GAO

March 2020

INFORMATION SECURITY

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

Accessible Version

March 2020

INFORMATION SECURITY

FCC Made Significant Progress, But Needs To Address Remaining Control Deficiencies And Improve Its Program

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

Partially implemented (7%) — 10
Not started (30%) — 41
Fully implemented (63%) — 85
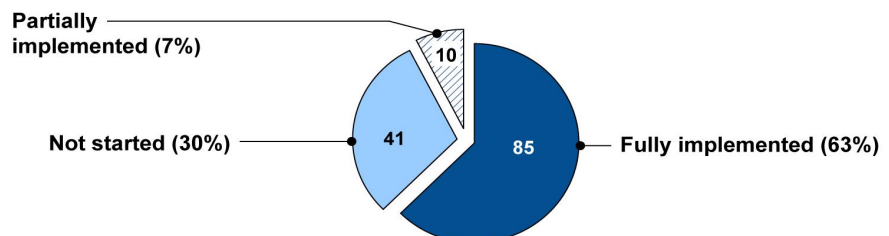
Source: GAO analysis of Federal Communications Commission data. | GAO-20-265

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.

—————————————— **United States Government Accountability Office**

Contents

Figures

Abbreviations

CIO	chief information officer
CISO	chief information security officer
ECFS	Electronic Comment Filing System
FCC	Federal Communications Commission
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act
FIPS	Federal Information Processing Standards
IT	information technology
ITC	Federal Communications Commission Information Technology Center
NIST	National Institute of Standards and Technology
NSOC	Network Security Operations Center
OGC	Federal Communications Commission Office of General Counsel
OIG	Federal Communications Commission Office of Inspector General
OMB	Office of Management and Budget
POA&M	plan of action and milestones
US-CERT	United States Computer Emergency Readiness Team

U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

March 25, 2020

Congressional Requesters

The security of federal information systems and data is critical to the nation's safety, prosperity, and well-being. To maintain that security, federal laws, policies, and guidelines require agencies to implement sufficient safeguards to protect the confidentiality, integrity, and availability of their information and information systems. However, threats to the federal information technology (IT) infrastructure continue to grow in number and sophistication, posing a risk to the reliable functioning of our government. Further, federal systems and networks are inherently at risk because of their complexity, technological diversity, and geographic dispersion.

The Federal Communications Commission (FCC) relies extensively on information systems to perform its mission of regulating interstate and international communications. One important information system is the Electronic Comment Filing System (ECFS), which FCC uses to receive public comments from interested parties (commenters) during rulemaking proceedings.[1]

In May 2017, ECFS experienced a surge in public comments that disrupted the system and affected its availability during a public comment period.[2] Specifically, the commission received more than 22 million comments through ECFS during the public comment period for FCC's 2017 Restoring Internet Freedom Notice of Proposed Rulemaking.[3] In August 2018, an FCC Office of Inspector General (OIG) investigative

---

[1]Rulemakings by many agencies are governed by the *Administrative Procedure Act*, which generally requires, among other things, that agencies allow any interested party the opportunity to comment on proposed regulations. This process, referred to as notice-and-comment rulemaking, gives the public an opportunity to provide information to agencies on the potential effects of a rule or to suggest alternatives for agencies to consider. 5 U.S.C. § 553.

[2]On May 8, 2017, the FCC Office of Media Relations issued a press release about the service availability of ECFS and stated the system was subjected to a distributed denial-of-service attack. A distributed denial-of-service attack is a malicious attempt to disrupt normal network traffic with excessive illegitimate traffic by multiple machines that are operating together to flood one target system.

[3]82 Fed. Reg. 25,568.

report attributed the disruption in ECFS's service to a combination of system capacity and performance issues.[4]

Given FCC's critical role in enabling the public to comment on its rulemaking process, you asked us to review the reported disruption to ECFS and the commission's efforts to secure its information systems. Specifically, our objectives were to determine: (1) the actions FCC took to respond to the May 2017 event that affected ECFS; and (2) the extent to which FCC implemented security controls to effectively protect the confidentiality, integrity, and availability of selected systems.

In September 2019, we issued a report that addressed the two objectives.[5] In the report, we made nine recommendations to FCC to improve its information security program and 127 additional recommendations to resolve technical control deficiencies in the information systems we reviewed. We designated that report as "limited official use only" (LOUO) and did not release it to the general public because of the sensitive information it contained about FCC systems' operating environments and shortcomings that could potentially be exploited.

This subsequent report publishes the findings discussed in our September 2019 report, but we have removed all of the sensitive information.[6] Specifically, we deleted the names of the information system software, network devices, and resource tools that we examined; disassociated identified control deficiencies from named systems; deleted certain details about information security controls and control deficiencies; and omitted an appendix contained in the LOUO report. That appendix contained sensitive details about the technical security control deficiencies in FCC's information systems and computer networks that we reviewed, and the 127 recommendations we made to mitigate those deficiencies. We also provided a draft of this report to FCC officials to review and comment on the sensitivity of the information contained herein and to affirm that the report can be made available to the public without

---

[4]Federal Communications Commission, Office of Inspector General, *Alleged Multiple Distributed Denial-Of-Service (DDoS) Attacks involving the FCC's Electronic Comment Filing System (ECFS)* Memorandum, (Washington, D.C.: June 20, 2018).

[5]GAO, *Information Security: FCC Improved Its Electronic Comment System, but Needs to Remedy Additional Control Weaknesses*, GAO-19-247SU (Washington, D.C.: September 26, 2019).

[6]GAO-19-247SU.

jeopardizing the security of the commission's information systems and networks.

In addition, this report addresses a third objective that was not included in the September 2019 report. Specifically, this objective was to determine the extent to which FCC has taken corrective actions to address the previously identified information security program and technical control deficiencies and related recommendations for improvement that we identified in the earlier report.

As noted in the September 2019 report, to address the first objective—to determine the actions FCC had taken to respond to the May 2017 event that affected ECFS—we reviewed the commission's security and incident response policy and procedures, examined FCC and its Office of Inspector General's reports, reviewed system enhancement and performance artifacts, and interviewed FCC officials, including the system and security staff and OIG officials.[7] We examined the aforementioned documents to determine whether updated incident response policy and procedures, along with system enhancement and performance artifacts, were directly related to changes made subsequent to the May 2017 event.

To address the second objective, we selected three systems for our review. We selected these systems because they (1) are essential to FCC's mission and (2) were assigned a Federal Information Processing Standards (FIPS) Publication 199 rating of moderate or high impact.[8] The results of our review are not generalizable to the commission's other systems.

We examined the information security program-related activities implemented for the three selected systems. For example, we analyzed FCC's information security policies; procedures; and artifacts associated

---

[7]GAO-19-247SU.

[8]National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems,* Federal Information Processing Standards (FIPS) Publication 199 (Gaithersburg, MD: February 2004). The standards require agencies to categorize each information system according to the magnitude of harm or impact should the system or its information be compromised. The standards define three impact levels where the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (low), a serious adverse effect (moderate), or a severe or catastrophic adverse effect (high) on organizational operations, organizational assets, or individuals.

with risk assessments, security plans, remedial action plans, and contingency plans. Specifically, we compared the commission's security policies and procedures to National Institute of Standards and Technology (NIST) special publications to assess the FCC documents' consistency with federal guidelines.[9] We also examined security-related artifacts, plans, and reports.

Additionally, we examined technical security controls implemented for the three systems. In this regard, we observed and analyzed controls in place to determine if they were appropriately designed, operating as intended, and effective. We supplemented our analysis with interviews of FCC Information Technology Center personnel and other relevant officials. We conducted our work at three FCC facilities located in Pennsylvania, Washington, D.C., and West Virginia.

To accomplish our third objective—our analysis of FCC's actions to address the previously identified information security program and technical control deficiencies and related recommendations—we requested that the agency provide a status report of its actions to implement each recommendation we made in the September 2019 report.[10] For each recommendation that FCC indicated it had implemented as of November 2019, we examined supporting documents, observed or tested the associated security control or procedure, and/or interviewed the responsible FCC officials to assess the effectiveness of the actions taken to implement the recommendation or otherwise resolve the underlying control deficiency. Based on this assessment and the FCC status reports, we categorized the status of each recommendation as

---

[9]These special publications include: National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, MD: April 2013); *Guidelines on Security and Privacy in Public Cloud Computing*, Special Publication 800-144 (Gaithersburg, MD: Dec. 2011); *Computer Security Incident Handling Guide*, Special Publication 800-61, Revision 2 (Gaithersburg, Md.: August 2012); *Contingency Planning Guide for Federal Information Systems* Special Publication 800-34, Revision 1 (Gaithersburg, Md.: May 2010); *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities,* Special Publication 800-84 (Gaithersburg, Md.: September 2006).

[10]GAO-19-247SU.

being "fully implemented," "partially implemented," or "not started."[11] Additional details on our objectives, scope, and methodology are provided in appendix I.

We conducted the performance audit for the first two objectives from February 2018 through September 2019 in accordance with generally accepted government auditing standards. We conducted work supporting the third objective and, where applicable, included updates to our work in the second objective from October 2019 through March 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Established by the *Communications Act of 1934*, FCC regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia, and U.S. territories.[12] FCC is responsible for, among other things, making available nationwide worldwide wire and radio communication service. More recently, it has been responsible for promoting competition and reducing regulation of the telecommunications industry in order to secure lower prices and higher quality services for consumers.[13]

FCC's functions include:

---

[11]These terms are defined as: *fully implemented*—FCC had implemented the recommendation (i.e., the commission provided evidence showing that it had effectively resolved the underlying control deficiency); *partially implemented*—FCC had made progress toward, but had not completed implementing the recommendation (i.e., the commission provided evidence showing that it had effectively resolved a portion of the underlying control deficiency); and *not started*—FCC did not provide evidence that it had acted to implement the recommendation (i.e., the commission provided no evidence showing that it had effectively resolved the underlying control deficiency).

[12]47 U.S.C. § 151.

[13]The *Telecommunications Act of 1996*, which substantially amended the *Communications Act of 1934*, comprehensively reformed the nation's telecommunications statutory and regulatory framework. Pub. L. No. 104-104, 110 Stat. 56 (1996).

- issuing licenses for broadcast television and radio;

- overseeing licensing, enforcement, and regulatory functions of carriers of cellular phones and other personal communication services;

- regulating the use of radio spectrum and conducting auctions of licenses for spectrum;

- investigating complaints and taking enforcement actions if it finds that there have been violations of the various communications laws and commission rules that are designed to protect consumers;

- addressing issues related to public safety, homeland security, emergency management, and preparedness;

- educating and informing consumers about communications goods and services; and

- reviewing mergers of companies holding FCC-issued licenses.

FCC Relies on Information Technology to Support Its Operations

FCC relies extensively on computerized systems to support its mission-related operations, and on information security controls to protect the commission's data. FCC's Information Technology Center, within the Office of the Managing Director, uses IT to perform the commission's business operations.[14] Through its computer network and systems, the commission collects and maintains nonpublic information, including proprietary information of businesses regulated by the commission, as well as information available to the public through rulemaking proceedings.

