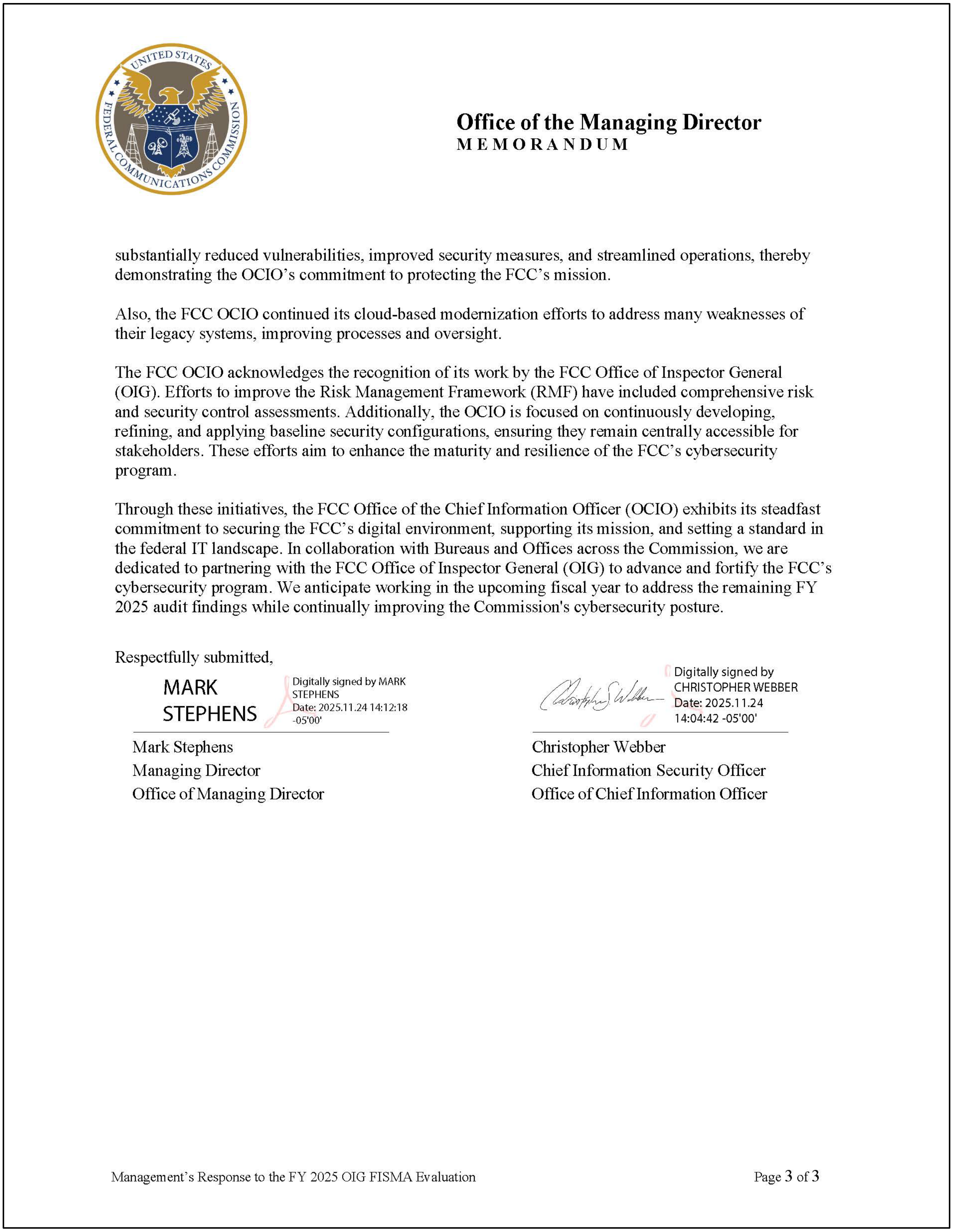
- Notification of Finding and Recommendation: *Inadequate Information Security Continuous Monitoring*
  The FCC OCIO is dedicated to enhancing its information security posture by improving its Information Security Continuous Monitoring (ISCM) program and expanding the automation of continuous monitoring capabilities. This will enable proactive risk management and advance the maturity of its information security program.

