FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

FCC'S TOP MANAGEMENT AND PERFORMANCE CHALLENGES FOR FY2025

Table of Contents

Introduction

The Reports Consolidation Act of 2000 requires the Federal Communications Commission (FCC or Commission), Office of Inspector General (OIG), to issue a report annually summarizing our independent assessment of the most serious management and performance challenges facing the Commission. In turn, the FCC is required to include this report with its annual agency financial report.

We identified the five top management and performance challenges listed on the right.

1. Ensuring Performance Management and Accountability
2. Leading Governmentwide Broadband Coordination Efforts
3. Managing Fraud Risks and Protecting the Public from Scams and Identity Theft
4. Safeguarding National Security and Promoting Public Health and Safety
5. Modernizing Information Technology and Enhancing Cybersecurity

While the FCC has made significant progress in each of these areas, opportunities exist for further advancements. Our goal is that this report fully informs our stakeholders and serves as a constructive roadmap to the FCC on strategies for addressing its key challenges and carrying out the critically important mission highlighted in its strategic plan: "Ensuring that every person in every community, of every geography and income, has access to modern telecommunications service."

We begin our report below by describing OIG's methodology for identifying and gathering information regarding the FCC's top management and performance challenges. Next, we discuss new and emerging issues that may impact how the FCC addresses these complex challenges. Throughout the report we use hyperlinks for easy access to referenced reports and resources on trusted government websites, and also provide the full titles and report numbers in call-out boxes for future use in finding cited materials.

Lastly, for each of the five challenges, we describe:

1. The elements of the challenge,
2. The connection to the FCC's Strategic Plan,
3. Relevant OIG and U.S. Government Accountability Office (GAO) reports and ongoing work, and
4. The FCC's progress in addressing related recommendations.

We thank all who contributed to developing this report and look forward to continuing to work with the FCC, Congress, Universal Service Administrative Company (USAC), and all of our partners and stakeholders to strengthen and protect the FCC's programs and deliver meaningful and impactful oversight in service to the American public.

OIG's Methodology

OIG takes its statutory responsibility to issue an annual report of the FCC's top management challenges seriously. We solicited, collected, reviewed, and analyzed information and data from a variety of stakeholders to ensure an objective and representative perspective.

We began by reviewing last year's FCC OIG Top Management and Performance Challenges Report and related progress made by the FCC, including actions taken to resolve open recommendations. Adopting a streamlined approach , we categorized the challenges into overarching themes that integrate common issues faced by the FCC, many of which are governmentwide challenges.

We reviewed FCC's 2022-2026 Strategic Plan, FCC's FY 23 Annual Performance Report, and recent Congressional testimony to ensure that this report incorporates the priorities and progress identified by the FCC, and each challenge aligns with the FCC's strategic goals and objectives. We considered new oversight work, findings, and recommendations from the FCC OIG, GAO, the Council of Inspectors General on Integrity and Efficiency (CIGIE), and the Pandemic Response Accountability Committee (PRAC). We leveraged the work of the IG community by using observations from CIGIE's Top Management Challenges Report and PRAC's Top Management Challenges Report.

We conducted outreach to the FCC's Chair and Commissioners, Bureau and Office Chiefs, program officials, and oversight partners such as GAO, to fully leverage their knowledge, experiences, and expertise. We used this feedback to inform our decisions as we developed our final list of top management challenges. Further, we sought and incorporated stakeholder perspectives on progress made by the FCC in addressing challenges and the obstacles that the Commission continues to face.

New and Emerging Issues

Current events and circumstances necessarily impact how FCC leadership and Congressional stakeholders address the critical and complex issues before them. Below, we identify recent judicial cases that may impact how the FCC performs its mission. We also highlight potential opportunities for Congress to resolve certain issues through legislative reform.

Navigating the Current Judicial Landscape

The FCC enters FY 2025 facing several judicial decisions that present immediate operational, enforcement, and resource challenges. Some have governmentwide implications, and others uniquely impact the FCC, presenting existential questions about the FCC's mechanism for providing universal service to the American public. The FCC may need to direct its limited resources to these high priority matters, leaving it less able to address some of the other challenges identified in this report. Finally, some of these decisions may limit the FCC's ability to effectively enforce its program requirements and limit its ability to hold accountable those who defraud its programs by potentially eliminating anti-fraud tools currently used to deter and combat waste, fraud, and abuse.

The summaries below highlight these core cases:

Loper Bright Enterprises v. Raimondo, No. 22-4751, 2024 WL 3208360 (U.S. June 28, 2024)

In *Loper Bright*, the Court held the Administrative Procedure Act requires courts to exercise their independent judgment to decide whether an agency has acted within its statutory authority, and courts may not defer to an agency interpretation of the law simply because the statute is ambiguous or leaves a gap. In this decision, the Supreme Court reversed *Chevron, U.S.A. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837, 843 (1984) – a longstanding and often cited doctrine holding that if federal legislation is ambiguous or silent, courts must defer to the regulatory agency's interpretation if the interpretation is reasonable. While *Loper Bright* does not affect agency action based on clear statutory authority, including when Congress clearly confers discretionary authority to an agency, it would impact rulemaking related to legislation that lacks clear direction.

SEC v. Jarkesy, No. 22-859, 2024 WL 3187811 (U.S. June 27, 2024)

In *Jarkesy,* the Supreme Court held that when the Securities and Exchange Commission (SEC) seeks civil monetary penalties against a defendant for securities fraud, the Seventh Amendment entitles the defendant to a jury trial. While the FCC enforcement scheme differs from the SEC enforcement scheme, this decision introduces some uncertainty about the FCC's current enforcement practice as enforcement actions that seek civil penalties may potentially implicate the Seventh Amendment. Moreover, only the Department of Justice has the authority to initiate judicial enforcement actions for the Commission. Together, this poses potential obstacles to the FCC's statutory obligation to enforce the Communications Act and Commission rules.

Consumers' Research V. FCC, 109 F.4th 743 (5th Cir. 2024)

In *Consumers' Research v. FCC*, the U.S. Court of Appeals for the Fifth Circuit held that the current funding mechanism for the Universal Service Fund (USF) is unconstitutional. Specifically, the Fifth Circuit, in the context of reviewing the first quarter of 2022's contribution factor, ruled that USF contributions are a tax and that 1) Congress may have improperly delegated authority to tax to the FCC; and 2) the FCC may have impermissibly delegated taxing power to the Universal Service Administrative Company (USAC). The Fifth Circuit ruled the combination of Congress's broad delegation, and the FCC's further delegation, violates Article 1, Section 1 of the U.S. Constitution, the Legislative Vesting Clause. The decision also creates a circuit split as the Sixth and Eleventh Circuits previously rejected constitutional challenges to the USF. The FCC describes universal service as, "one of the core mandates," of the Communications Act, and this decision challenges the core of the Commission's mechanism — USF contributions — for accomplishing that mandate. The FCC filed a petition for certiorari on September 30, 2024. It is a challenge for the FCC to plan for all potential outcomes of this litigation.

U.S. ex rel. Todd Heath v. Wisconsin Bell, Inc., No. 22-1515 (7th Cir. 2024).

In this 2008 lawsuit under the Civil False Claims Act (FCA), a whistleblower alleged that Wisconsin Bell charged schools and libraries more than allowed under FCC's USF E-rate program, which is funded by contributions from telecommunications companies. Wisconsin Bell argued that the case should be dismissed because the False Claims Act does not apply to claims for E-Rate funds. The Seventh Circuit held that E-Rate funds are federal funds subject to the False Claims Act. The Seventh Circuit's decision created a circuit split, as in 2014, the Fifth Circuit held that the FCA does not apply to E-Rate claims. *United States ex rel. Shupe v. Cisco Systems Inc.*, 759 F.3d 379 (2014). On November 4, 2024, the Supreme Court will hear arguments in this matter. The question before the Court is whether reimbursement requests submitted to the E-rate program are claims under the FCA.

Congressional Opportunities to Help the FCC Address its Priorities and Challenges

Over the past several years, there have been multiple studies conducted, reports issued, and hearings held on USF Reform and additional issues facing the FCC's leadership. These have been directed, supported, and informed by the FCC; bipartisan Congressional stakeholders; state, tribal, non-profit organizations, and industry groups whose members are most impacted by the FCC's operations, subsidies, and services.

For its part, Congress may be best suited to address one or more of the above judicial decisions that impact the FCC and the public, by offering legislative clarifications, reforms, and mandates. As noted in other sections of this report, Congress may also want to consider legislation pertaining to the following areas: USF contributions reform; the FCC's auction authority; and the FCC Enforcement Bureau's statute of limitations and ability to independently pursue judicial enforcement actions. Further, Congress may consider more precise legislative authorities for the Commission and USAC to address the Court's ruling in *Loper Bright*.