FCC Has Defined Organizational Roles and Responsibilities for Information Security

FCC's Chairman, chief information officer (CIO), and chief information security officer (CISO) each have specific responsibilities for information

---

[14]The Office of the Managing Director is responsible for the administration and management of the commission. Specifically, the office manages the commission's budget and financial programs; human resources; contracts and purchasing; communications and computer services; physical space; security; the commission meeting schedule; and distribution of official FCC documents.

security. Specifically, the FCC Chairman has responsibility for, among other things:

1. providing information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the commission's information systems and information;

2. ensuring that senior officials provide security for the information and systems that support the operations and assets under their control; and

3. delegating to the CIO the authority to ensure compliance with the information security requirements imposed on the commission.

In addition, the CIO is responsible for establishing and enforcing policies and procedures for protecting information resources. Toward this end, the CIO has designated and assigned responsibilities to the CISO for managing the cybersecurity program. The CISO, among other things, is responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the commission.

Federal Law and Guidance Establish Security Requirements to Protect Federal Information and Systems

The *Federal Information Security Modernization Act of 2014* (FISMA) provides a comprehensive framework for information security controls over information resources that support federal operations and assets.[15] The law also requires each agency to develop, document, and implement an agency-wide information security program to provide risk-based protections for the information and information systems that support the operations and assets of the agency.

---

[15]The *Federal Information Security Modernization Act of 2014* (FISMA) (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

Such a program should include assessing risks; developing and implementing policies and procedures to cost-effectively reduce risks; developing and implementing plans for providing adequate information security for networks, facilities, and systems; and providing security awareness and specialized training. Further, the program should include testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; developing and implementing procedures for detecting, reporting, and responding to security incidents; and ensuring continuity of operations.

FISMA requires agencies to comply with the federal information processing standards (FIPS) publications issued by NIST and Office of Management and Budget (OMB) Circular A-130[16] requires agencies to comply with the information security guidelines prescribed in NIST special publications. Consequently, NIST FIPS publications and special publications contain many of the cybersecurity-related requirements for federal agencies. For example, NIST FIPS Publication 199 requires agencies to categorize their information and information systems according to the potential harm and impact to agency assets, operations, or individuals should the confidentiality, integrity, or availability of its information and information systems be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction.[17]

In addition, NIST FIPS Publication 200[18] requires agencies to meet minimum security requirements by selecting the appropriate security controls, as described in NIST Special Publication 800-53.[19] This special publication provides a catalog of 18 security control areas for federal information systems and a process for selecting controls to protect

[16]Office of Management and Budget, *Managing Information as a Strategic Resource*, OMB Circular A-130 (Washington, D.C.: July 2016).

[17]National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication 199 (Gaithersburg, MD: Feb. 2004).

[18]National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards Publication 200 (Gaithersburg, MD: March 2006).

[19]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, MD: April 2013).

organizational operations and assets.[20] The publication provides baseline security controls for low-, moderate-, and high-impact systems, and agencies have the ability to tailor or supplement their security requirements and policies based on agency mission, business requirements, and operating environment.

Further, in May 2017, the President issued an executive order[21] requiring agencies to immediately begin using NIST's cybersecurity framework for managing their cybersecurity risks.[22] The framework, which provides guidance for cybersecurity activities, is based on five core security functions:

- Identify: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

- Protect: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

- Detect: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.[23]

- Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity incident.

---

[20]Security control topics, referred to as families of security controls, covered by NIST Special Publication 800-53 include access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

[21]The White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Executive Order No. 13800, 82 Fed. Reg. 22391 (May 11, 2017).

[22]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Feb. 12, 2014). The framework was developed in response to an executive order issued by the prior administration, *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636 (Washington, D.C.: Feb. 12, 2013). It was originally intended for use in protection of critical infrastructure. The framework has since been updated in April 2018. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Apr. 16, 2018).

[23]According to NIST, a cybersecurity event is defined as a cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).

- Recover: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

According to NIST, these five functions occur concurrently and continuously, and provide a strategic view of the life cycle of an organization's management of cybersecurity risk. Within the five functions are 23 categories and 108 subcategories that include information security program-related controls and technical controls for achieving the intent of each function.[24] Appendix II provides a description of the framework categories and subcategories of controls.

FCC Experienced a Service Disruption in May 2017

On May 7 and 8, 2017, FCC experienced a dramatic surge in the number of comments sent to the commission through its ECFS during a public comment period. This surge led to a disruption of services, which prevented the system from being able to accept additional comments for a period of time. The FCC Office of Inspector General determined that the system service disruption was likely due to a combination of the sudden increase in traffic from commenters all trying to access the system's website over a short period of time and system design deficiencies that negatively impacted the capacity and performance of the system to collect and process the increase in traffic.[25] Figure 1 presents a timeline of the May 2017 ECFS service disruption and subsequent related events. Additional details on the timeline are provided in appendix III.

---

[24]For example, "risk assessment" is one of six categories that comprise the "identify" function. The risk assessment category is divided into six subcategories that involve activities such as identifying and documenting internal and external threats; identifying potential business impacts and likelihoods; and determining risk based on threats, vulnerabilities, likelihoods, and impacts. Each subcategory activity cross-references information system controls from various information security publications, including NIST's Special Publication 800-53.

[25]Federal Communications Commission, Office of Inspector General, *Alleged Multiple Distributed Denial-Of-Service (DDoS) Attacks involving the FCC's Electronic Comment Filing System (ECFS)*, memorandum (Washington, D.C.: June 20, 2018).

Figure 1: The Federal Communications Commission's Electronic Comment Filing System May 2017 Service Disruption and Subsequent Related Events Timeline

May 2017 service disruption of the Electronic Comment Filing System

APRIL 27
Federal Communications Commission (FCC) issued a public notice of Restoring Internet Freedom rulemaking proceedings

MAY 8
EARLY MORNING:
Electronic Comment Filing System (ECFS) site became unavailable to commenters

Vendor sent alert and network data to FCC Information Technology Center

MID-MORNING:
FCC Information Technology Center responded to alerts and initiated stabilization efforts

LATE AFTERNOON:
FCC issued a press release statement of an alleged cyberattack on ECFS

MAY 7
LATE EVENING:
Late night talk show aired a segment on making comments on the Restoring Internet Freedom proceedings

Heavy web traffic slowed down ECFS

MAY 9-10
FCC Information Technology Center restored ECFS but experienced system performance issues

MAY 10
FCC Information Technology Center responded to inquiries from the Federal Bureau of Investigations and FCC Office of Inspector General

June 21, 2017	FCC Office of Inspector General opened an investigation of an alleged cyberattack of ECFS.
January 4, 2018	FCC Office of Inspector General referred the ECFS investigation to the Department of Justice.
August 7, 2018	FCC Office of Inspector General published an investigative report on the ECFS event.
August 16, 2018	FCC Chairman testified at a Senate oversight hearing on the investigative report on the ECFS event.

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

FCC Increased ECFS's Capacity and Performance to Reduce Risk of Future Service Disruptions

In response to the ECFS service disruption that occurred on May 7 and 8, 2017, FCC Information Technology Center officials took four key actions to reduce the risk of future service disruptions to the system.

1. Conducted Internal Assessments

- In response to the service disruption, in early May 2017, the FCC CIO initially stated that the cause was a cyberattack on the ECFS. However, upon further assessment, FCC Information Technology Center officials later determined that the disruption was caused by a surge in comment traffic to the system and existing system performance and capacity deficiencies.

- In response to multiple congressional inquiries, in late July 2017, FCC Information Technology Center officials assessed the extent to which malicious intent was involved in causing the disruption based on whether: (a) internet protocol (IP) addresses from foreign sources[26] were present on the commission's network at the time of the May 2017 event; (b) comment submissions were denied (i.e., dropped) from the commission's network, (c) observable botnet traffic was present;[27] and (d) duplicate comment submissions were accepted into ECFS.[28] The assessment concluded that the commission did not have sufficient information and tools to determine whether there was any malicious intent.

2. Deployed Additional Virtual Hardware

- Following the disruption, in early May 2017, FCC deployed additional virtual hardware to address system performance issues and support

---

[26]According to FCC's response letter to Congress, dated February 5, 2018, the ECFS is designed to accept (i.e., allow) comments in any form or source, which would include foreign IP source locations. ECFS does not obtain or store IP addresses as part of the comment data it collects when a public user submits a comment. Within the current architecture, ECFS would require officials to match date and time stamps from the proxy server log to the ECFS comment data to connect a given IP address to a specific comment. GAO, *Federal Rulemaking: Selected Agencies Should Clearly Communicate Practices Associated with Identity Information in the Public Comment Process,* GAO-19-483 (Washington, D.C.: June 26, 2019).

[27]Botnets are a network of remotely controlled systems used to coordinate attacks and distribute malware, spam, and phishing scams. Bots (short for "robots") are programs that are covertly installed on a targeted system, allowing an unauthorized user to remotely control the compromised computer for a variety of malicious purposes.

[28]Duplicate comment submissions are regularly accepted as part of the rulemaking process under the *Administrative Procedure Act*, and we have previously reported on how selected agencies, including FCC, post these comments on their respective comment sites, GAO-19-483.

system stabilization efforts of ECFS during the period in which service was disrupted.[29]

- In early July 2017, the commission installed security sensors and forwarding agents on the ECFS virtual servers.[30] These devices are intended to provide additional layers of security capability for the system.

- In mid-July 2017, FCC automated the process for deploying virtual hardware resources to support system availability subsequent to the May 2017 service disruption.

3. Optimized and Acquired System Software

- From late May 2017 to early June 2017, FCC acquired a diagnostic tool to measure system performance. According to the commission, this tool is used to determine the maximum amount of simultaneous user capacity within ECFS during periods of high web traffic.

- In early June 2017, the commission optimized the search functionality within the ECFS database to reduce the system response time.

- In mid-June 2017, FCC removed redundant internal processes for ECFS web requests to increase the responsiveness of the system.

- During late July 2017, the commission acquired a security information and event management tool to collect and analyze security-related events that may indicate a cybersecurity incident.

- In late August 2017, FCC established rate control limits within ECFS to safeguard against potential distributed denial-of-service attacks aiming to flood one target with network traffic.[31]

4. Updated Incident Response Policy and Procedures

---

[29]Virtual hardware is a simulation of the hardware (such as central processing units, disk storage, memory, and network interface cards) upon which other software runs like operating systems and their associated applications.

[30]Forwarding agents are software features that copy network traffic data from a virtual hardware resource device to a sensor for the purpose of passively monitoring network traffic.

[31]A denial-of-service attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. A distributed denial-of-service (DDoS) attack occurs when multiple machines are operating together to attack one target. DDoS allows for exponentially more requests to be sent to the target, therefore increasing the attack power. It also increases the difficulty of attribution, as the true source of the attack is harder to identify.

- In January 2018 and March 2018, during its annual policy review, FCC Information Technology Center officials updated the commission's incident response and reporting policy and procedures to incorporate lessons learned from the May 2017 ECFS service disruption and clarify their processes. For example, FCC Information Technology Center officials revised the commission's incident response procedures to document internal escalation time frames for notifying management of potential security incidents and reporting the incidents to the United States Computer Emergency Readiness Team within 1 hour of identification of an incident.

Figure 2 shows a chronological sequence of the hardware and software improvements that FCC officials implemented after the May 2017 event.

