OFFICE OF
INSPECTOR GENERAL
FEDERAL COMMUNICATIONS COMMISSION

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

FCC OIG Office of Audits Closed Recommendations Report

(April 1, 2025 – September 30, 2025)

FCC OIG Office of Audits
Closed Recommendations Report
April 1, 2025 through September 30, 2025

EXECUTIVE SUMMARY

Pursuant to our oversight mission, the Federal Communications Commission Office of Inspector General (FCC OIG) conducts audits, inspections, and evaluations and issues recommendations to the Commission to address identified findings and risks. FCC OIG monitors the Commission's progress in taking associated corrective actions. When the Commission provides adequate support that it has addressed and implemented each recommendation, FCC OIG closes the recommendation.

As demonstrated in the following table, between April 1, 2025, and September 30, 2025, FCC has taken action and provided associated documentation to close 18 recommendations. Seventeen of these closures resulted from corrective actions taken by the FCC, and one was an administrative closure resulting from a recommendation that is no longer actionable.

The purpose of this product is to provide an overview of the corrective actions taken by FCC to close these recommendations, with a description of the associated impact of each closure. Several recommendations are considered sensitive and contain non-public information. For those, we provide modified descriptions to avoid the release of sensitive and non-public information.

We appreciate FCC's cooperation in taking the below referenced corrective actions. We look forward to continuing to coordinate with the Commission as it works to address remaining open recommendations.

Table 1: Closed Recommendations

Number	Project Name	Recommendation	Action Taken by the FCC	Impact of Closure
1	FY 2024 Federal Information Security Modernization Act Evaluation	20. Identity and Access Management	FCC implemented and updated policies and procedures.	Strengthens the FCC's cybersecurity program for identity and access management.
2	FY 2024 Federal Information Security Modernization Act Evaluation	22. Access Controls	FCC decommissioned the application where a prior year access control weakness was identified. However, test work completed in FY 2025 surrounding the new system identified similar access control issues. Thus, the old recommendation was closed, and a new recommendation was issued to reflect the access control issue in the new system.	N/A Administrative closure
3	FY 2024 Federal Information Security Modernization Act Evaluation	23. Access Controls	FCC ensured that all managers provided responses during the review period and all users received a response from their manager.	Reduces the Commission's risk of unauthorized or excessive access, to avoid unauthorized use of information systems.
4	FY 2023 Federal Information Security Modernization Act Evaluation	2. Risk and Asset Management	FCC updated its system inventory.	Ensures that FCC's information systems have appropriate oversight and implementation of security controls.
5	FY 2023 Federal Information Security Modernization Act Evaluation	6. Cybersecurity Supply Chain Risk Management (SCRM)	FCC developed and implemented an organization-wide SCRM strategy.	Ensures that the Commission addresses the management of supply chain risks.
6	FY 2023 Federal Information Security Modernization Act Evaluation	17. Identity and Access Management	FCC effectively enforced its policies and procedures regarding account management.	Reduces the Commission's risk that users may have inappropriate access.

Number	Project Name	Recommendation	Action Taken by the FCC	Impact of Closure
7	FY 2023 Federal Information Security Modernization Act Evaluation	18. Identity and Access Management	FCC effectively documented and implemented a quality control checklist.	Provides reasonable assurance that access rights are timely reviewed.
8	FY 2022 Federal Information Security Modernization Act Evaluation	12. Identity and Access Management	FCC effectively documented and implemented a quality control checklist.	Ensures consistency, accuracy, and security access throughout the user lifecycle.
9	FY 2022 Federal Information Security Modernization Act Evaluation	13. Identity and Access Management	FCC effectively implemented the documented process enhancements and completed a review of privileged accounts.	Ensures regulatory compliance and increases operational efficiency.
10	FY 2022 Federal Information Security Modernization Act Evaluation	14. Identity and Access Management	FCC defined policies and procedures for the maintenance of and review over test accounts.	Enhances security and improves testing accuracy.
11	FY 2022 Federal Information Security Modernization Act Evaluation	17. Configuration Management	FCC effectively established and documented configuration settings.	Ensures systems operate as intended.
12	FY 2022 Federal Information Security Modernization Act Evaluation	18. Configuration Management	FCC effectively performed configuration scans and documented non-compliant controls and remediation plans.	Mitigates security risks.

Number	Project Name	Recommendation	Action Taken by the FCC	Impact of Closure
13	FY 2019 Federal Information Security Modernization Act Evaluation	4. Identity and Access Management	FCC developed a Standard Operating Procedure (SOP)/Policy to issue and track HSPD-12 PIV cards.	Provides a centralized view of security access events.
14	FY 2021 Privacy and Data Protection Program Inspection	5. Data and Privacy Protection	FCC OGC updated the privacy manual to include a template of privacy impact assessments (PIAs) used for proposed rules.	Ensures that Commission rules and orders inclusively and informatively account for the type of personally identifiable information collected and the number of people affected.
15	FY 2021 Payment Integrity Information Act Audit	14. Continue to enhance USACs applicant outreach program to educate applicants on the Schools & Libraries (S&L/E-Rate) program rules, especially rules relating to the competitive bidding processes.	FCC and USAC conducted several webinars and trainings and issued news briefs concerning E-Rate program rules and competitive bidding to educate program participants.	Helps to reduce the E-Rate Program IP and UP rate and ensure the integrity of the program.
16	FY 2021 Payment Integrity Information Act Audit	15. Enhance the use of automation tools in E-Rate Productivity Center (EPC) to check invoices for common errors and invoices that are flagged as high risk of non-compliance with program invoicing requirements.	EPC invoicing enhancements include improved upfront system validations to prevent calculation errors. EPC also enables E-Rate invoicing team to more readily pull invoices for corrective action prior to disbursing payments.	Helps to reduce the E-Rate Program IP and UP rate and ensure the integrity of the program.

Number	Project Name	Recommendation	Action Taken by the FCC	Impact of Closure
17	FY 2014 WCB Audit	4. Implement a plan that ensures the closure of pending appeals in a timely manner and prioritizes the resolution of appeals filed 2010 and earlier.	WCB has resolved all pending appeals from the original audit and has established a process to provide status updates on outstanding appeals to help ensure the closure of pending appeals is performed in a timely manner.	Reduces the risk that providers and USAC will not have clear guidance on the application of FCC rules.
18	FY 2021 DATA Act Audit	5. Develop and implement oversight policies and procedures to ensure component entities report financial assistance awards timely. [New Recommendation for FY 2021] Finding #3	FCC submitted the USAC March 2025 activity in FABS as evidence that oversight policies and procedures were implemented to ensure component entities report financial assistance awards in a timely manner.	Ensures compliance with all DATA Act and FAR requirements.

Visit our website, or follow us on LinkedIn, X, Facebook or Instagram

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