Finally, to protect the FCC and federal funds at large from fraud, waste, and abuse, Congress can consider the passage of legislation previously recommended by the IG Community related to:

- Enhancing the Program Fraud Civil Remedies Act to better allow agencies to pursue administrative action for false statements and claims, and claw money back from fraudsters;
- Imposing a statutory exclusion from receiving discretionary federal funding for felony convicts who have defrauded federal programs, to avoid preventable repeat offenses; and
- Providing testimonial subpoena authority to OIGs, so that cases can be fully investigated.

Themes Identified in Listening Sessions:

In listening sessions, we heard about the following themes and issues impacting the FCC and stakeholders, which may warrant future attention and oversight:

- Workforce Planning: Succession Planning, Ability to Timely Process Upcoming Retirements, Retention in Certain Job Series, and Recruitment
- Emerging Threat and Opportunity: Artificial Intelligence
- Organizational Issues: Decision-making Processes, Effective Coordination, Communication, and Information Sharing
- Capacity Challenges: Budget and resources, especially around government-wide mandates
- Lapsed Authorities or Insufficient Funding: Auctions, ACP, SCRP
- Operational Challenge: Procurement
- Data: Access, Availability, Collection and Privacy

COMMON RESOURCES CITED THROUGHOUT

- FCC OIG's FY 24 Top Management and Performance Challenges Report, October 13, 2023
- FCC 2022-2026 Strategic Plan, March 29, 2022
- FCC FY 23 Annual Performance Report, March 11, 2024
- FCC Report: Future of the Universal Service Fund, August 15, 2022
- USAC's 2023 Annual Report, March 31, 2024
- CIGIE Top Management Challenges Report, September 2023
- PRAC Update Top Challenges in Pandemic Relief and Response , February 3, 2021
- PRAC Blueprint, Ch. 1: Best Practices for Strengthening Federal Programs, May 2024
- PRAC Blueprint, Ch. 2: Opportunities to Improve Program Integrity, August 2024

OPEN RECOMMENDATIONS

- GAO Open Recommendations for the Federal Communications Commission
- FCC OIG's Open Recommendations for the Federal Communications

1 Ensuring Performance Management and Accountability

Related FCC Strategic Goal 1: Pursue a "100 Percent" Broadband Policy, Objectives 1.1 and 1.4

Elements of the Challenge

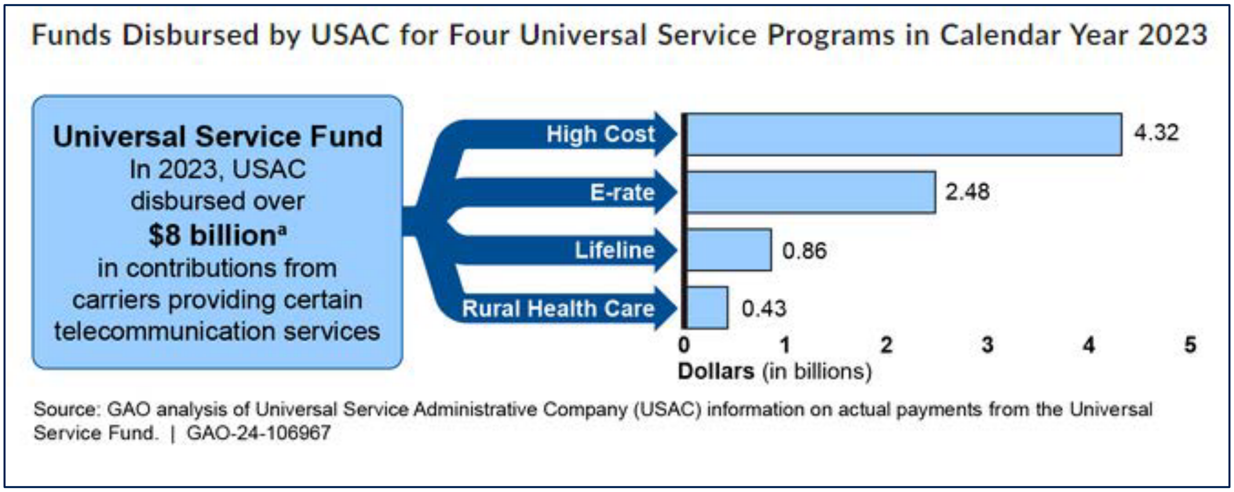
- Ensuring USF Subsidy Programs Meet Their Goals
- Effectively Administering Supplemental & Emergency Programs
- Preventing, Reducing, and Recovering Improper Payments

According to GAO, effective organizations set performance goals that clearly define intended program outcomes and establish performance measures that directly link with the performance goals. Ultimately, performance management is meant to instill accountability in federal programs and help ensure agencies are good stewards of federal tax dollars. A robust performance framework can also bring transparency to key questions about whether or to what extent agencies have used program funds in accordance with law and program rules. For example, it may help answer questions about whether programs have delivered goods or services to those eligible to receive them, and whether programs have minimized improper payments, including overpayments, duplicate payments, payments made by mistake, or fraudulent payments.

With the billions of dollars in federal and fee-based funding in universal service and other programs, it is critical that the FCC implement and maintain a robust performance management and accountability framework. As discussed below, the FCC has made progress in addressing FCC OIG and GAO recommendations focused on performance management and reducing improper payments, but there is more work to be done. We encourage the Commission to continue its focus on this challenge, which goes to the core of FCC's program mission.

Ensuring USF Subsidy Programs Meet their Goals

The Telecommunications Act of 1996 created the framework for USF, which in accordance with the FCC's strategic objective 1.2, is intended to facilitate affordable broadband deployment and meaningful access to essential services for all Americans. USF is administered by the Universal Service Administrative Company (USAC), a non-profit corporation, under the direction of the FCC.



USF consists of four programs:

1. High-Cost/Connect America Fund Program: Providing financial support to eligible telecommunications carriers serving rural, insular, and other high cost areas;
2. Schools and Libraries/E-Rate Program: Assisting schools and libraries to obtain telecommunications services, internet access, and internal connections;
3. Lifeline Program: Assisting low-income consumers to obtain affordable telephone and broadband internet service; and
4. Rural Health Care Program: Assisting rural health care providers to gain access to telecommunications and broadband services.

Telecommunications providers are required by law to make contributions to the USF by paying in a percentage of their end-user interstate and international revenues. Based upon this contributions system, USF disbursed over $8 billion in USF programs in 2023.

OIG's and GAO's previous audit work noted areas where the FCC's processes for developing and implementing performance goals related to administering and monitoring USF programs can be improved, including:

- In a GAO Audit of the National Verifier System, GAO recommended that the FCC develop and implement a plan to educate eligible consumers about the Lifeline Program and National Verifier, develop performance measures to track the Verifier's progress in reaching its goals, and ensure that the system's online application is accurate, clear, easy to understand, and includes an option to provide feedback. While the FCC addressed two recommendations and has committed to address them all, four recommendations related to consumer outreach/education, performance management, the manual review process, and website updates remain open and unresolved. The FCC and USAC must continue to monitor whether the National Verifier meets its intended goals to reduce the risk of enrollment of ineligible subscribers and improve the customer application and enrollment experience.
- Likewise, in GAO's Report Related to Performance Management in the High-Cost Program it noted that although the performance goals for the High-Cost program reflect principles in the Telecommunications Act of 1996, not all of the goals are expressed in a measurable or quantifiable manner and therefore do

not align with leading practices. The report also found that the FCC's measures for its performance goals do not always align with leading practices, which call for measures to have linkage with the goal they measure and clarity, objectivity, and measurable targets, among other key attributes. All four recommendations remain open, and as of May 2024, the FCC informed GAO that it was working on a plan to resolve them.