Figure 2: FCC Improvements to the Electronic Comment Filing System (ECFS) in Response to the May 2017 Service Disruption (as of November 2018)

Early May 2017
Deployed additional virtual hardware resources to address system performance issues with the Electronic Comment Filing System (ECFS)

Late May/Early June 2017
Acquired diagnostic tool to measure system performance

Early June 2017
Optimized the search functionality within the ECFS database

Mid-June 2017
Removed redundant internal processes for ECFS web requests

Early July 2017
Installed security sensors on ECFS virtual servers

Mid-July 2017
Automated process for deploying virtual hardware resources to support system availability

Late July 2017
Acquired security information and event management tool to collect and analyze security-related events

Late August 2017
Established rate control limits within ECFS to safeguard against potential cyber security attacks aiming to flood one target with network traffic

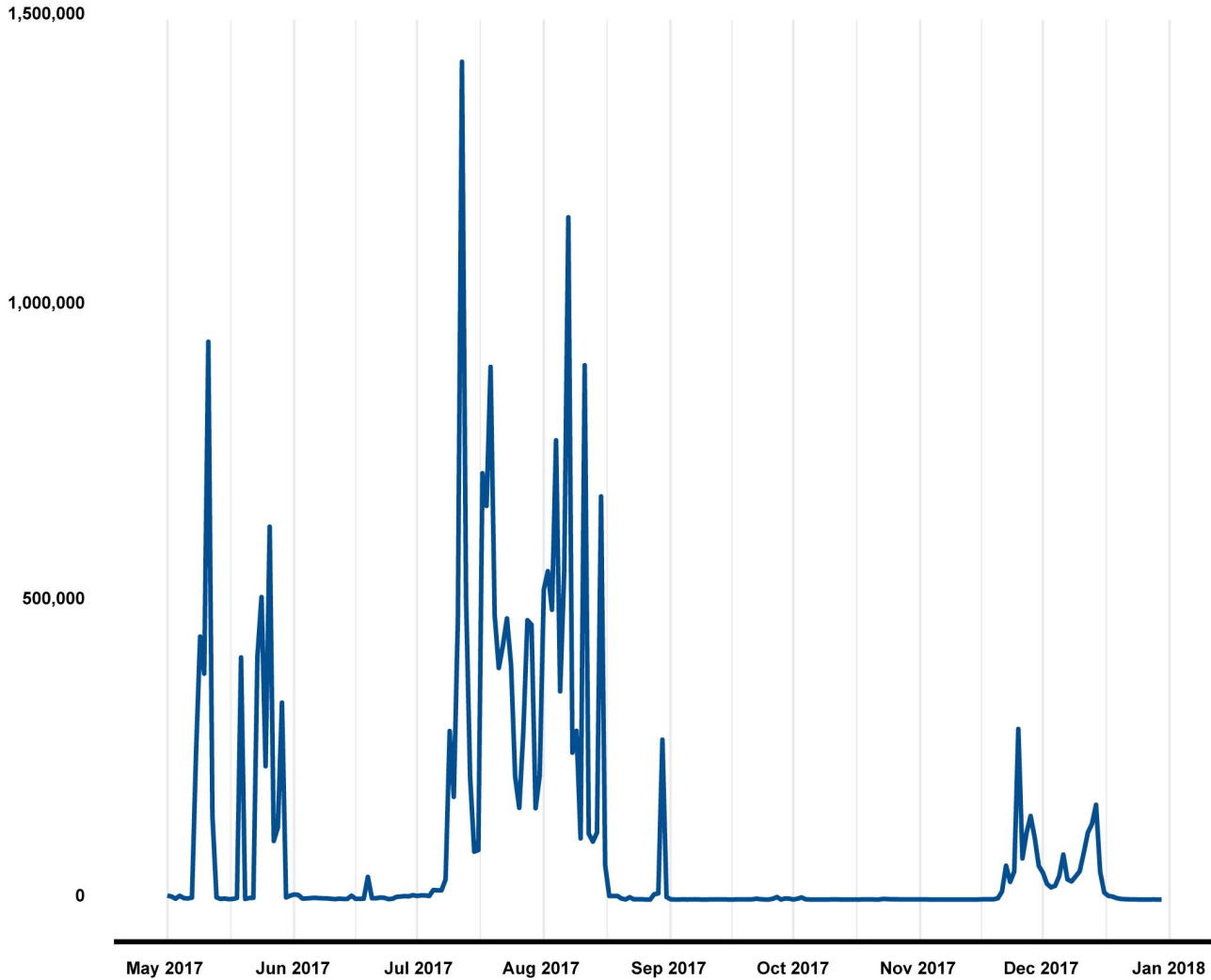Source: GAO analysis of Federal Communications Commission information. | GAO-20-265

FCC provided evidence that indicated its actions to add additional hardware and software resources increased ECFS's capacity and performance and demonstrated that the system was stable from June 2017 through December 2017. For example, FCC acquired a performance diagnostic tool in late May 2017, which was designed to

determine the maximum number of potential simultaneous public users within ECFS during periods of high web traffic. Using the diagnostic tool, FCC Information Technology Center officials determined in June 2017, that the system became unstable when the number of simultaneous simulated public users reached 500. However, by December 2017, the system had demonstrated that it could accept a capacity of over 3,000 simultaneous public users without a service disruption.

FCC data showed that the increased capacity and improved performance of the ECFS prevented further service disruptions during periods of sharp spikes in the volume of comments received. For example, on May 8, 2017, service was disrupted on the system when it received a peak of about 249,000 comments in 1 day, whereas on July 12, 2017, the system accepted and processed at least 1.4 million comments in 1 day without a reported service disruption. Similar spikes in traffic volumes that occurred through December 2017 also did not result in service disruptions. Figure 3 shows the daily comment submissions to ECFS from May 2017 through December 2017 and demonstrates FCC's ability to accept a higher volume of comments without a service disruption.

Figure 3: Daily Comments Submitted to, and Accepted by, FCC's Electronic Comment Filing System (ECFS), May 1, 2017 through December 31, 2017

Number of daily submissions to ECFS application programming interface (API)

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

Note: This graphic reflects the total number of submissions, by day, for all Standard and Express filings submitted to Federal Communications Commission proceedings, including the Restoring Internet Freedom rulemaking proceeding. These data may include non-rulemaking proceedings, but do not include non-docketed filings. The underlying data were extracted by GAO and derived from the data.gov application programming interface.

FCC Did Not Consistently Implement Security Controls, Which Placed Selected Systems at Risk

We reported in September 2019 that FCC had implemented numerous security controls for the three systems we reviewed, but it had not consistently implemented the NIST cybersecurity framework's five core security functions to effectively protect the confidentiality, integrity, and availability of these systems and the information maintained on them.[32] Deficiencies existed in the FCC information security program and technical controls for the five core functions that were intended to (1) identify risk, (2) protect systems from threats and vulnerabilities, (3) detect cybersecurity events, (4) respond to these events, and (5) recover system operations when disruptions occur. These deficiencies increased the risk that sensitive information could be disclosed or modified without authorization or be unavailable when needed.

As shown in table 1, deficiencies existed in all five core security functions for the FCC systems we reviewed. Also shown are the numbers of recommendations we made to FCC to rectify the deficiencies.

Table 1: 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	Number of information security program deficiencies	Number of information security program recommendations	Number of technical control deficiencies	Number of technical control deficiency 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.

Note: The five core security functions are part of the NIST cybersecurity framework, as updated in National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure*

---

[32]GAO-19-247SU.

Cybersecurity (Gaithersburg, MD: Apr. 16, 2018). As discussed later in this report, FCC has taken action to address many of these deficiencies and associated recommendations.

FCC Generally Identified Risks and Developed Security Plans for Selected Systems, but Shortcomings Remained

Activities associated with the identify core security function are intended to help an agency to develop an understanding of its resources and related cybersecurity risks to its organizational operations, systems, and data. Essential elements of a FISMA-mandated information security program include assessing risks, developing system security plans, and authorizing information systems to operate.[33] NIST guidance states that agencies should assess risks and authorize systems on an ongoing basis.[34] Additionally, FCC requires that security plans, risk assessments, and system authorizations be reviewed annually or whenever significant changes occur to the information system, computing environment, or business operations.

Consistent with its guidance, FCC had developed system security plans for each of the three systems we reviewed and had updated the risk assessments for two of the systems in 2017 and 2018, respectively. However, as of March 2019, the commission had not reviewed or updated the risk assessment for the third system reviewed since May 2017—a lag of about 22 months. Commission officials stated that they had not reviewed or updated the system's risk assessment because the commission had implemented a new risk assessment process and officials had not yet had time to review and update documentation for this system.

[33]According to the Office of Management and Budget, the authorization to operate an information system is based on a determination of the risk to agency operations and assets, individuals, other organizations, and the nation, resulting from the operation and use of the system and the decision by the authorizing official that this risk is acceptable. The authorizing official is to be a senior federal official or executive with the authority to authorize the operation of the system and be responsible and accountable for the risks associated with operating the system. See OMB, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016).

[34]National Institute of Standards and Technology, *Supplemental Guidance on Ongoing Authorization, Withdrawn White Paper* (Gaithersburg, MD: June 2014). NIST defines "ongoing" as a frequency that is sufficient to support risk-based security decisions to adequately protect organizational information. (Note: This publication was withdrawn by NIST in April 2019 and has been rolled into Special Publication 800-37 Rev. 2 (December 2018).)

In addition, FCC continued to operate two of the three selected systems on expired authorizations to operate. Although FCC granted a full authorization to operate to one system in May 2018, the commission allowed the authorizations for the other two systems we reviewed to expire. Both of these systems had received a conditional authorization to operate[35] so that the systems could continue to operate while the commission mitigated known system vulnerabilities. However, in December 2018, the conditional authorizations for both systems expired because, according to FCC officials, the commission had not mitigated the vulnerabilities. Nevertheless, FCC continued to operate the systems.

By not regularly updating the risk assessment of one system and continuing to operate another system without a current authorization to operate, FCC unnecessarily exposed the information on these systems to increased risks of unauthorized changes and access to information.

Subsequent to our September 2019 report, FCC reviewed and updated the system's risk assessment in accordance with its new risk assessment process. In addition, FCC granted a full authorization to operate to one of the systems in October 2019, but does not expect to grant a full authorization to operate for the other system until later in 2020.

FCC's Contract Provisions with Its Cloud Service Provider Did Not Reflect All Applicable Security Requirements

NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, states that a service-level agreement should define the terms and conditions for access and use of the services offered by the cloud service provider.[36] In addition, FedRAMP Control Specific Contract Clauses provides security control specifications that may need to be included in the task order for the service and specified in the service level agreement.[37] These contract clauses include specifications related to data

---

[35]A conditional authority to operate is a temporary authorization that can become a full authorization when certain conditions are met.

[36]National Institute of Standards and Technology, *Guidelines on Security and Privacy in Public Cloud Computing*, Special Publication 800-144 (Gaithersburg, MD: Dec. 2011).

[37]Federal Risk and Authorization Management Program, *FedRAMP Control Specific Contract Clauses* (Washington, D.C.: Dec. 2017). A service-level agreement defines levels of service and performance that the agency expects the contractor to meet and the agency uses the information to measure the effectiveness of its cloud services.

jurisdiction, audit records storage, time frames for reporting security incidents, and system boundary protection.[38]

FCC's task order and service level agreement with its cloud service provider specified activities the provider was to perform, such as providing access and support for products and services, and completing performance deliverables to ensure service availability. However, FCC had not documented specific contract clauses associated with implementing security control requirements related to retaining audit records, meeting reporting incident time frames, and protecting system boundaries in accordance with FedRAMP.

