March 2020

INFORMATION SECURITY

FCC Made Significant Progress, but Needs to Address Remaining Control Deficiencies and Improve Its Program

GAO Highlights

Highlights of GAO-20-265, a report to congressional requesters

Why GAO Did This Study

FCC relies extensively on information systems to accomplish its mission of regulating interstate and international communications in the United States. FCC uses one such system, ECFS, to receive public comments about proposed changes in FCC regulations. In May 2017, a surge in comments caused a service disruption of ECFS during a public comment period.

GAO was requested to review ECFS and the reported disruption. In September 2019, GAO issued a limited official use only report on the actions FCC took to respond to the May 2017 event, and the extent to which FCC had effectively implemented security controls to protect the confidentiality, integrity, and availability of selected systems.

This current report is a public version of the September 2019 report with sensitive information removed. In addition, for this public report, GAO determined the extent to which FCC has taken corrective actions to address the previously identified security program and technical control deficiencies and related recommendations for improvement. In the prior report, GAO compared FCC's policies, procedures, and reports to federal cybersecurity laws and policies. GAO examined logical access controls and security management controls for three systems selected based on their significance to FCC. For this report, GAO examined supporting documents regarding FCC's actions on previously identified recommendations, observed controls in operation, and interviewed personnel at FCC.

View GAO-20-265. For more information, contact Vijay A. D'Souza at (202) 512-6240 or dsouzav@gao.gov.

What GAO Found

As GAO reported in September 2019, the Federal Communications Commission (FCC) bolstered the capacity and performance of the Electronic Comment Filing System (ECFS) to reduce the risk of future service disruptions. FCC also implemented numerous information security program and technical controls for three systems that were intended to safeguard the confidentiality, integrity, and availability of its information systems and information.

However, GAO identified program and control deficiencies in the core security functions related to *identifying* risk, *protecting* systems from threats and vulnerabilities, *detecting* and *responding* to cyber security events, and *recovering* system operations. GAO made 136 recommendations to address these deficiencies (see table).

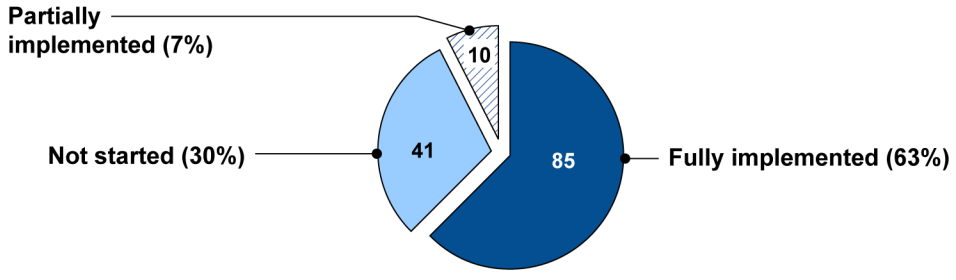
Number of GAO-Identified Information Security Program and Technical Control Deficiencies at FCC and Associated Recommendations by Core Security Function, as of September 2019

Core Security Function	Program-related deficiencies	Program-related recommendations	Technical control deficiencies	Technical control–related recommendations
Identify	3	4	0	0
Protect	1	1	37	108
Detect	0	0	6	17
Respond	2	2	1	2
Recover	2	2	0	0
Total	**8**	**9**	**44**	**127**

Source: GAO analysis of Federal Communications Commission information security program and technical controls. | GAO-20-265.

As of November 2019, FCC had made significant progress in resolving many security deficiencies by fully implementing 85 (about 63 percent) of the 136 recommendations GAO made in September 2019. FCC had also partially implemented 10, but had not started to implement the remaining 41 recommendations (see figure).

Status of the Federal Communications Commission's Efforts to Implement GAO Recommendations, as of November 2019



Source: GAO analysis of Federal Communications Commission data. | GAO-20-265

Additionally, FCC has created remedial action plans to implement the remaining recommendations by April 2021. Until FCC fully implements these recommendations and resolves the associated deficiencies, its information systems and information will remain at increased risk of misuse, improper disclosure or modification, and loss.