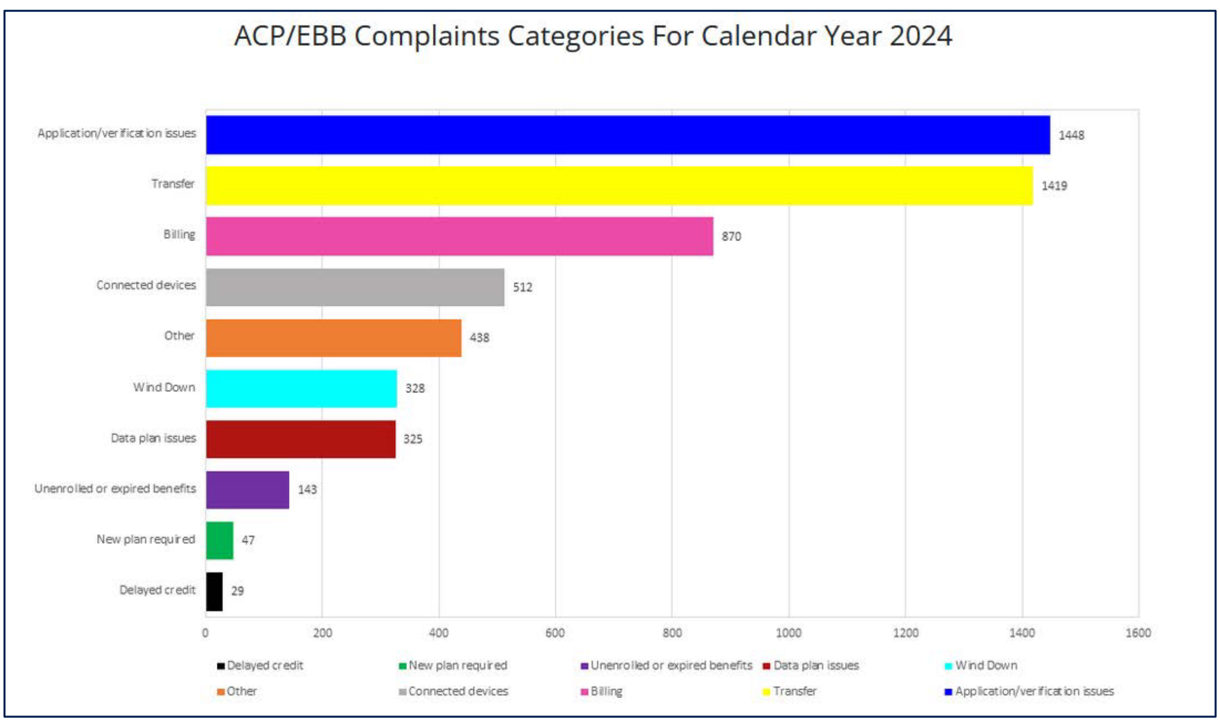
Performance goals and measures permit stakeholders to evaluate a program's success in achieving program objectives. For example, in a prior OIG Audit of the Consumer and Governmental Affairs Bureau Risk Management Strategy for Informal Consumer Complaints, OIG noted the FCC's performance goals for processing informal consumer complaints were not objective, relevant, or sufficiently rigorous. Specifically, performance measures were not reflective of the actual level of effort required for processing informal consumer complaints. The FCC took action to close all three recommendations. Ensuring all of the FCC's programs have performance goals and measures that align with leading practices, and are specific, clear, and measurable, is critical to effectively demonstrating program achievements to Congress and other stakeholders.

Effectively Administering Supplemental & Emergency Programs

Establishing clear, specific, and measurable performance goals is especially important for supplemental programs intended to serve vulnerable populations during emergency circumstances. These are often short-term, high-risk programs implemented and executed at an expedited pace.

Enhancing Transparency in FCC's Consumer Complaints Reporting for ACP

The Infrastructure Investment and Jobs Act ("Infrastructure Act"), 47 U.S.C. § 1752, required the FCC to periodically issue public reports containing consumer complaints involving participating provider compliance with ACP rules. OIG's Performance Audit of the ACP Program found the FCC did not publish any consumer complaint reports from January 2022, through December 2022. Subsequent to the audit scope period, the FCC made progress by developing and posting a complaint dashboard on its website, as depicted below:



There are opportunities to enhance the information on this dashboard to maximize transparency into the program and assist in identifying and addressing problematic trends. For example, between January 1, 2021, and July 8, 2024, the FCC received over 4,700 reported complaints that are listed as “other complaints,” and providing examples of concerns contained in that category would be useful. In addition, connecting the complaints received to specific providers would provide important information to consumers regarding customer satisfaction upon which they could base decisions on subscribership. Increased transparency, even if not mandated by law, would allow all stakeholders, to include the Commission and Congress, to timely address challenges identified by the public and better evaluate whether the program is operating as intended.

Ensuring Effective Performance Measures in ACP to Allow for Meaningful Program Evaluation

Two related audits of the $14.2 billion ACP looked at the FCC’s performance management and fraud risk management of this program. OIG’s Report and GAO’s Report both included findings and recommendations to improve the FCC’s ability to evaluate the ACP’s progress against its performance goals and measures for the program.

The FCC made progress in addressing the two related OIG recommendations by adding objective, measurable, and quantifiable goals for the ACP to its Performance Plan in its Budget Estimates to Congress for FY 2025 and performing an evaluation of the ACP and including the results and additional updates in its FY 2023 Annual Performance Report. In addition, the FCC resolved the GAO-related recommendation by revising its performance measures for the ACP to include specific, numeric targets and timeframes, making their performance metrics more objective, clear, and measurable. GAO determined that based on the FCC’s corrective actions, it will be better able to assess and effectively demonstrate the ACP's achievements to Congress and other stakeholders.

Maximizing Outreach to Increase Program Participations by Eligible Participants

The FCC should also apply lessons learned from supplemental and emergency programs to improve programs in the agency’s portfolio. For example, last year, we identified Lifeline’s low participation rates as a challenge and noted that the FCC and USAC must develop and implement a plan to address the low participation rate for the Lifeline Program. FCC OIG’s ACP audit revealed shortcomings in the implementation of the ACP outreach grant program, highlighting the need for a more proactive and targeted approach to reach the full scope of intended households and fully assess the program's impact. The FCC informed OIG the Commission developed comprehensive outreach, targeting, and paid media plans outlining the FCC’s strategy for: (1) engaging government and community-based partners for ACP outreach; (2) a targeted nationwide paid and earned media strategy; (3) prioritized language access for ACP program materials; and (4) layered FCC-led engagement activities to promote community trust in ACP.

GAO’s ACP report also identified gaps in the outreach efforts of both the FCC and USAC. A key factor contributing to this issue was the absence of a comprehensive consumer education plan. The FCC made progress in this area, resolving two recommendations from GAO’s Report related to developing ACP non-English outreach materials and a consumer outreach plan that aligns with leading practices. Specifically, the FCC took steps to improve its language translation process and create a Consumer Outreach Plan for ACP. According to GAO, the FCC’s new plan set goals for ACP outreach based on household enrollment targets, specifically for the overall eligible population and for first-time internet users. GAO found that the plan included metrics for measuring success geared toward program awareness and enrollment, as well as specific metrics for certain portions of the plan (such as paid media and outreach grants). GAO concluded that with the new outreach plan, the FCC would be better positioned to make decisions about which mix of outreach tools will be most effective in helping to meet its goals of raising awareness of and participation in ACP. GAO has closed all of the recommendations from this report.

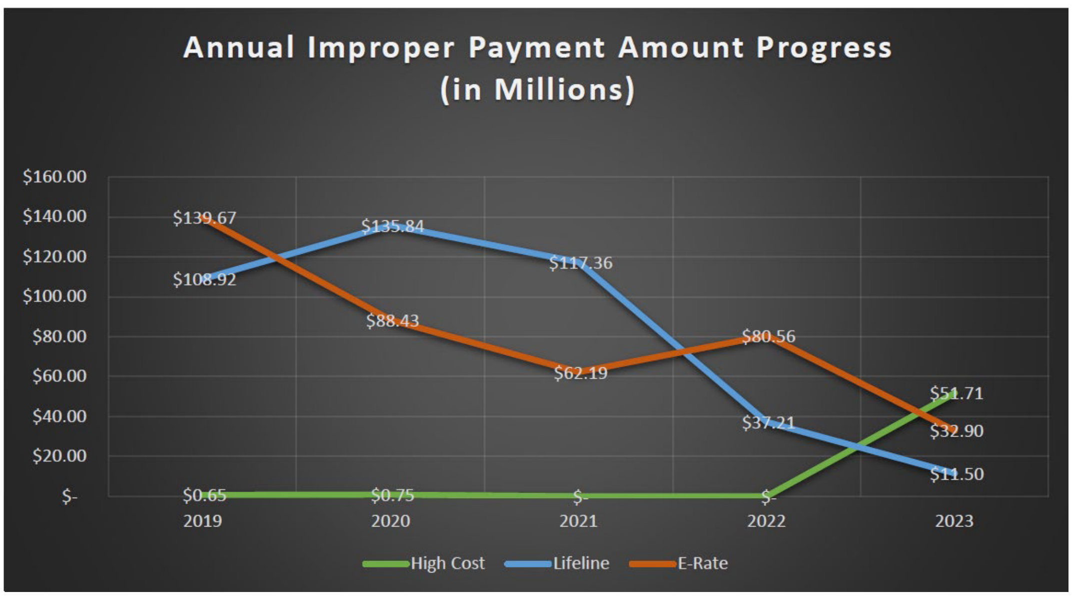
Even though the ACP is no longer in effect, by incorporating lessons learned from the previous outreach efforts, including the importance of early, targeted, and data-driven outreach, the FCC can enhance the effectiveness of existing and future programs and ensure they reach their intended beneficiaries.