According to FCC's associate chief information officer, the commission relied on FedRAMP's oversight to ensure that its cloud provider implemented security controls that comply with federal data requirements. However, FedRAMP assesses and monitors only the security controls that the program and cloud service provider agree that the provider will implement. These agreed-upon controls may not include an agency's specific security requirements. Thus, responsibility falls on FCC to ensure that its information security requirements are being implemented in cloud computing environments.

Nevertheless, by not specifying its specific control requirements when procuring services from its cloud provider, FCC increased the risk that its data and sensitive regulatory information will not be adequately protected in the event that its cloud service provider experiences a security breach.

Subsequent to our September 2019 report, FCC developed a plan of action and milestones (POA&M) for this deficiency and stated that it plans to rectify the deficiency by May 2020.

FCC Did Not Consistently Implement Appropriate Safeguards to Protect Information on Selected Systems

Activities associated with the protect core security function are intended to help agencies develop and implement appropriate system safeguards. These activities include limiting access to computing resources to

---

[38]Agencies with specific data location or jurisdiction requirements must include contractual requirements identifying where data-at-rest (primary and replicated storage) shall be stored. The controls in NIST SP 800-53 do not govern data location, and providers may describe boundaries that include foreign data centers.

authorized users, processes and devices; encrypting data to protect its confidentiality and integrity; configuring devices securely; and updating software to protect systems from known vulnerabilities.

FCC implemented activities that established multiple layers of technical controls, including access controls and firewalls, encryption of sensitive data, and system configuration management. However, we reported in September 2019 that implementation of these technical controls were not consistent.[39] For example, 37 technical control deficiencies and an information security program-related deficiency diminished the effectiveness of the controls protecting the systems we reviewed. A brief summary of the results of our tests of FCC's controls for protecting the three systems we reviewed follows.

FCC Did Not Consistently Implement Effective Access Controls

FCC policy states that, in accordance with NIST SP 800-53 guidelines, users should not share the same identifier and the commission should configure its information systems to require users to create complex passwords.[40] FCC's policy also stipulates that the commission employ the principle of "least privilege"[41] and enforce approved authorizations for controlling the flow of information within the system and between interconnected systems.[42]

However, FCC did not consistently implement technical controls to effectively limit access to the systems we reviewed, as the following examples illustrate.

- Although FCC policy states that individual user accounts are not to be shared, the commission allowed multiple users to share the credentials of several privileged accounts.

---

[39]GAO-19-247SU.

[40]Federal Communications Commission, *FCC Identification and Authentication Policy*, Version 1.3 (Washington, D.C.: March 30, 2018).

[41]Federal Communications Commission, *FCC Policy for Access Control*, Version 4.1 (Washington, D.C.: March 30, 2018). Least privilege states that a subject should be given only those privileges needed for it to complete its task.

[42]Federal Communications Commission, *FCC Policy for System and Communications Protection*, Version 1.5 (Washington, D.C.: March 30, 2018).

- While FCC policy established minimum requirements for password complexity and account lock-out provisions, the commission did not routinely enforce these requirements.

- While FCC policy requires limiting access rights for users to only those they need to perform their work, the commission inappropriately granted excessive permissions to users to access server configuration files.

- Although FCC established a policy for monitoring and controlling access between systems, it did not securely configure network devices to effectively control access and communications between systems.

Access control deficiencies existed primarily because FCC network administrators did not adequately monitor configuration settings and did not implement sufficient controls to enforce consistent authentication and authorization across all of the commission's systems that we reviewed. However, until FCC fully implements those actions and remediates related technical deficiencies, the commission remains at increased risk that unauthorized individuals or attackers could obtain inappropriate access to its network devices, firewalls, and servers, and compromise its network.

As of November 2019, FCC had acted to address several technical control deficiencies related to access control.

FCC Did Not Consistently Encrypt Sensitive Data

NIST SP 800-53 recommends that organizations employ cryptographic mechanisms to prevent the unauthorized disclosure of information during transmission and establish a trusted communications path between users and security functions of information systems. NIST also requires that, when agencies use encryption, they use an encryption algorithm that complies with FIPS Publication 140-2.[43] In addition, FCC's System and Communication Protection Policy states that confidentially sensitive data

---

[43]National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards Publication 140-2 (Gaithersburg, MD: May 25, 2001).

must be encrypted before being transmitted using any nonprotected communication method and that all passwords must be encrypted.[44]

However, in seven instances, the commission did not consistently deploy strong encryption capabilities to protect sensitive data or establish a secure communications path between users and information systems. For example, FCC sometimes sent data in clear text over the network and did not enable FIPS 140-2 compliant encryption algorithms on certain devices. These deficiencies existed primarily because commission personnel did not adequately monitor configuration settings. By not consistently deploying strong encryption capabilities, FCC limits its ability to protect the confidentiality and integrity of its sensitive information.

According to Information Technology Center officials, as of November 2019, the commission was still working toward full compliance with federal encryption standards.

<u>FCC Did Not Consistently Configure Servers Securely or Update Software in a Timely Manner</u>

NIST SP 800-53 states that agencies should configure security settings to the most restrictive mode consistent with operational requirements and disable services within the information system deemed to be unnecessary or non-secure. FCC policy on risk assessment states that systems and devices should be scanned periodically and software patches should be applied for all known critical security vulnerabilities.[45] In addition, OMB Circular A-130 states that agencies are to implement current updates and patches for all software components of information systems, and prohibit the use of unsupported systems and system components.[46]

Although FCC established policies for applying software patches on a prescribed basis, it did not update software in a consistent or timely manner to effectively protect the three systems we reviewed. For

---

[44]Federal Communications Commission, *FCC Policy for System and Communications Protection*, Version 1.5 (Washington, DC: March 30, 2018).

[45]Federal Communications Commission, *FCC Policy for Risk Assessment*, Version 1.4 (Washington, DC: March 30, 2018). DHS Binding Operational Directive 19-02 requires federal agencies to remediate the critical and high vulnerabilities within 15 and 30 days upon initial detection, respectively.

[46]Office of Management and Budget, *Managing Federal Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016).

example, FCC did not apply software patches in a timely manner to resolve known security vulnerabilities, and used unsupported or out-of-date system software on multiple network devices, firewalls, and servers.

Patching control deficiencies existed because FCC did not adequately monitor configuration settings of devices on its network. According to Information Technology Center officials, as of February 2019, the commission was in the process of (1) migrating and modernizing its systems' portfolio and (2) implementing an application monitoring and testing tool to reduce patching times. However, until FCC applies software patches in a timely manner, and replaces unsupported software and devices, it will remain at increased risk that individuals could exploit known vulnerabilities to gain unauthorized access to its computing resources.

As of November 2019, FCC had taken corrective actions to address certain technical control deficiencies related to configuring servers securely and updating software in a timely manner.

Although FCC Had Documented Security Policies, It Had Not Documented Operational Procedures

Developing, documenting, and implementing information security policies and procedures are essential elements of an agency's FISMA-mandated information security program. FCC's Policy for Information Security and Privacy states that FCC shall implement procedures and controls at all levels to protect the confidentiality and integrity of information stored and processed on the commission's systems, and to ensure that the systems and information are available to authorized persons when required.[47]

Although FCC developed and documented commission-wide policies addressing the 18 control areas—such as access control, configuration management, security awareness training, and contingency planning—identified in NIST SP 800-53, the commission had not fully developed or documented the detailed operating procedures that are needed to effectively implement its security policies. For example, FCC had not documented detailed procedures for implementing the following NIST-specified control areas: (1) access control, (2) configuration management, (3) identification and authentication, (4) system maintenance, (5) media

---

[47]Federal Communications Commission, *FCC Policy for Information Security and Privacy*, Version 4.0 (February 26, 2016).

protection, (6) physical and environmental protection, (7) information security program management, (8) risk assessment, (9) system and services acquisition, (10) system and communication protection, and (11) system and information integrity. The lack of detailed operating procedures likely was an underlying cause for many of the technical control deficiencies we identified.

According to the FCC CISO, as of February 2019, the commission was in the process of reviewing and revising its information security policies and had issued POA&Ms to develop and document the missing procedures. Nevertheless, until FCC fully develops and documents detailed operating procedures for implementing its security policies, the commission faces increased risks that it will not effectively protect its information systems and information from cyber threats.

FCC Had Not Effectively Implemented Controls Intended to Detect Cybersecurity Events or Deficiencies

The detect core security function is intended to allow for the timely discovery of cybersecurity events and deficiencies. Controls associated with this function include logging and monitoring system activities, and assessing security controls in place. NIST SP 800-53 states that agencies should enable system logging features and retain sufficient audit logs to support the investigations of security incidents and monitoring of select activities for significant security-related events.[48] Additionally, NIST SP 800-53 and industry leading practices state that organizations should increase their situational awareness through enhanced monitoring capabilities to analyze network traffic data over an extended period of time at external boundaries and inside their internal network to identify anomalous, inappropriate, or unusual malicious activities. Lastly, FISMA requires each agency to periodically test and evaluate the effectiveness of its information security controls in place applicable to policies, procedures, and practices.

In September 2019, we reported that FCC had implemented security monitoring controls, such as performing regular vulnerability scanning and deploying a system information and event management tool, to detect the presence of potential malicious threats. However, six technical control

---

[48]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, MD: April 2013).

deficiencies in these capabilities diminished the effectiveness of the controls to detect cybersecurity events in the systems we reviewed. For example, FCC did not fully capture system log data on certain devices and had limited network monitoring visibility into portions of its data center environment.

According to Information Technology Center officials, FCC had deficiencies in logging, retention, and monitoring because the commission had not fully configured its security information and event monitoring tool to capture and monitor sufficient system log and network traffic data to adequately detect cybersecurity events. As a result, FCC may not be able to detect or investigate anomalous activities inside its network.

In addition, although the commission established a process for assessing the effectiveness of the security controls for its systems, its control tests and evaluations were not sufficiently robust. For example, the commission's evaluations did not identify many of the security control deficiencies we identified. Consequently, FCC had limited assurance that the security controls were in place and operating as intended.

As of November 2019, FCC had acted to address several technical control deficiencies, and associated recommendations, such as capturing network traffic data and providing for real-time network monitoring; however, other technical control deficiencies remain.

FCC Did Not Fully Implement Its Incident Response Controls and Remediate Deficiencies in a Timely Manner

The respond core security function is intended to support the ability to contain the impact of a potential cybersecurity event. Controls associated with this function include implementing an incident response capability and remediating newly identified deficiencies.

We reported in September 2019 that, as part of its information security program, FCC had implemented controls for incident response by developing, documenting, and annually updating its incident handling policy and procedures, along with its guidelines for remediating deficiencies.[49] However, two information security program-related deficiencies and a technical control deficiency diminished the effectiveness of the controls to respond to cybersecurity events for the

---

[49]GAO-19-247SU.

systems we reviewed. For example, the commission did not adequately address security incidents and mitigate known deficiencies in a timely manner.

FCC Had Developed and Documented an Incident Response Capability, but Did Not Report Several Incidents in a Timely Manner

NIST SP 800-53[50] and SP 800-61[51] state that agencies should develop, document, and implement incident response policy and procedures, and keep them updated according to agency requirements. FCC incident response policy also states that all employees are required to report suspected security incidents to the FCC Network Security Operations Center (NSOC) group within 1 hour of discovery or detection, and all other incidents within 24 hours of discovery. Further, FCC's incident response procedures require internal escalation and external notification to the United States Computer Emergency Readiness Team (US-CERT) within 1 hour.[52]

FCC had developed, documented, and updated its incident response policy and procedures on an annual basis to address security incidents. The commission also established a NSOC group as the single point of contact for potential security incidents.