- Notification of Finding and Recommendation: *Universal Service Administrative Company (USAC) – Ineffective EPC Access Controls*
  The USAC will continue to improve the EPC user access review process to ensure the process is implemented as documented and validate all users with access to its information systems.

- Notification of Finding and Recommendation: *USAC – Ineffective UNIFi Access Controls*
  The USAC will take necessary remediation steps to improve the UNIFi access control practices and steps to help ensure that new employees and contractors are informed of the procedures.

- Notification of Finding and Recommendation: *USAC – Inadequate Configuration Management*
  The USAC intends to strengthen the UNIFi system's adherence to USAC policies and procedures including the configuration management process to help ensure all configuration-controlled changes, including patches, are appropriately approved and documented prior to implementation in the production environment.

In FY 2025, FCC's Chief Information Officer (CIO) and Chief Information Security Officer (CISO) continued their focus on improving the Commission's cybersecurity posture. Through these ongoing efforts, the CIO and CISO built upon work completed in prior fiscal years and will continue to work diligently to resolve the open findings. The FCC OCIO has made significant advancements in enhancing the agency's cybersecurity posture and modernizing its IT infrastructure. Key initiatives have



Office of the Managing Director
MEMORANDUM

substantially reduced vulnerabilities, improved security measures, and streamlined operations, thereby demonstrating the OCIO's commitment to protecting the FCC's mission.

Also, the FCC OCIO continued its cloud-based modernization efforts to address many weaknesses of their legacy systems, improving processes and oversight.

The FCC OCIO acknowledges the recognition of its work by the FCC Office of Inspector General (OIG). Efforts to improve the Risk Management Framework (RMF) have included comprehensive risk and security control assessments. Additionally, the OCIO is focused on continuously developing, refining, and applying baseline security configurations, ensuring they remain centrally accessible for stakeholders. These efforts aim to enhance the maturity and resilience of the FCC's cybersecurity program.

Through these initiatives, the FCC Office of the Chief Information Officer (OCIO) exhibits its steadfast commitment to securing the FCC's digital environment, supporting its mission, and setting a standard in the federal IT landscape. In collaboration with Bureaus and Offices across the Commission, we are dedicated to partnering with the FCC Office of Inspector General (OIG) to advance and fortify the FCC's cybersecurity program. We anticipate working in the upcoming fiscal year to address the remaining FY 2025 audit findings while continually improving the Commission's cybersecurity posture.

Respectfully submitted,

MARK
STEPHENS
Digitally signed by MARK
STEPHENS
Date: 2025.11.24 14:12:18
-05'00'

Mark Stephens
Managing Director
Office of Managing Director

Digitally signed by
CHRISTOPHER WEBBER
Date: 2025.11.24
14:04:42 -05'00'

Christopher Webber
Chief Information Security Officer
Office of Chief Information Officer

APPENDIX B: ACRONYM LIST

Acronym	Definition
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CSF	Cybersecurity Framework
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.
N/A	Not applicable
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
SP	Special Publication
USAC	Universal Service Administrative Company
USF	Universal Service Fund

Report Fraud, Waste, and Abuse

We accept tips and complaints from all sources about potential fraud, waste, abuse, and mismanagement in FCC programs

Contact:

PHONE: 1-888-863-2244 or 202-418-0473

WEBSITE: https://www.fcc.gov/inspector-general/hotline

Who can report?

Anyone who suspects fraud, waste, and abuse in an FCC program should report their concerns to OIG. We investigate alleged or suspected fraud and other misconduct related to all FCC programs and operations.

How Does it help?

By reporting concerns to OIG, you help us perform effective oversight, safeguard taxpayer investments, and increase FCC program integrity.

Who is protected?

The Privacy Act, the Inspector General Act, and other applicable laws protect people who report fraud, waste, and abuse. The Inspector General Act of 1978 states that the Inspector General shall not disclose the identity of an employee who reports an allegation or provides information without the employee's consent, unless the Inspector General determines that disclosure is unavoidable during the investigation. By law, Federal employees may not take or threaten to take a personnel action because of whistleblowing or the exercise of a lawful appeal, complaint, or grievance right. Non-FCC employees who report allegations may also specifically request confidentiality.

OFFICE OF INSPECTOR GENERAL
OIG
FEDERAL COMMUNICATIONS COMMISSION

Stay in Touch *with*
FCC Office of Inspector General

Follow us: FCC OIG

https://www.fcc.gov/inspector-general