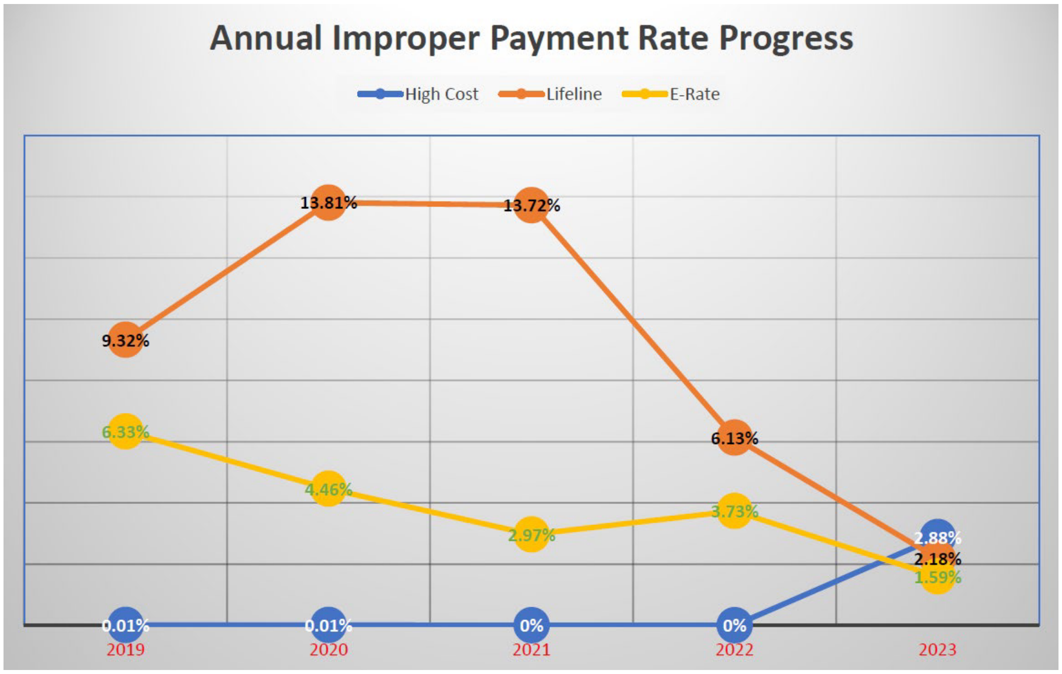
Preventing, Reducing, and Recovering Improper Payments

The Payment Integrity Information Act (PIIA) of 2019 directs federal agencies and departments to undertake activities designed to identify, report, reduce, and recover improper payments (IPs) in the government's programs and activities. The 2023 PIIA Audit Report noted three USF programs (Lifeline, Schools and Libraries, and High-Cost) with IP amounts and rates above the statutory threshold.

Although the FCC made strides in reducing improper payments, as depicted below, it needs to continue making improvements to reduce improper payments below the statutory threshold, and in establishing and meeting the annual tolerable rates for each program.

The charts below provide the Commission's progress on improper payment amounts and rates over the past five years based on data reported on www.paymentaccuracy.gov.





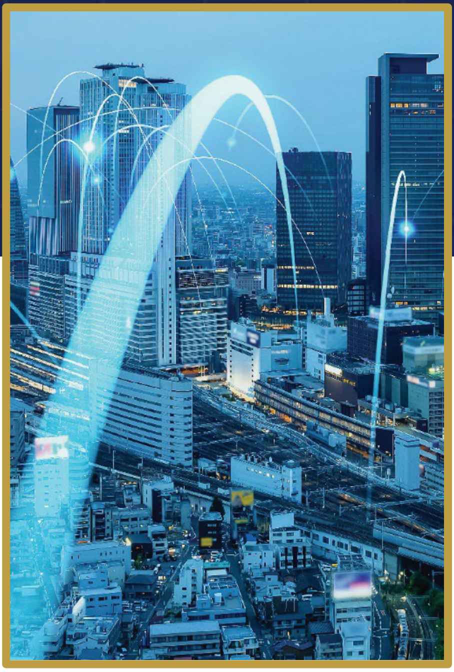
As of September 2024, five recommendations remain open from 2019, 2021, and 2023 OIG PIIA audit reports. We encourage the FCC to continue to work towards addressing these recommendations and strengthening program integrity in each of these programs.

OIG AND GAO HIGHLIGHTED REPORTS

- FCC OIG Report 23-AUD-01-04: Performance Audit of the Affordable Connectivity Program
- FCC OIG Report 24-AUD-01-01: Audit of FCC's FY 2023 Compliance with Payment Integrity Information Act of 2019 Requirements
- FCC OIG Report 18-AUD-12-08: Audit of the Consumer and Governmental Affairs Bureau Risk Management Strategy for Informal Consumer Complaints FY 2017 and FY 2018
- GAO Report 21-24: FCC Should Enhance Performance Goals and Measures for Its Program to Support Broadband Service in High-Cost Areas
- GAO Report 23-105399: FCC Could Improve Performance Goals and Measures, Consumer Outreach, and Fraud Risk Management
- GAO Report 21-235: FCC Has Implemented the Lifeline National Verifier but Should Improve Consumer Awareness and Experience

2 Leading Governmentwide Broadband Coordination Efforts

Related FCC Strategic Goal 1: Pursue a "100 Percent" Policy
Related FCC Strategic Goal 6: Foster Operational Excellence



Elements of the Challenge

- Maintaining and Enhancing Broadband Maps for Governmentwide Data-Informed Funding Decisions and Oversight
- Effectively Leading and Coordinating Efforts to Manage Spectrum

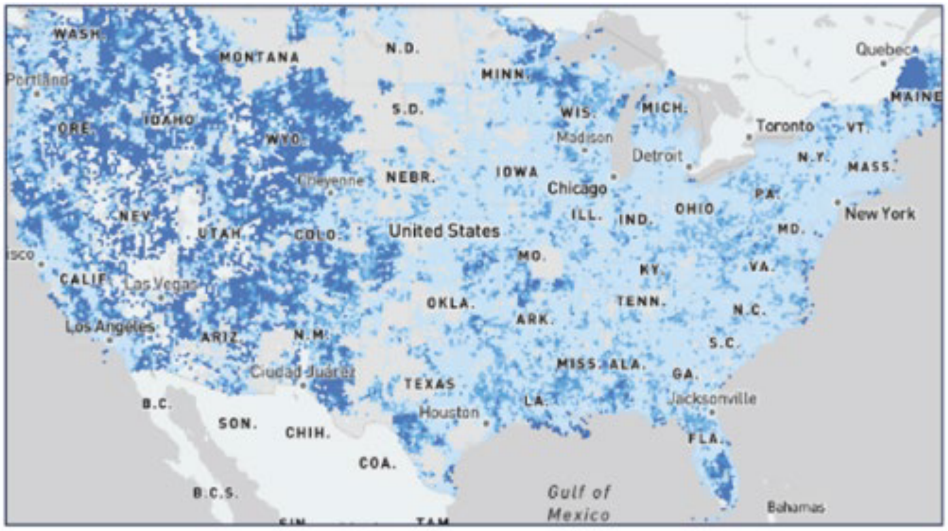
Expanding broadband coverage to 100% of the United States is a national priority to which the federal government has invested billions of dollars in taxpayer funds. Everyone in the United States needs to be connected to broadband service for their everyday needs, work, education, healthcare, and for emergency circumstances – pandemics, terrorist attacks, natural disasters – all of which have unfortunately impacted us over the past decade. In a recent report**,** GAO identified more than 133 broadband funding programs administered by 15 agencies and concluded that federal broadband efforts are fragmented and overlapping. GAO determined that without a national strategy with clear roles, goals, objectives, and performance measures, federal broadband efforts continue to risk overlap and duplication of efforts, and that lack of coordination leads to agency disputes and inability to reach agreements.

The FCC has direct statutory authority for broadband mapping, and to regulate the non-Federal use of spectrum, respectively. The FCC has been tasked with leading complex broadband projects including mapping multiple streams of broadband data and funding data, and ensuring the most effective use of spectrum to meet the telecommunications needs of our country. These important projects often require the Commission to coordinate among multiple stakeholders. Coordinating and leading various groups of stakeholders is a challenge for the FCC as many of the stakeholders have separate leadership teams, missions, and objectives.

Maintaining and Enhancing Broadband Maps for Governmentwide Data-Informed Funding Decisions and Oversight

In March 2020, the Broadband Deployment Accuracy and Technological Availability Act (Broadband DATA Act) was enacted. The Broadband DATA Act required the Commission to, among other things, collect location-specific information about broadband services available in the U.S., share that information via a public-facing map, and implement a public challenges process. Further, in 2021, the Infrastructure Act allocated $42.45 billion for the Broadband Equity, Access, and Deployment (BEAD) program, funding broadband service deployment to underserved locations.