However, FCC did not report internally to the NSOC group or externally to US-CERT in a timely manner for three of 10 security incidents we reviewed.[53] Specifically,

---

[50]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations,* Special Publication 800-53, Revision 4 (Gaithersburg, MD: April 2013).

[51]National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61, Revision 2 (Gaithersburg, Md.: August 2012).

[52]Federal Communications Commission, *Standard Operating Procedures for Incident Respo*nse, Version 7.0 (Washington, D.C.: January 2018). Within the Department of Homeland Security, US-CERT is a component of the National Cybersecurity and Communications Integration Center. It serves as the central federal information security incident center specified by FISMA.

[53]The security incidents we reviewed were the 10 that the FCC Information Technology Center officials identified as the commission's most significant since January 2017.

- A FCC employee took 2 days to report the existence of an information spillage incident to the NSOC instead of the required 1-hour reporting time frame.[54]

- The NSOC group took approximately 4 hours to report a December 2017 distributed denial-of-service attack incident and a February 2018 malicious attack incident to the US-CERT, instead of the 1 hour required for each.

According to the FCC CISO, the commission plans to review its incident response policy and procedures, as well as re-train its staff, to ensure that staff consistently follow the commission's policy and US-CERT incident notification guidelines.

Subsequent to the issuance of our September 2019 report, FCC indicated that it plans to address these matters by October 2020. Until it does so, the commission may impede its ability to receive timely assistance from appropriate federal agencies and mitigate any harm.

FCC Had Action Plans to Remedy Identified Deficiencies for Selected Systems, but Did Not Implement Them in a Timely Manner

NIST 800-53 states that agencies are to develop a POA&M for an information system to document the agencies' planned remedial actions to correct identified deficiencies. FCC's *Plan of Action and Milestone Guide* also states that the maximum completion time frames for implementing POA&M items related to critical and high severity level deficiencies[55] are 30 and 60 days, respectively.[56]

Although FCC developed a remedial action process and maintained a management system to document and track the status of POA&M items, it did not complete remedial actions in a timely manner for the three

---

[54]According to NIST, information spillage refers to instances where either classified or sensitive information is inadvertently placed on information systems that are not authorized to process such information

[55]According to FCC's *Plan of Action and Milestone Guide*, severity level deficiencies are FCC-defined information security weaknesses assigned based on risk that could be exploited by a threat source to compromise the confidentiality, integrity, or availability of its information systems, system security procedure, internal control, or other security implementation.

[56]Federal Communications Commission, *FCC Plan of Action and Milestone Guide*, Version 3.0 (Washington, D.C.: March 2018).

systems we reviewed. Specifically, FCC did not remedy critical and high severity level deficiencies within the required time frames as stated in its policy. For example,

- FCC took an average of approximately 3 months to implement four critical severity level POA&M items for one system.

- FCC took an average of more than 1 year to remediate three critical and nine high severity level POA&M items for another system. Additionally, as of October 2018, this system had seven open critical and four open high severity level POA&M items that exceeded the remediation threshold on average by 1 year, 4 months, and 5 months, respectively.

- FCC took an average of more than 3 years to implement two critical and seven high severity level POA&M items for the third system.

FCC officials attributed these delays to operational priorities and resource constraints, such as financial, personnel, and technological factors. However, such longstanding delays in remediating weaknesses pose a significant threat to the overall security posture of the commission, since the delays could allow intruders to exploit critical and high severity level deficiencies to gain access to FCC's information resources.

As of November 2019, FCC stated that it planned to address security program deficiencies related to remediating weaknesses in a timely manner by October 2020.

FCC Developed Contingency Plans, but Had Not Developed Restoration Procedures or Conducted Annual Disaster Recovery Testing

The recover core security function is intended to support timely recovery of system operations to reduce the impact from a cybersecurity event. Controls associated with this function include developing and testing contingency plans to ensure that, when unexpected events occur, critical operations can continue without interruption or can be promptly resumed, and that information resources are protected.

In September 2019, we reported that, as part of its information security program, FCC had developed contingency plans for selected systems

and established priorities for application disaster recovery.[57] However, two information security program-related deficiencies diminished the effectiveness of the controls to recover the systems we reviewed. Specifically, the commission did not

- document detailed procedures for restoring two of the three systems we reviewed and

- conduct an annual test of its disaster recovery plan for the three selected systems in fiscal year 2018.

FCC Established Contingency Plan Restoration Procedures for One System, but Had Not Fully Documented Restoration Procedures for Two Other Systems Reviewed

NIST SP 800-34 *Contingency Planning Guide for Federal Information Systems* states that an information system contingency plan should provide detailed procedures to restore the information system or components to a known state.[58] In addition, FCC's *Policy for Contingency Planning* states that system contingency plans should reflect the restoration activities required for information systems to recover after an incident.[59]

FCC developed and documented a contingency plan for one system that specified detailed procedures for restoring system operations, data, and supporting applications. However, FCC did not include detailed procedures for restoring the other two systems we reviewed in their respective contingency plans—both of which are major application systems.[60] For example, the contingency plans for these two systems did not specify procedures for restoration activities such as restoring critical operating system, application software, and system data to a known state.

---

[57]GAO-19-247SU.

[58]National Institute of Standards and Technology, *Contingency Planning Guide for Federal Information Systems*, SP 800-34, Revision 1 (Gaithersburg, Md.: May 2010).

[59]Federal Communications Commission, *FCC Policy for Contingency Planning*, Version 1.3 (Washington, D.C.: March 2018).

[60]According to FCC's *IT Disaster Recovery Plan*, a major application system is a business application that the agency uses to perform its mission essential functions.

According to Information Technology Center officials, they did not consider the two systems as supporting mission essential functions, which would necessitate the inclusion of the applications in the detailed restoration procedures.[61] However, both of the systems are major application systems and support mission essential functions at FCC.

Subsequent to our September 2019 report, FCC documented detailed restoration procedures in the two other systems' contingency plans that included activities associated with restoring critical operating system, application software, and system data to a known state. By doing so, FCC increased the likelihood that it will be able to restore operations to its mission essential functions in the event of a disaster.

FCC Had Not Tested Disaster Recovery Capabilities on an Annual Basis

NIST SP 800-84 states that a disaster recovery test should assess the ability of an agency to restore IT processing capabilities in the event of a disruption.[62] Moreover, FCC's policy for contingency planning states that all information system and facility disaster recovery plans should be tested annually to determine the effectiveness of the plan and the organizational readiness to execute the plan.[63]

In September 2019, we reported that FCC did not conduct test exercises of the disaster recovery plans for the three systems we reviewed during fiscal year 2018, nor did it test system backup, recovery, restoration, and reconstitution procedures for these systems.[64] According to FCC officials, the test exercise did not take place in fiscal year 2018 because other business operation activities took precedence over the exercise since the

---

[61]According to the Department of Homeland Security's *Federal Continuity Directive 1*, mission essential functions are directly related to accomplishing the organization's mission as set forth in statute or executive charter. Department of Homeland Security, Federal Emergency Management Agency, Federal Executive Branch National Continuity Program and Requirements, *Federal Continuity Directive 1* (Washington, DC: January 2017).

[62]National Institute of Standards and Technology, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, Special Publication 800-84 (Gaithersburg, Md.: September 2006).

[63]Federal Communications Commission, *FCC Policy for Contingency Planning*, Version 1.3 (Washington, D.C.: March 2018).

[64]GAO-19-247SU.

test exercise requires all mission-essential function applications to be unplugged.

As a result, FCC had limited assurance that it would be able to recover from unexpected disruptions in a timely and efficient manner. While it did not complete the exercise in fiscal year 2018, FCC did subsequently conduct a disaster recovery exercise at the beginning of fiscal year 2019. By doing so, FCC increased its assurance that it would be able to recover use of its systems from unexpected disruptions in a timely and efficient manner.

FCC Has Implemented Most Recommendations in Our September 2019 Report and Plans to Implement the Remainder

In our September 2019 report,[65] we made 136 recommendations to FCC to bolster its agency-wide information security program and strengthen its technical security controls. Specifically, we recommended that FCC take nine actions to improve its information security program by, among other things, authorizing systems to operate, documenting operating procedures, resolving known vulnerabilities and reporting security incidents in a timely manner, and testing disaster recovery plans. We also recommended that FCC take 127 actions to address technical control deficiencies by implementing stronger access controls, encrypting sensitive data, configuring network devices securely, strengthening firewall rules, implementing audit and monitoring controls more effectively, among other actions.
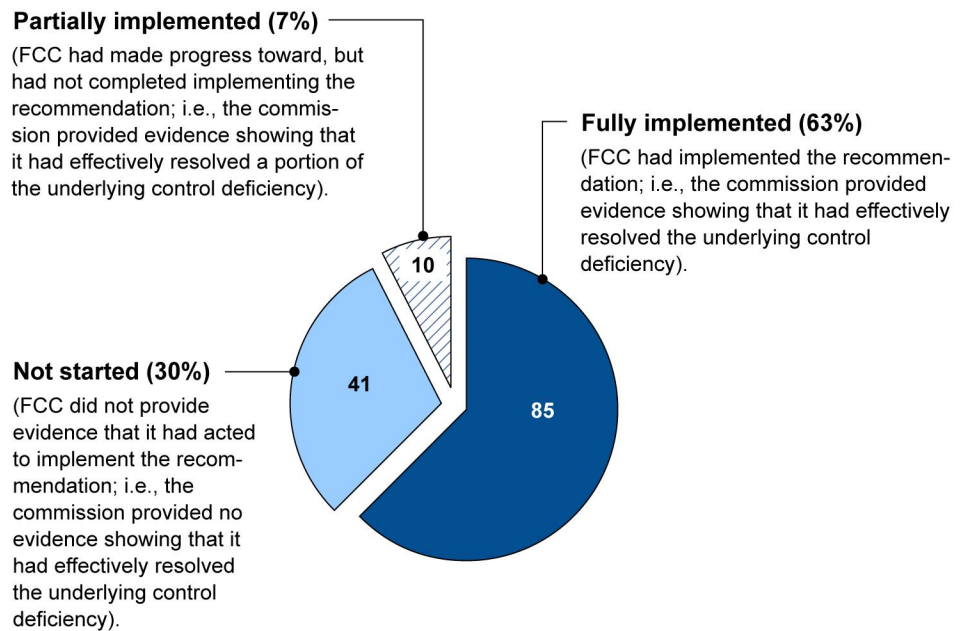
Since the issuance of our September 2019 report, FCC has made significant progress in implementing the recommendations we made to improve its information security program and resolve the technical control deficiencies in the information systems we reviewed.

Specifically, as of November 2019, FCC had implemented 85 (63 percent) of the 136 recommendations we made in the September 2019 report and had effectively resolved the underlying deficiencies associated

---

[65]GAO-19-247SU.

with the recommendations.[66] The commission also had partially, but not fully, implemented 10 recommendations. In these instances, FCC provided evidence that it had resolved a portion of the underlying control deficiency, but had not completed all of the actions necessary to fully resolve the underlying control deficiencies.[67] FCC did not provide any evidence that it had begun implementing the remaining 41 (30 percent) recommendations.[68] The status of our recommendations to FCC is illustrated in figure 4.