The FCC's National Broadband Map (NBM) was initially launched in November 2022 and provides information about the internet services available to individual locations across the country, along with new maps of mobile coverage, as reported by Internet Service Providers (ISPs) in the FCC's ongoing Broadband Data Collection (BDC). The NBM is used by various government agencies to identify areas that need broadband deployment.



For example, the Infrastructure Act directs NTIA to determine which areas are underserved using the data the Commission collects and compiles into the National Broadband Map pursuant to the Broadband DATA Act.

OIG is currently conducting a performance audit of the FCC's administration of the High-Cost Universal Broadband (HUBB) Portal Data. The FCC and USAC use the data submitted in the HUBB to ensure that participating carriers of the Connect America Fund (CAF) programs are meeting broadband deployment obligations in accordance with FCC rules. HUBB reporting is not currently based on the Broadband Serviceable Location Fabric (Fabric), a dataset of all locations in the United States and its Territories where fixed broadband internet access service is or could be installed. However, the FCC expects carriers to compare the broadband deployment data they certify in the HUBB with the Fabric or availability data in the BDC and to take steps to ensure data alignment.

Beyond the NBM, the Infrastructure Act tasked the FCC with creating a map to be the centralized, authoritative source of information on funding made by the federal government for broadband infrastructure deployment, now located here: FCC Broadband Funding Map. This map provides an important overview of broadband infrastructure deployment projects funded by the federal government throughout the United States. Each federal agency compiles funding project data for its own programs and reports the data for inclusion on the map. The Broadband Funding Map also includes NBM data on the availability of broadband services across the United States.

Federal agencies and Congress rely on the FCC's broadband data and funding maps to identify the unserved and underserved communities most in need of funding for high-speed internet infrastructure investments. Given this responsibility, the FCC is challenged to ensure their accuracy.

Effectively Leading and Coordinating Efforts to Manage Spectrum

GAO has issued several reports related to the significant challenges faced by both the FCC and NTIA for managing spectrum—a finite natural resource which enables wireless communication services critical to the U.S. economy and government. Nearly all usable spectrum has been allocated either by NTIA for federal use, or by the FCC for commercial and nonfederal use.

Because demand for spectrum is increasing to support 5G and new technologies that require more spectrum, there is pressure to identify opportunities to repurpose spectrum. Both agencies face the significant challenge of being able to efficiently and effectively manage spectrum for our nation.

For the past three decades, FCC employed spectrum auctions as a tool to meet national spectrum goals and support beneficial new technologies, while at the same time bringing significant revenue into the government. However, the FCC's authority to conduct new auctions and grant a license or permit expired in March 2023.

In a July 2024 Report, GAO recognized that in 2023, as part of the FCC's broader efforts to improve spectrum efficiency, the FCC established principles for spectrum management, which set expectations for users of nonfederal receivers. Specifically, the FCC's principles established policy and technical considerations for receivers, which include that users should design receivers to reduced unwanted signals from nearby services. However, the report found that in implementing the principles, the FCC has not applied key practices that GAO determined could help better manage the results of improving receiver performance, including identifying goals, strategies, and barriers. GAO made the following three recommendations to the FCC to address its findings: (1) define measurable goals related to implementing the spectrum management principles outlined in the FCC's April 2023 policy statement; (2) identify strategies and resources necessary to achieve these goals; and (3) identify internal and external factors that could affect the FCC achieving its goals, to inform its efforts.

As the FCC continues to address these recommendations towards developing defined measurable goals for implementing spectrum management principles, its role in achieving spectrum efficiency remains a top challenge.

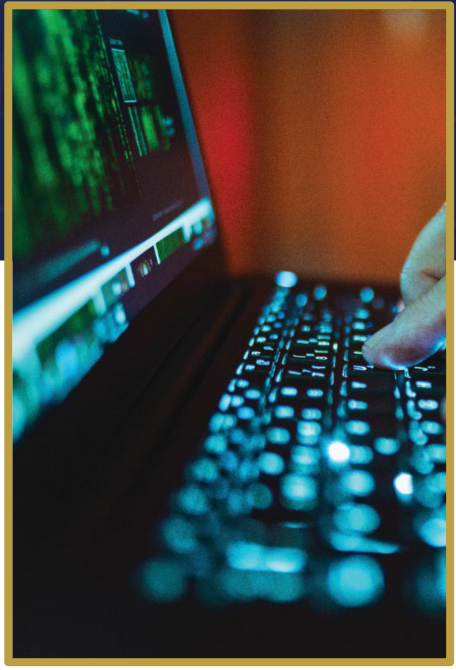
OIG AND GAO HIGHLIGHTED REPORTS

- GAO Report 23-106818: A National Strategy Needed to Coordinate Fragmented, Overlapping Federal Programs
- GAO Report 24-106325: Spectrum Management, Key Practices Could Help Address Challenges to Improving Receiver Performance

3

Managing Fraud Risks and Protecting the Public from Scams and Identity Theft

Related FCC Strategic Goal 3: Empower Consumers
Related FCC Strategic Goal 6: Foster Operational Excellence



Elements of the Challenge

- Preventing and Addressing Fraud in USF and Supplemental Programs
- Prioritizing Fraud Risk Management
- Developing a Strong Suspension and Debarment Program
- Opportunity to Protect FCC Funds Through Mandatory Disclosure Requirements

In a recent report, GAO estimated that the federal government lost between $233 billion and $521 billion annually to fraud between 2018 and 2022, a range representing three to seven percent of average federal obligations. Beyond eroding public trust in government, fraud significantly diminishes each agency's ability to deliver critical programs to the communities they are intended to serve, and results in other serious consequences for our most vulnerable populations, such as children, the elderly, and low income and underserved communities.

Based upon the FCC OIG's investigations, advisories, audits, and proactive reviews, as well as the oversight work of GAO and the IG Community, we have identified fraud risk management and protecting FCC programs and consumers as a top challenge for the FCC. Over the years, our investigative team and data scientists have uncovered and shared gaps and loopholes in the FCC's programs that have allowed fraudsters not only to engage in egregious schemes to divert FCC program funds for personal gain, but also to prey on our most vulnerable populations through identity theft and other scams.

The Commission recognizes the need to prioritize fraud prevention, enforcement, and protecting consumers, as set forth in strategic objectives 3.1 and 6.3 of its strategic plan. In addition, the FCC has been responsive to our related recommendations and has closed many of the gaps we identified. However, there is more work to be done and protecting FCC programs and consumers from fraud continues to be a top management challenge.

Preventing and Addressing Fraud in USF and Supplemental Programs

Our mission is to protect FCC programs from fraud, waste, and abuse. The IG Act provides that we do so through investigations and other reviews to identify, prevent, and deter fraud, as well as through education and outreach to all of our stakeholders.

In our previous statement summarizing FCC's most serious Management and Performance Challenges, we focused on known fraud risks and gaps in FCC subsidy programs. When we find those risks, we share them with the FCC and the public through our Advisories and Outreach, Press Releases, and Semiannual Reports.

Most recently, we shared a press release announcing the $6.5 million dollar settlement to resolve allegations that a High-Cost Subsidy Provider made improper subsidy claims to FCC's High Cost Program. This was initially brought to the government's attention by a whistleblower, the company's former Controller, who filed a lawsuit under the *qui tam* provisions of the False Claims Act, which allows whistleblowers to receive a portion of funds recovered, in this case, over $1.2 million.

We also identified the following fraud schemes and risks associated with several aspects of the FCC's low-income broadband subsidy programs, Lifeline, the COVID-Era Emergency Broadband Benefit (EBB) Program, and the ACP, including:

- CEP School Lunch Enrollment Fraud and Abuse
- Unauthorized and Abusive Transfers
- National Verifier Manual Review Process
- Non-compliant Provider Usage
- Monitoring and De-Enrollment Practices

In response, the Commission and USAC have dedicated significant resources to protecting the integrity of these programs and have taken steps to address non-compliance and ensure effective controls are in place. Although the EBB program expired and the ACP is currently out of funding, these issues continue to exist for the Lifeline program and continue to arise in our ongoing investigations of fraud in these programs, which we will continue to pursue as authorized by applicable statutes of limitations. Moreover, the lessons learned should be applied to all future funding programs, where applicable.

We have also shared the following ideas with the FCC for its consideration:

<u>With respect to the E-Rate Program</u>: Following up on suggestions by an internal USAC risk assessment and a GAO review, OIG recommended a process by which USAC would collect and release competitive bidding documents and standardize bid responses from service providers to assist applicants in reviewing and selecting the most effective bid. The Commission sought comments on this recommendation in 2022 through a notice of proposed rulemaking but has not taken action on this issue. Resolving this issue in a manner that best protects program integrity is a management challenge.