Figure 4: Status of Federal Communications Commission's Efforts to Implement GAO Recommendations, as of November 2019

Partially implemented (7%)
(FCC had made progress toward, but had not completed implementing the recommendation; i.e., the commission provided evidence showing that it had effectively resolved a portion of the underlying control deficiency).

Fully implemented (63%)
(FCC had implemented the recommendation; i.e., the commission provided evidence showing that it had effectively resolved the underlying control deficiency).

Not started (30%)
(FCC did not provide evidence that it had acted to implement the recommendation; i.e., the commission provided no evidence showing that it had effectively resolved the underlying control deficiency).

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

Table 2 provides additional details on the status of FCC's actions to implement our recommendations to improve its information security program and the technical controls for the systems we reviewed.

---

[66]We categorized the status of these recommendations as *fully implemented.*

[67]We categorized the status of these recommendations as *partially implemented.*

[68]We designated the status of these recommendations as *not started*.

Table 2: Status of Actions Taken by the Federal Communications Commission to Implement GAO's Information Security Program and Technical Control-Related Recommendations, as of November 2019

Category	Number of recommendations	Fully implemented	Partially implemented	Not started
Information Security Program	9	4	1	4
Technical Control	127	81	9	37
Totals	**136**	**85**	**10**	**41**

Legend:

Fully implemented (FCC had implemented the recommendation; i.e., the commission provided evidence showing that it had effectively resolved the underlying control deficiency).

Partially implemented (FCC had made progress toward, but had not completed implementing the recommendation; i.e., the commission provided evidence showing that it had effectively resolved a portion of the underlying control deficiency).

Not started (FCC did not provide evidence that it had acted to implement the recommendation; i.e., the commission provided no evidence showing that it had effectively resolved the underlying control deficiency).

Source: GAO analysis of FCC data. | GAO-20-265

By implementing 85 recommendations, FCC (as of November 2019) had reduced risks associated with certain key activities. Specifically, FCC's actions to implement four information security program-related recommendations included conducting a disaster recovery test exercise, documenting detailed system restoration procedures, and updating risk assessments to reflect the commission's current computing environment.

Regarding the technical controls, the commission had implemented 81 of our recommendations to rectify technical control-related deficiencies. For example, FCC strengthened firewall rules and access controls on its information system servers and internal networks—that we highlighted in our September 2019 report as being particularly vulnerable and requiring the commission to take immediate corrective actions.[69]

FCC also had developed a POA&M for each of the identified information security program-related and technical control deficiencies that remained open as of November 2019. The POA&M items contained required elements, such as severity levels (i.e., high, medium, and low) for identified weaknesses; identified estimated costs; designated points of contact; and established time frames for resolving those weaknesses and fully implementing the related recommendations. The commission's plans

---

[69]GAO-19-247SU.

called for it to implement the majority of the remaining information security program and technical control-related recommendations by May 1, 2020, and all recommendations by April 30, 2021, as shown in figure 5.[70]

Figure 5: The Federal Communications Commission's Planned Timeline for Implementing GAO's Remaining Information Security Program and Technical Control-Related Recommendations

Number of remaining recommendations as of date

Planned number of remaining recommendations
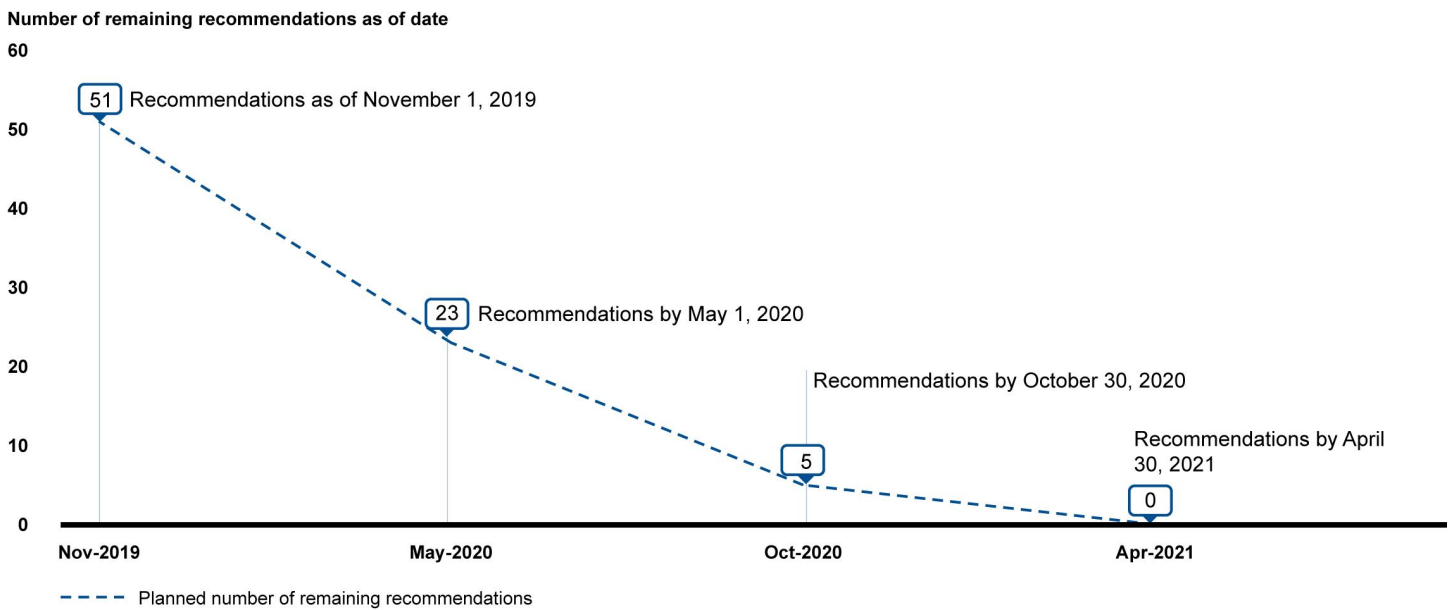
Source: GAO analysis of Federal Communications Commission data. | GAO-20-265

Fully implementing the remaining recommendations is essential to ensuring that the commission's systems and sensitive information are adequately protected from cyber threats. Key actions that remain include:

- resolving known vulnerabilities,
- documenting operational procedures,
- applying security patches and software updates, and
- enhancing network monitoring capabilities.

Until FCC fully implements all of our recommendations and resolves the associated deficiencies, its information systems and information will

---

[70]We categorized remaining recommendations as those that were either *partially implemented* or *not started*.

remain at increased risk of misuse, improper disclosure or modification, and loss.
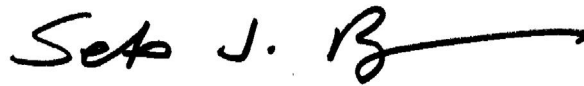
Agency Comments

We received written comments on a draft of this report from FCC. In its comments, which are reprinted in appendix IV, the commission expressed its commitment to protecting the confidentiality, integrity, and availability of its information systems. FCC noted our evaluation of its efforts to implement 85 of the 136 recommendations made in our September 2019 report and stated that it had also addressed nine additional recommendations. The commission further stated that it plans to address the remaining recommendations over the next 14 months with full mitigation anticipated by April 2021.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the appropriate congressional committees. We are sending copies of this report to the appropriate congressional committees, the Federal Communications Commission, the commission's Office of the Inspector General, and interested congressional parties. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.
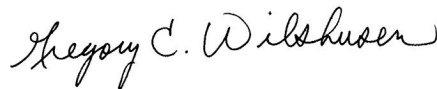
If you or your staff have any questions about this report, our primary point of contact is Vijay A. D'Souza at (202) 512-6240 or dsouzav@gao.gov. You may also contact Seto J. Bagdoyan at (202) 512-4749 or bagdoyans@gao.gov. GAO staff who made key contributions to this report are listed in appendix V.

Vijay A. D'Souza
Director
Information Technology and Cybersecurity

Seto J. Bagdoyan
Director of Audits
Forensic Audits and Investigative Service

Gregory C. Wilshusen
Director
Information Technology and Cybersecurity

List of Requesters

The Honorable Frank Pallone, Jr.
Chairman
Committee on Energy and Commerce
House of Representatives

The Honorable Carolyn B. Maloney
Chair
Committee on Oversight and Reform
House of Representatives

The Honorable Diana DeGette
Chair
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
House of Representatives

The Honorable Mike Doyle
Chairman
Subcommittee on Communications and Technology
Committee on Energy and Commerce
House of Representatives

The Honorable Gerald E. Connolly
Chairman
Subcommittee on Government Operations
Committee on Oversight and Reform
House of Representatives

The Honorable Brian Schatz
United States Senate

The Honorable Yvette D. Clarke
House of Representatives

The Honorable Debbie Dingell
House of Representatives

The Honorable Eliot L. Engel
House of Representatives

The Honorable Gregory W. Meeks
House of Representatives

The Honorable Hakeem Jeffries
House of Representatives

The Honorable Robin L. Kelly
House of Representatives

The Honorable Jerry McNerney
House of Representatives

The Honorable Paul D. Tonko
House of Representatives

The Honorable Nydia Velázquez
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine 1) the actions FCC took to respond to the May 2017 event that affected the Electronic Comment Filing System (ECFS), and 2) the extent to which FCC implemented security controls to effectively protect the confidentiality, integrity, and availability of selected systems. In September 2019, we issued a report which detailed the findings from our work in response to these two objectives.[1] In the report, we made 127 recommendations to FCC to resolve the technical security control deficiencies in the information systems we reviewed and nine additional recommendations to improve its information security program. We designated that report as "limited official use only" (LOUO) and did not release it to the general public because of the sensitive information it contained.

This report publishes the findings discussed in our September 2019 report, but we have removed all references to the sensitive information. Specifically, we deleted the names of the information system software, network devices, and resource tools that we examined, disassociated identified control deficiencies from named systems, deleted certain details about information security controls and control deficiencies, and omitted an appendix that was contained in the LOUO report. The appendix contained sensitive details about the technical security control deficiencies in the FCC's information systems and computer networks that we reviewed, and the 127 recommendations we made to mitigate those deficiencies. We also provided a draft of this report to FCC officials to review and comment on the sensitivity of the information contained herein and to affirm that the report can be made available to the public without jeopardizing the security of the commission's information systems and networks.

In addition, this report addresses a third objective that was not included in the September 2019 report.[2] Specifically, this objective was to determine

---

[1]GAO, *Information Security: FCC Improved Its Electronic Comment System, but Needs to Remedy Additional Control Weaknesses*, GAO-19-247SU (Washington, D.C.: September 12, 2019).

[2]GAO-19-247SU.

the extent to which FCC had taken corrective actions to address the previously identified security program and technical control deficiencies and related recommendations for improvement that we identified in the earlier report.

To address the first objective, we reviewed FCC's security and incident response policies and procedures, examined related reports prepared by the commission and its Office of Inspector General, reviewed an internal assessment of the May 2017 event that was performed by the FCC Information Technology Center, and reviewed artifacts associated with system enhancement and performance such as change requests and email. We also extracted comment submission data derived from the data.gov application programming interface between May 1, 2017 and December 31, 2017 to identify the peak periods of increased comment submissions during and after the May 2017 event.

In addition, we examined the aforementioned documents to assess whether the updated incident response policy and procedures, along with system enhancement and performance artifacts, were directly related to changes made subsequent to the May 2017 event. Lastly, we interviewed FCC Information Technology Center officials, including system and security staff, and Office of Inspector General officials to identify FCC's actions to respond to the May 2017 event.