<u>With respect to the Lifeline/EBB/ACP and Controls in FCC's National Verifier</u>: OIG has identified several challenges related to oversight of USF, COVID era, and Infrastructure Act low-income broadband subsidy programs. While the EBB program and the ACP are now expired or out of funds, these lessons are important to address in Lifeline and any potential future renditions of these programs.

Manual Review Process

A significant number of the ACP subscriber applications require manual review to confirm subscriber eligibility. Many Lifeline Subscriber applications also undergo manual review to confirm eligibility. Multiple OIG audits have identified instances where manual review improperly qualified ineligible households to receive program benefits. USAC continues to make significant improvements to the manual review process, by adding the recommended layers and volume of quality control reviews, and by training reviewers. Our work indicates more improvements are needed. For example, late last year, we made additional recommendations to make the application process less vulnerable. The Commission and USAC should remain vigilant against provider and sales agents' attempts to defraud the program by exploiting manual review process vulnerabilities.

Agent Registration

OIG investigations and analyses have consistently shown that enrollment fraud is frequently perpetrated by provider enrollment representatives or agents. USAC implemented the Representative Accountability Database (RAD) to identify and block enrollment representatives who engage in fraudulent or abusive enrollment activity. In order for USAC's system to work, providers must register their enrollments in RAD and accurately report when agents are involved in enrollment transactions. However, OIG analyses since 2021 reveal many Lifeline and ACP providers that employ enrollment representatives fail to register all their enrollment representatives or report their enrollment activity. Since then, we shared with USAC and the Commission, warning letters our office sent to several large ACP providers describing OIG's concern that those providers failed to register their enrollment representatives in RAD even though those providers regularly used enrollment representatives to enroll subscribers.

To address this challenge, FCC and USAC must vigorously enforce requirements that providers furnish enrollment agent identification information for all National Lifeline Accountability Database (NLAD) and National Verifier transactions.

Challenges in Enforcement due to the FCC Enforcement Bureau's One-Year Statute of Limitations for Issuing Notices of Apparent Liability for Forfeitures

The FCC faces a significant challenge in enforcing compliance with USF obligations due to the constraints imposed by the one-year statute of limitations for issuing Notices of Apparent Liability for Forfeiture (NAL). Specifically, Section 503(b)(6) of the Communications Act of 1934, as amended, prohibits the Commission from imposing a forfeiture if the violation charged occurred more than one-year prior to the date of issuance of the required notice or notice of apparent liability. 47 U.S.C. § 503(b)(6). This limitation requires the FCC to quickly discover, investigate, and act on violations, which can result in some cases going unpunished and weaken the program's integrity.

A recent OIG Audit of USAC's Oversight of the USF Contributions Process concluded there were internal control weaknesses in USAC's process for referring service providers to the FCC's Enforcement Bureau (EB) for potential enforcement action. Specifically, during calendar year 2022, USAC did not refer any eligible service providers to the EB, despite instances where eligible service providers did not make their universal service contributions obligation as required by the Telecommunications Act of 1996. The audit identified known uncollected amounts owed to the USF totaling $28,632,140. Since USAC did not make timely referrals to the EB, it created a risk that the Commission would be unable to take necessary enforcement action against noncompliant service providers. The report contained one finding and three recommendations to strengthen internal controls over USF contributions. The recommendations remain open as the FCC seeks to resolve them.

Similarly, OIG's Performance Audit on the Affordable Connectivity Program further highlighted the challenges posed by the one-year statute of limitations. The audit found that four providers were unable to substantiate reimbursement claims or did not respond to audit requests. One of the providers was removed from participation in ACP under another proceeding for its serious and willful misconduct, and USAC conducted separate program integrity reviews of the other three providers as a result of the audit. While the Commission is seeking recovery based on the results of the program integrity reviews, enforcement actions against the remaining providers were not feasible due to the one-year statute of limitations. However, EB has issued NALs and Removal Orders against additional ACP providers that engaged in serious, willful misconduct.

Opportunity to Protect FCC Funds Through Mandatory Disclosure Requirements

In April 2024, the Office of Management and Budget updated its Uniform Guidance for Federal Financial Assistance, incorporating anti-fraud provisions highly recommended by the IG Community, to include a mandatory disclosure provision (2 C.F.R. 200.113). This provides that:

> "An applicant, recipient, or subrecipient of a Federal award must promptly disclose whenever, in connection with the Federal award (including any activities or subawards thereunder), it has credible evidence of the commission of a violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 of the United States Code or a violation of the civil False Claims Act (31 U.S.C. 3729–3733). The disclosure must be made in writing to the Federal agency, the agency's Office of Inspector General, and pass-through entity (if applicable)."

The above language helps promote good stewardship of federal funds and mirrors the longstanding disclosure requirements for contractors under the Federal Acquisition Regulation (FAR) 52.203-13, which has had demonstrated success in protecting federal procurement funds from fraud, waste, and abuse. The FCC and USAC could enhance stewardship of FCC funding and increase deterrence by incorporating this provision in all FCC subsidy programs.

Prioritizing Fraud Risk Management

With unprecedented levels of fraud against pandemic-relief programs, it is now clearer than ever before that fraud risk management — developing and implementing a risk-based strategy to protect federal programs — must be a top priority. The FCC has taken steps to adopt leading practices identified by GAO's Fraud Risk Framework. The FCC has also prioritized protecting consumers from robocalls and texts, as demonstrated by its active partnership with Attorneys General across the country and the significant enforcement efforts it has taken to pursue related matters.

GAO and OIG have issued reports related to fraud risk management in FCC's High-Cost, EBB, and ACP programs, with recommendations adhering to GAO's Fraud Risk Framework. While FCC has made significant progress to address related recommendations, we encourage the FCC to continue to advance its fraud risk management strategy and program. In addition, we believe that the FCC should consider incorporating risks associated with artificial intelligence and other emerging technologies that are being used to carry out more sophisticated fraud schemes.

FCC's Progress in Managing Fraud Risks

- In response to a GAO Report recommending that the FCC enhance fraud risk management in the High-Cost Program, the FCC took action to resolve three recommendations to adopt leading practices from GAO's Fraud Risk Framework, to include creating a dedicated Fraud Risk Group to focus on fraud risk prevention and detection; planning regular fraud risk assessments for the High Cost program; and developing a related fraud risk management strategy.
- In GAO's ACP Report, GAO found that the FCC had not implemented fraud risk management with respect to its ACP program, or its predecessor, the Emergency Broadband Benefits Program. GAO made six recommendations that the FCC adopt leading practices from its Fraud Risk Framework related to processes, strategies, and assessments.

  The FCC resolved all six recommendations, to include developing and implementing policies and procedures that establish responsibilities for fraud risk assessments across FCC and establishing an antifraud strategy that aligns with GAO's Fraud Risk Framework.

Developing a Strong Suspension and Debarment Program

In previous semiannual reports, FCC OIG highlighted the importance of the FCC establishing a robust suspension and debarment program to protect the FCC and other federal agencies from doing business with individuals or entities who have demonstrated they are not good stewards of federal funds.

Currently, the FCC may debar an individual or entity only after a criminal conviction or civil judgment for misconduct related to USF programs. However, conduct that falls short of this high bar may nonetheless pose a significant threat to program integrity. The FCC's limited criteria restrict efforts to protect the USF, the FCC's emergency and supplemental programs, and the entire federal government from individuals and entities who lack present responsibility.

In 2005, OMB issued Guidelines to Agencies on Governmentwide Debarment and Suspension (Non-Procurement), 2 C.F.R. Part 180, which provide model suspension and debarment non-procurement regulations. OMB's guidelines significantly differ from the FCC's current suspension and debarment program, and provide a broader and more comprehensive approach to protecting federal funds, with a centralized government-wide suspension and debarment program coordinated by the Interagency Suspension and Debarment Committee.

In 2020, the Commission issued a "Modernizing Suspension and Debarment Rules" Notice, which proposed to adopt rules consistent with the OMB Guidelines, and to supplement the Guidelines through FCC-specific regulations, including rules addressing those matters for which the Guidelines give each agency discretion. The notice recognized that other federal agencies have adopted most of the OMB Guidelines with limited changes and proposed to do the same. Comments were received in March 2020, but no final action has yet been taken by the Commission.

Government-wide suspension and debarment are critical administrative remedies that protect federal funds from fraud, waste, abuse, and mismanagement. We strongly urge the Commission to promptly adopt stronger and more comprehensive suspension and debarment regulations that align with the model practices set forth by 2 C.F.R. Part 180. This would provide the FCC and its Enforcement Bureau, as well as the FCC OIG, with another effective tool to protect FCC and all federal programs from individuals and entities who are not responsible stewards of federal funds.