To address the second objective, we reviewed FCC's overall network environment, identified interconnectivity and control points, and examined controls for the commission's networks and facilities. We performed this work at FCC facilities located in West Virginia, Pennsylvania, and Washington, D.C.

As noted in our September 2019 report, we determined the extent to which FCC had implemented security controls to effectively protect the confidentiality, integrity, and availability of selected systems.[3] To do so, we selected three of the commission's information systems for review. We selected these systems because they (1) are essential to FCC's mission and (2) were assigned a Federal Information Processing Standards Publication 199 rating of moderate or high impact. The results of our review of these systems is not generalizable to the commission's other systems.

---

[3]GAO-19-247SU.

To evaluate FCC's controls for its information systems, we used GAO's
Federal Information System Controls Audit Manual, which contains
guidance for reviewing information system controls that affect the
confidentiality, integrity, and availability of computerized information.[4] We
based our assessment of controls on requirements of the *Federal
Information Security Modernization Act of 2014* (FISMA),[5] which
establishes key elements for an effective agency-wide information
security program; National Institute of Standards and Technology (NIST)
guidelines and standards;[6] FCC policies and procedures; and standards
and guidelines from relevant security organizations, such as the National
Security Agency, and the Center for Internet Security.[7]

For reporting purposes, we categorized the security controls that we
assessed into the five core security functions described in the NIST
cybersecurity framework.[8] The five core security functions are:

---

[4]GAO, *Federal Information System Controls Audit Manual* (FISCAM), GAO-09-232G
(Washington, D.C.: February 2009).

[5]*The Federal Information Security Modernization Act of 2014* (FISMA) (Pub. L. No. 113-
283, Dec. 18, 2014) largely superseded the *Federal Information Security Management Act
of 2002* (FISMA 2002), enacted as Title III, *E-Government Act of 2002*, Pub. L. No. 107-
347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to
FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into
FISMA 2014 or were unchanged and continue in full force and effect.

[6]For example, see National Institute of Standards and Technology, *Minimum Security
Requirements for Federal Information and Information Systems*, Federal Information
Processing Standards Publication 200 (Gaithersburg, MD: March 2006), and National
Institute of Standards and Technology, *Security and Privacy Controls for Federal
Information Systems and Organizations*, Special Publication 800-53, Revision 4
(Gaithersburg, MD: April 2013).

[7]The Center for Internet Security is a nonprofit entity that uses a global information
technology community to safeguard private and public organizations against cyber threats.
We used the Center for Internet Security benchmark criteria to assess FCC's information
systems. These benchmark criteria are included in NIST's National Checklist Program
repository which contains publicly available security guidelines that agencies can use as
detailed low-level guidance on setting the security configuration of operating systems and
applications.

[8]National Institute of Standards and Technology, *Framework for Improving Critical
Infrastructure Cybersecurity* (Gaithersburg, MD: Feb. 12, 2014). The framework was
developed in response to an executive order issued by the prior administration, *Improving
Critical Infrastructure Cybersecurity*, Executive Order 13636 (Washington, D.C.: Feb. 12,
2013). It was originally intended for use in protection of critical infrastructure. The
framework has since been updated in April 2018. National Institute of Standards and
Technology, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*
(Gaithersburg, MD: Apr. 16, 2018).

- Identify: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

- Protect: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

- Detect: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

- Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

- Recover: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

These core security functions are described in more detail in appendix II.

For each of the five core security functions, we examined selected FCC security controls and related documentation:

- For the identify core security function, we examined FCC's reporting for its hardware and software assets; analyzed risk assessments for the three selected systems to determine whether threats and vulnerabilities were being identified; analyzed FCC policies and procedures to determine their effectiveness in providing guidance to personnel responsible for securing information and information systems; and analyzed security plans for the three selected systems to determine if those plans had been documented and updated according to federal guidance.

- For the protect core security function, we examined access controls for the three systems. These controls included the password complexity and settings to determine if password management was being enforced; administrative users' system access permissions to determine whether their authorizations exceeded the access necessary to perform their assigned duties; and firewall configurations, among other things, to determine whether system boundaries had been adequately protected. We also examined configurations for providing secure data transmissions across the network to determine whether sensitive data were being encrypted. In addition, we examined configuration settings for routers, network management servers, switches, and firewalls to determine if settings adhered to configuration standards, and we inspected key servers and network devices to determine if critical patches had been installed and/or were up to date.

- For the detect core security function, we analyzed security control assessments, and centralized logging and network traffic monitoring capabilities for key assets connected to the network.

- For the respond core security function, we reviewed FCC's implementation of incident response practices, including an examination of incident tickets for 10 incidents the commission considered most significant from January 1, 2017 to May 29, 2018; and examined the commission's process for correcting identified deficiencies for the three selected systems.

- For the recover core security function, we examined contingency and disaster recovery plans for the three selected systems to determine whether those plans had been developed and tested.

For the core security functions, as appropriate, we evaluated elements of FCC's information security program. For example, we analyzed risk assessments, security plans, remedial action plans, and contingency plans for each of the three selected systems. We also evaluated FCC's security policies and procedures. In assessing FCC's controls associated with these core functions, we interviewed FCC's Information Technology Center personnel, chief information officer, chief information security officer, general counsel, inspector general, and Public Safety and Homeland Security Bureau officials, as needed.

To determine the reliability of FCC's computer-processed data for incident response records, we evaluated the materiality of the data to our audit objective and assessed the data by various means, including reviewing related documents, interviewing knowledgeable FCC officials, and reviewing internal controls. Through a combination of these methods, we concluded that the data were sufficiently reliable for the purposes of our work.

To accomplish our third objective—on FCC's actions to address the previously identified security program and technical control deficiencies and related recommendations—we requested that the commission provide a status report of its actions to implement each of the recommendations.[9] For each recommendation that FCC indicated it had implemented as of November 2019, we examined supporting documents, observed or tested the associated security control or procedure, and/or interviewed the responsible agency officials to assess the effectiveness of the actions taken to implement the recommendation or otherwise resolve

---

[9]GAO-19-247SU.

the underlying control deficiency. Based on this assessment and FCC
status reports, we defined the status of each recommendation according
to three categories:

- fully implemented—FCC had implemented the recommendation (i.e.,
  the commission provided evidence showing that it had effectively
  resolved the underlying control deficiency);

- partially implemented—FCC had made progress toward, but had not
  completed implementing the recommendation (i.e., the commission
  provided evidence showing that it had effectively resolved a portion of
  the underlying control deficiency); and

- not started—FCC did not provide evidence that it had acted to
  implement the recommendation (i.e., the commission provided no
  evidence showing that it had effectively resolved the underlying
  control deficiency).

We conducted the performance audit for the first two objectives from
February 2018 through September 2019 in accordance with generally
accepted government auditing standards. We conducted work supporting
the third objective and, where applicable, included updates to our work in
the second objective, from October 2019 through March 2020 in
accordance with generally accepted government auditing standards.
Those standards require that we plan and perform the audit to obtain
sufficient, appropriate evidence to provide a reasonable basis for our
findings and conclusions based on our audit objectives. We believe that
the evidence obtained provides a reasonable basis for our findings.

Appendix II: National Institute of Standards and Technology's Cybersecurity Framework

The National Institute of Standards and Technology's cybersecurity framework consists of five core functions: identify, protect, detect, respond, and recover.[1] Within the five functions are 23 categories and 108 subcategories of security-related controls (see table 3).

Table 3: National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity

Category	Subcategory
Identify (ID) Function	
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried.
	ID.AM-2: Software platforms and applications within the organization are inventoried.
	ID.AM-3: Organizational communication and data flows are mapped.
	ID.AM-4: External information systems are catalogued.
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, and partners) are established.
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1: The organization's role in the supply chain is identified and communicated.
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated.
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated.

[1]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1 (Gaithersburg, MD: Apr. 16, 2018). The framework was developed in response to an executive order issued by the prior administration, Executive Order 13636 (Washington, D.C.: Feb. 12, 2013). It was originally intended for use in protection of critical infrastructure.

	ID.BE-4: Dependencies and critical functions for delivery of critical services are established.
	ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations).
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational cybersecurity policy is established and communicated.
	ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
	ID.GV-4: Governance and risk management processes address cybersecurity risks.
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented.
	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources.
	ID.RA-3: Threats, both internal and external, are identified and documented.
	ID.RA-4: Potential business impacts and likelihoods are identified.
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
	ID.RA-6: Risk responses are identified and prioritized.
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed.
	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.
Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.
	ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.
	ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.

Protect (PR) Function

Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
	PR.AC-2: Physical access to assets is managed and protected.
	PR.AC-3: Remote access is managed.
	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).
	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.
	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained.
	PR.AT-2: Privileged users understand roles and responsibilities.
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, and partners) understand roles and responsibilities.
	PR.AT-4: Senior executives understand roles and responsibilities.
	PR.AT-5: Physical and cybersecurity personnel understand roles and responsibilities.
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected.
	PR.DS-2: Data-in-transit is protected.
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.
	PR.DS-4: Adequate capacity to ensure availability is maintained.
	PR.DS-5: Protections against data leaks are implemented.
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.
	PR.DS-7: The development and testing environment(s) are separate from the production environment.
	PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality).
	PR.IP-2: A System Development Life Cycle to manage systems is implemented.
	PR.IP-3: Configuration change control processes are in place.
	PR.IP-4: Backups of information are conducted, maintained, and tested.
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.
	PR.IP-6: Data destroyed according to policy.
	PR.IP-7: Protection processes are improved.

	PR.IP-8: Effectiveness of protection technologies is shared.
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
	PR.IP-10: Response and recovery plans are tested.
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).
	PR.IP-12: A vulnerability management plan is developed and implemented.
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets performed and logged, with approved and controlled tools.
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
	PR.PT-2: Removable media is protected and its use restricted according to policy.
	PR.PT-3: The principle of least functionality is incorporating by configuring systems to provide only essential capabilities.
	PR.PT-4: Communications and control networks are protected.
	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.
Detect (DE) Function	
Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.
	DE.AE-2: Detected events are analyzed to understand attack targets and methods.
	DE.AE-3: Event data are collected and correlated from multiple sources and sensors.
	DE.AE-4: Impact of events is determined.
	DE.AE-5: Incident alert thresholds are established.
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events.
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.
	DE.CM-4: Malicious code is detected.
	DE.CM-5: Unauthorized mobile code is detected.
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.
	DE.CM-8: Vulnerability scans are performed.

Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability.
	DE.DP-2: Detection activities comply with all applicable requirements.
	DE.DP-3: Detection processes are tested.
	DE.DP-4: Event detection information is communicated to parties.
	DE.DP-5: Detection processes are continuously improved.

Respond (RS) Function

Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	RS.RP-1: Response plan is executed during or after an incident.
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-1: Personnel know their roles and order of operations when a response is needed.
	RS.CO-2: Events are reported consistent with established criteria.
	RS.CO-3: Information is shared consistent with response plans.
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans.
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.
Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated.
	RS.AN-2: The impact of the incident is understood.
	RS.AN-3: Forensics are performed.
	RS.AN-4: Incidents are categorized consistent with response plans.
	RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers).
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-1: Incidents are contained.
	RS.MI-2: Incidents are mitigated.
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned.
	RS.IM-2: Response strategies are updated.