OIG AND GAO HIGHLIGHTED REPORTS

- FCC OIG Report 23-AUD-05-01: Audit of USAC's Oversight of the Universal Service Fund Contributions Process
- FCC OIG Report 23-AUD-01-04: Performance Audit of the Affordable Connectivity Program
- GAO Report 20-27: FCC Should Take Additional Action to Manage Fraud Risks in its Program to Support Broadband Service in High-Cost Areas
- GAO Report 23-105399: FCC Could Improve Performance Goals and Measures, Consumer Outreach, and Fraud Risk Management (Related to ACP)

4 Safeguarding National Security and Promoting Public Health and Safety

Related FCC Strategic Goal 4: Enhance Public Safety and National Security

Elements of the Challenge

- Effectively Administering the Supply Chain Reimbursement Program to Protect National Security
- Participating in Governmentwide Efforts to Respond to Natural Disasters
- Implementing Critical Telecommunications Programs to Promote Public Health

FCC has a leading role in pursuing policies and enforcement to ensure the availability of secure, reliable, critical communications infrastructure and services—to guard against external threats, support day-to-day activities, and prepare for emergency situations, including natural disasters, terrorist attacks, and public health crises.

Among its leadership efforts to promote public health, safety, and national security, the FCC has supported and enhanced the nation's 911 and Next Generation 911 system; improved Wireless Emergency Alerts for the public and first responders; promoted telecommunications policies to protect survivors of domestic abuse; and ensured public access to the 988 Suicide and Crisis Lifeline, even in times of outages.

As reflected in its most recent FY 23 performance report, while the FCC has made significant strides in these critical areas, given the serious nature of these high-risk, high-impact responsibilities, we have identified this as a top management challenge.

Effectively Administering the Supply Chain Reimbursement Program to Protect National Security

Protecting the United States against national security threats to the communications networks and supply chains is a critical part of the FCC's purpose. To this end, at the direction of Congress, the FCC established the Supply Chain Reimbursement Program (SCRP) to reimburse providers of advanced communications services with ten million or fewer customers for reasonable expenses incurred in the removal, replacement, and disposal of covered communications equipment and services from their networks deemed to pose security threats to the United States.

To qualify for reimbursements, the covered equipment and services must have been produced or provided by Huawei Technologies Company or ZTE Corporation on or before June 30, 2020. The SCRP was appropriated $1.9 billion, but demand was far greater. The program received applications for approximately $5.6 billion, of which the FCC determined approximately $4.6 billion was reasonable and supported. Managing this funding shortfall and ensuring program requirements are implemented efficiently and effectively are key challenges facing the FCC.

The FCC must ensure the SCRP requirements are implemented efficiently and effectively. The FCC is tasked with: (1) determining whether the costs claimed are in line with what is typically incurred when transitioning from covered communications equipment or services to a replacement, comparing the cost relative to alternative equipment and services; and (2) comparing the capabilities and functions performed by the replacement equipment and services to determine whether they are comparable to the equipment and services removed. Additionally, the statute requires the FCC to conduct audits and field reviews of the program participants for compliance with the program requirements, and the FCC has established a plan to conduct field reviews both during the course of the participants' efforts to remove, replace, and dispose of covered communications equipment and services and after all of this work has been completed. The FCC has completed one field review as of August 2024. The combination of all programmatic and tactical issues facing the program poses significant challenges for the FCC.

Participating in Governmentwide Efforts to Respond to Natural Disasters

Ensuring the federal government can respond to natural disasters effectively and immediately is a serious challenge. Effective emergency response requires agencies to provide clear guidance and to coordinate efforts across myriad programs, often raising questions about jurisdictional boundaries, legal authorities, and funding availability. In a 2021 report (GAO-21-297), GAO found that in the aftermath of Hurricane Maria's network restoration, the FCC took several actions to support telecommunications restoration, including gathering network outage information and creating a task force to support communications restoration in Puerto Rico and the U.S. Virgin Islands. Further, in August 2018, the FCC issued a lessons-learned report pertaining to its disaster response and recovery efforts that included observations from the work done in response to four hurricanes, including Hurricane Maria. However, GAO noted federal guidance from the Department of Homeland Security (DHS) on the FCC's role in disaster response was not clear and found the FCC had not provided a complete and accurate account of its disaster response and the activities of its task force, which could help with preparation for future disasters, and recommended that:

(1) The DHS, in consultation with the FCC, update Emergency Support Function #2 of the National Response Framework to list specific roles and responsibilities for the FCC. The FCC worked with DHS to resolve this recommendation; and,

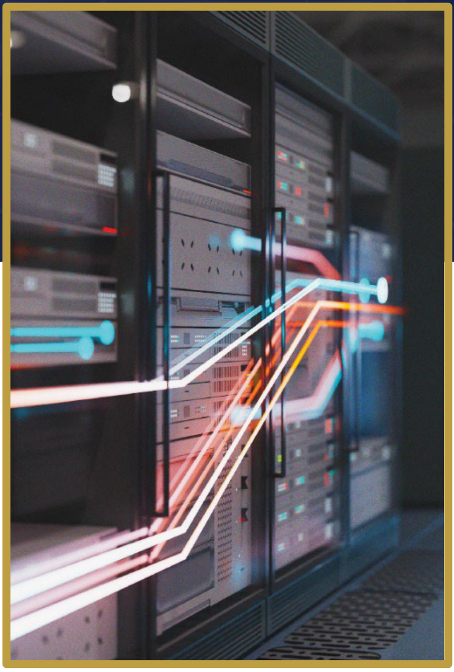
(2) The FCC enhance the transparency and accountability of FCC's operations by publicly reporting on the actions and findings of its Hurricane Recovery Task Force and determine if any changes in policy are needed to ensure FCC has transparent operations for any future disaster-related task forces. As of August 2024, FCC officials reported that it was working on implementing this recommendation.

Implementing Critical Telecommunications Programs to Promote Public Health

The FCC's COVID-19 Telehealth program was established to help healthcare providers deliver telehealth services to patients at their homes or mobile locations in response to the COVID-19 pandemic. Since COVID-19 Telehealth funds were issued to respond to the COVID-19 pandemic quickly, there was an increased risk of improper use and disbursement of the $449.95 million appropriated to the program, which sunset in April 2023, coinciding with the end of the COVID-19 pandemic. FCC OIG is conducting an inspection to determine whether the FCC effectively managed and administered the COVID-19 Telehealth Program to ensure that telehealth funding was disbursed and used in accordance with the enabling statute.

5 Modernizing Information Technology and Enhancing Cybersecurity

Related FCC Strategic Goal 6: Foster Operational Excellence
Strategic Objectives 6.2 and 6.3



Elements of the Challenge

- Managing Government-wide Information Security Risks
- IT Modernization/Upgrading Legacy Systems
- Privacy and Data Protection

The modernization of information technology and the need to enhance cybersecurity are significant common challenges across the government. As set forth in the Council of Inspectors General on Integrity and Efficiency's Top Management and Performance Challenges Facing Multiple Federal Agencies, other major federal government-wide hindrances to IT modernization efforts that could also hamper the FCC include IT funding shortages, shifting priorities, and poor IT investment and project management. As discussed below, while the FCC continues to make progress in these areas, it should continue to work towards addressing OIG recommendations to meet this challenge.

Managing Government-wide Information Security Risks

Annually federal agencies undergo an independent OIG assessment of their information security programs, using the Federal Information Security Management Act (FISMA) reporting metrics issued by Office of Management and Budget (OMB) and the Department of Homeland Security (DHS), and Cybersecurity and Infrastructure Agency (CISA). The metrics are used to determine whether the agency's federal information security programs are in compliance with FISMA legislation and other applicable guidance. The Office of Management and Budget (OMB) provided an annual government-wide assessment of cybersecurity in its FISMA Annual Report for FY 2023, which showed an increase in cybersecurity events reported by federal agencies. The report cited improved detection capabilities at the security operations centers, additional automation and training, and changes in event and incident tracking methodologies as a reason for the increased reporting of cybersecurity events. The detection capabilities described in the report are related to the FISMA identity and access management (I&AM) domain. I&AM is at the heart of cybersecurity, including critical practices for authentication, user and privilege user access management and credentialing–which has been an ongoing challenge for FCC.

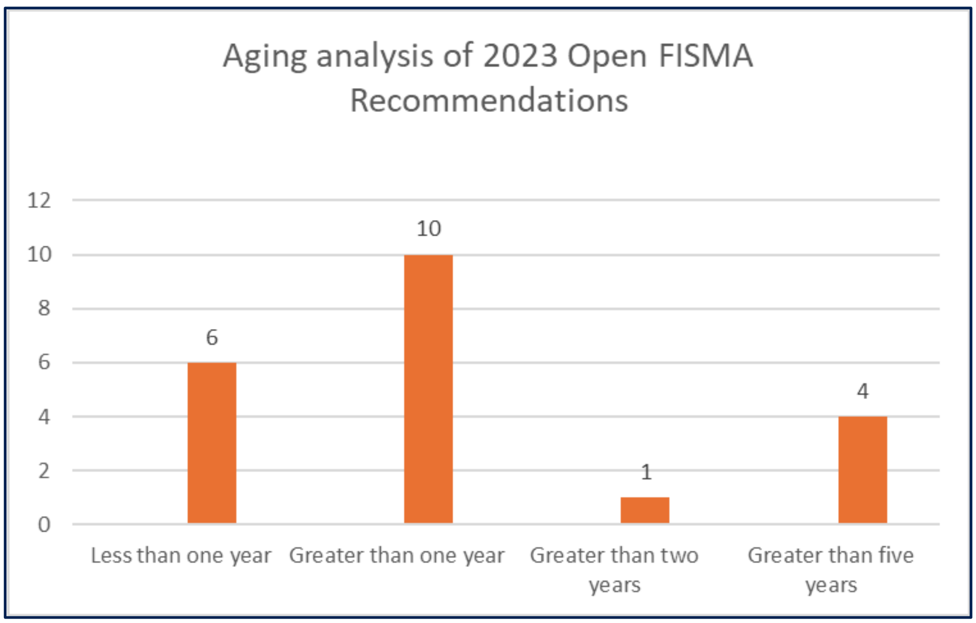
The FCC FY 2023 FISMA evaluation identified marked improvement for USAC in the I&AM domain, for which USAC implemented corrective actions to close three recommendations related to access control log reviews. However, OIG's FY 2023 FISMA report included eight recommendations related to deficiencies in the FCC's I&AM domain related to authentication, phishing, and access and privileged access management. The other cybersecurity domains with the remaining 13 open recommendations include risk management (RM), supply chain risk management (SCRM), configuration management (CM), and information systems continuous monitoring (ISCM).

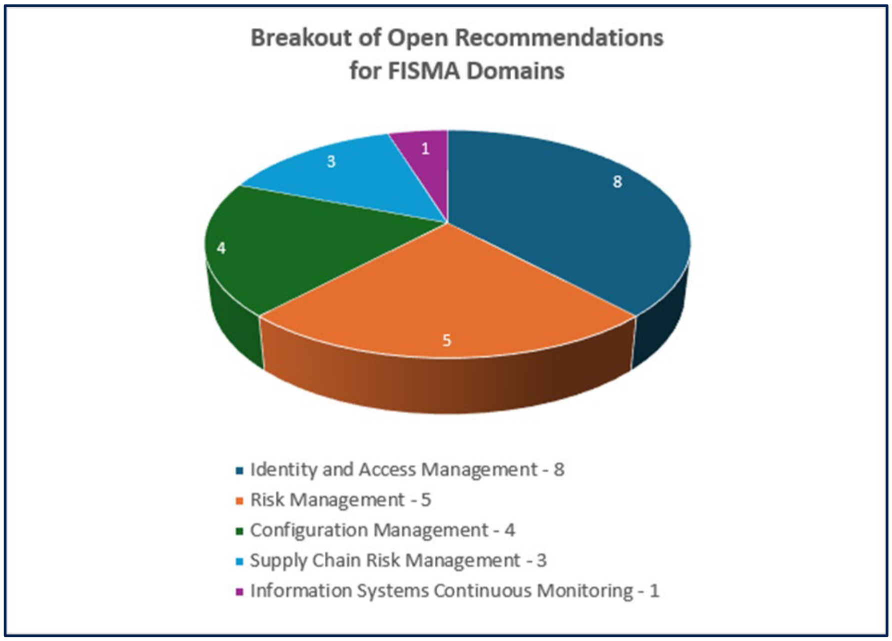
Compliance and effectiveness of the information and cyber security program will continue to be a significant challenge moving forward into FY 2025 and beyond as the Commission works to develop a focused approach to strengthen and sustain controls in all of the areas related to cybersecurity.

The FCC's history of longstanding FISMA recommendations, more than five years old, is consistent with the types of findings noted in the 2023 governmentwide FISMA report. As per the report, patch management, unsupported operating systems or applications and authentication bypass are the three most prevalent findings amongst federal agencies. For the FCC, two of these issues date back to FY 2017 and continue to remain a significant concern. FCC open recommendations more than five years old include a 2016 recommendation related to HSPD-12 authentication (I&AM); a 2017 recommendation related to action plans (risk management); and two 2018 recommendations, one for legacy systems (configuration management), and one for patching (Information Security Continuous Monitoring).

We are now closing out the FY 2024 FISMA evaluation and the overall result for this year mirrors FY 2023. The FCC's information security program was assessed as ineffective and not in compliance with FISMA legislation, OMB memoranda, and other applicable guidance. As a result of testing performed during the FY 2024 FISMA evaluation, we noted that one significant finding related to phishing from the I&AM domain that has been longstanding issue, was closed. This is a significant accomplishment, and the FCC's challenge will be to sustain the effort as the threat landscape for cybersecurity continues to increase and evolve.

See charts below for details of open recommendations aging and open recommendations by FISMA domain:





We continue to encourage the FCC to prioritize OIG recommendations to limit the risk of unauthorized access and to ensure consistent governance and compliance.

IT Modernization/Upgrading Legacy Systems

Since last year, the Commission reduced the number of legacy systems at the FCC from 40 to 27, marking progress in this important area. We note that the Commission's reliance on these systems increase the risk of exposure to security threats as many legacy systems lack patch updates or supported technology and may not be in compliance with changing standards. The FCC's migration of its on-premises systems to cloud computing is an important step towards IT modernization. It should ensure faster delivery of applications and services, scalability, and improved security, all of which will aid in more efficient operations. Implementing these cloud approaches is a huge undertaking, sometimes involving the need for cloud computing architecture, to ensure all of the systems can utilize the new cloud technologies. The FCC remains vulnerable and exposed to security and data breaches and management needs to continue to modernize the IT infrastructure and minimize the use of legacy systems.

As the FCC increasingly moves IT infrastructure and applications to the cloud, adversaries are advancing their capabilities to exploit features unique to cloud systems. Identity-based attacks are taking center stage, as adversaries focus on social engineering attacks that bypass multifactor authentication. The use of legitimate tools to execute an attack is an increasingly prevalent technique and impedes the FCC's ability to differentiate between normal activity and a breach. We are entering an era of a cyber arms race where artificial intelligence (AI) will amplify the impact for both the FCC security organization and the adversary. The FCC cannot afford to fall behind and the legacy technology currently in use is no match for the speed and sophistication of the modern adversary

This challenge and overall compliance and effectiveness of the information and cyber security program will continue to be a significant effort moving into FY 2025, until the Commission develops a focused approach to strengthening and sustaining controls in all the areas discussed above. We encourage the Commission to continue to address open recommendations related to IT modernization.

Privacy and Data Protection

In March 2024, OIG completed an Inspection of the FCC's Privacy and Data Protection Program, to determine whether the FCC implemented effective privacy and data protection policies and procedures in accordance with federal laws, regulations, and policies. The report concluded that the FCC has effectively implemented five of the nine privacy requirements in Title 42 U.S.C. § 2000ee-2 and offered six recommendations to implement technologies and update policies and directives related to privacy, which remain open.

These recommendations pertained to implementing technologies that sustain and do not erode privacy protections relating to the use, collection, and disclosure of information; implementing Endpoint Detection and Response tool for privacy protection; and annually reviewing and updating all privacy policies and directives. By implementing these recommendations, the FCC can mitigate risks to Personally Identifiable Information (PII), thereby limiting the impact of information system breaches and other privacy-related incidents. Additionally, updating FCC policies and directives in line with current federal guidance is important to ensure compliance with updated federal requirements.

OIG encourages the Commission's continued attention to addressing these important recommendations.

OIG AND GAO HIGHLIGHTED REPORTS

- FCC OIG Report 23-EVAL-05-01: FY 23 FISMA Evaluation for the FCC
- FCC OIG Report 21-INSP-10-01: FY 21 Privacy & Data Protection Inspection

Conclusion

Careful attention to these top management and performance challenges will help the Commission achieve its crucial mission of closing the digital divide by bringing affordable, reliable, high-speed broadband to 100% of our country. The FCC must also manage taxpayer dollars responsibly, and effectively carry out its regulatory telecommunications functions to promote public health and safety and safeguard national security.

Stay in Touch *with*

FCC Office of Inspector General

FCC Office of Inspector General

@FCCOIG

www.fcc.gov/inspector-general

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

EMAIL: hotline@fcc.gov

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.