Recover (RC) Function

Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident.
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned.
	RC.IM-2: Recovery strategies are updated.
	RC.CO-1: Public relations are managed.
	RC.CO-2: Reputation is repaired after an event.

Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, internet service providers, owners of attacking systems, victims, other CSIRTs, and vendors.	RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.

Source: National Institute of Standards and Technology. | GAO-20-265.

Appendix III: Timeline of May 2017 Event Involving the FCC Electronic Comment Filing System

Below is a timeline of the Federal Communications Commission's (FCC) May 2017 Electronic Comment Filing System (ECFS) event and subsequent related events:

- On April 27, 2017, FCC issued the Restoring Internet Freedom Notice of Proposed Rulemaking in the *Federal Register*. The notice directed interested parties to submit comments via FCC's ECFS.

- On the evening of May 7, 2017, a late night talk show aired a segment on the Restoring Internet Freedom notice and encouraged viewers to submit comments via ECFS.

- On the evening of May 7, 2017, according to a report by the FCC Office of Inspector General (IG), ECFS experienced a significant increase in the level of comment traffic attempting to access the system, resulting in the disruption of system availability. A contractor providing web performance and cloud security solutions to FCC identified a 3,116 percent increase in traffic to ECFS between May 7 and May 8, 2017.

- In the early morning of May 8, 2017, ECFS became unavailable to commenters. FCC's vendor sent automated alerts indicating a spike in network traffic, in addition to preliminary network statistical data, to FCC.

- During the mid-morning of May 8, 2017, FCC's Information Technology Center responded to the alerts from the vendor and initiated stabilization efforts to ECFS.

- During the afternoon of May 8, 2017, FCC issued a press release in which FCC's chief information officer (CIO) at that time provided a statement about the cause of delays experienced by commenters trying to file comments on the ECFS. The CIO's statement said that

FCC was subjected to multiple distributed denial-of-service attacks.[1] He further stated that, "these were deliberate attempts by external actors to bombard the FCC's comment system with a high amount of traffic."

- During May 9-10, 2017, FCC restored ECFS but still experienced response-time problems relating to system performance.

- On May 10, 2017, FCC's Information Technology Center responded to inquiries from the Federal Bureau of Investigations and FCC OIG via email and phone.

- On June 21, 2017, the FCC OIG opened a full investigation into the event because of, according to the OIG, the importance of FCC's cybersecurity posture and the possibility that cybercrimes had been committed that had the potential of being ongoing threats to the integrity of FCC's computer systems.

- On January 4, 2018, FCC OIG referred the investigation to the Justice Department.

On August 7, 2018, the FCC OIG published an investigative report on the ECFS event. According to the OIG report, the allegations of multiple distributed denial-of-service attacks alleged by the FCC CIO at that time were not substantiated.[2] The FCC OIG concluded that the spikes in web traffic to ECFS had coincided exactly with the timing of the late night television show where the host discussed the FCC's Restoring Internet Freedom proceeding and encouraged viewers to visit the commission's website and file comments. The FCC OIG's report also indicated that the commission did not define the event (i.e., any observable occurrence in a network or system) as a cybersecurity incident (i.e., an imminent threat or violation of computer security policies, or security practices). Therefore, according to the OIG report, FCC did not take actions to:

---

[1]A denial-of-service attack is a cyberattack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. In a distributed denial-of-service attack (DDoS), multiple machines are operating together to attack one target. DDoS allows for exponentially more requests to be sent to the target, thereby increasing the difficulty of identifying the culprit and the magnitude of harm.

[2]Federal Communications Commission, *Office of Inspector General, Memo: Alleged Multiple Distributed Denial-Of-Service (DDoS) Attacks involving the FCC's Electronic Comment Filing System (ECFS)*, (Washington, D.C.: June 20, 2018).

- refer the matter to the United States Computer Emergency Readiness Team (US-CERT) in accordance with federal policy,

- implement internal incident handling procedures in accordance with its incident handling policy, or

- conduct a thorough analysis before or after the event to determine if it was an incident.

On August 16, 2018, the FCC Chairman testified at a Senate Committee on Commerce, Science and Transportation oversight hearing on the conclusions of the FCC OIG investigative report on the ECFS event.

Appendix IV: Comments from the Federal Communications Commission

Federal Communications Commission
Washington, D.C. 20554

March 11, 2020

Mr. Gregory Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548
Email: WilshusenG@gao.gov

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report entitled, *Information Security: FCC Made Significant Progress, but Needs to Address Remaining Control Deficiencies and Improve Its Program* (GAO-20-265) (hereinafter *Draft Report*). The Federal Communications Commission (FCC) is committed to protecting the confidentiality, integrity, and availability of our information systems. We appreciate your team's careful analysis of our information technology (IT) environment and your recommendations about how we can better protect our resources.

As noted in our comment letter to the September 2019 non-public version of this report, the FCC has been engaged in a major, multi-year strategic effort to modernize our IT capabilities and deliver secure, scalable, and reliable systems for both our internal operations and our public-facing systems. A key part of this initiative is moving our systems and applications from outdated legacy technologies and aging physical infrastructure to more efficient computing platforms and technologies—in particular, to cloud computing. We recognize the "unique opportunity" cloud technology provides federal agencies "to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services provided to its citizens."[1] Seizing this opportunity, we have adopted a "Cloud Smart"[2] approach to our IT resources and have already moved a number of our legacy systems (including the Electronic Comment Filing System (ECFS)) to cloud environments, and will continue this process over the next several years. Your report's description of how the FCC was able to quickly deploy additional virtual hardware and optimize system software to manage the high volumes of public comments ECFS received during the summer of 2017 is a good example of the operational advantages of cloud hosting.[3]

As the FCC's IT staff explained to your staff during your inquiry, moving our IT infrastructure and applications to a cloud-based architecture has changed our approach to information security. We work with Federal Risk and Authorization Management Program (FedRAMP) certified cloud service providers (CSPs) as our information security partners. While

---

[1] OMB Memorandum for Chief Information Officers, "Security Authorization of Information Systems in Cloud Computing Environments," (Dec. 8, 2011).
[2] *See e.g.*, Federal Chief Information Officers Council, "From Cloud First to Cloud Smart," available at https://cloud.cio.gov/strategy/.
[3] *Draft Report* at 17.

the FCC remains ultimately responsible for the security of its systems, we can rely on and inherit, with a high degree of confidence, the FedRAMP CSP baseline of security controls necessary to effectively protect the confidentiality, integrity, and availability of our systems. The ability to incorporate these controls into our security strategy is a critical part of the value proposition that FedRAMP CSPs provide federal agencies—particularly small federal agencies with limited security resources like the FCC. The FCC and many other federal agencies are using this FedRAMP model to deliver services to their users that are both more efficient and secure. We think an accurate assessment of how we manage risk in our IT security environment should consider how our expanding use of FedRAMP-approved services has improved our overall security posture. Nevertheless, as noted in your report, we developed a plan of action and milestones (POA&M) regarding service-level agreements with CSPs that we plan to implement by May 2020. [4]

We acknowledge the nine non-technical and 127 technical recommendations in this draft report. We have been working diligently to address them, prioritizing those recommendations that are most operationally practical to implement and those that will immediately improve our security. By November 2019, after release of the non-public report, we received your concurrence that we had mitigated 85 of the recommendations made in the *Draft Report*. We provided additional evidence related to nine recommendations and now believe we have addressed 94 of the 136 recommendations in the *Draft Report*. As discussed with your staff, we will be providing additional evidence that we have corrected the remaining weaknesses you identify in the draft report on a rolling basis until all findings are remediated. We appreciate your commitment to review the forthcoming evidence and provide feedback to us about it in a timely manner.

We plan to address the remaining number of open recommendations over the next 14 months with full implementation anticipated by April 2021. We developed this remediation time frame after considering our current resources, enterprise architecture, and communications needs. Some of the outstanding findings will be addressed in the course of system modernization and cloud transition efforts that we have already initiated. For example, the FCC is currently in the process of upgrading both ECFS and another system GAO reviewed in its study. The new versions of these applications will not have the security deficiencies that you have identified in their current versions.

Thank you again for the opportunity to respond to this draft report. Please do not hesitate to contact me if you have questions about this response.

Sincerely,

Mark Stephens
Managing Director

---

[4] *Draft Report* at 25.

Text of Appendix IV: Comments from the Federal Communications Commission

Page 1

Federal Communications Commission
Washington, D.C. 20554

March 11, 2020

Mr. Gregory Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548
Email: WilshusenG@gao.gov

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report entitled, Information Security: FCC Made Significant Progress, but Needs to Address Remaining Control Deficiencies and Improve Its Program (GAO-20-265) (hereinafter Draft Report). The Federal Communications Commission (FCC) is committed to protecting the confidentiality, integrity, and availability of our information systems. We appreciate your team's careful analysis of our information technology (IT) environment and your recommendations about how we can better protect our resources.

As noted in our comment letter to the September 2019 non-public version of this report, the FCC has been engaged in a major, multi-year strategic effort to modernize our IT capabilities and deliver secure, scalable, and reliable systems for both our internal operations and our public- facing systems. A key part of this initiative is moving our systems and applications from outdated legacy technologies and aging physical infrastructure to more efficient computing platforms and technologies—in particular, to cloud computing. We recognize the "unique opportunity" cloud technology provides federal agencies "to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services provided to its citizens."1 Seizing this opportunity, we have adopted a "Cloud Smart"2 approach to our IT resources and have already moved a number of our legacy systems

(including the Electronic Comment Filing System (ECFS)) to cloud environments, and will continue this process over the next several years. Your report's description of how the FCC was able to quickly deploy additional virtual hardware and optimize system software to manage the high volumes of public comments ECFS received during the summer of 2017 is a good example of the operational advantages of cloud hosting.3

As the FCC's IT staff explained to your staff during your inquiry, moving our IT infrastructure and applications to a cloud-based architecture has changed our approach to information security. We work with Federal Risk and Authorization Management Program (FedRAMP) certified cloud service providers (CSPs) as our information security partners. While

Footnotes:

1 OMB Memorandum for Chief Information Officers, "Security Authorization of Information Systems in Cloud Computing Environments," (Dec. 8, 2011).

2 See e.g., Federal Chief Information Officers Council, "From Cloud First to Cloud Smart," available at https://cloud.cio.gov/strategy/.

Page 2

the FCC remains ultimately responsible for the security of its systems, we can rely on and inherit, with a high degree of confidence, the FedRAMP CSP baseline of security controls necessary to effectively protect the confidentiality, integrity, and availability of our systems. The ability to incorporate these controls into our security strategy is a critical part of the value proposition that FedRAMP CSPs provide federal agencies—particularly small federal agencies with limited security resources like the FCC. The FCC and many other federal agencies are using this FedRAMP model to deliver services to their users that are both more efficient and secure. We think an accurate assessment of how we manage risk in our IT security environment should consider how our expanding use of FedRAMP-approved services has improved our overall security posture. Nevertheless, as noted in your report, we developed a plan of action and milestones (POA&M) regarding service-level agreements with CSPs that we plan to implement by May 2020. 4

We acknowledge the nine non-technical and 127 technical recommendations in this draft report. We have been working diligently to address them, prioritizing those recommendations that are most

operationally practical to implement and those that will immediately improve our security. By November 2019, after release of the non-public report, we received your concurrence that we had mitigated 85 of the recommendations made in the Draft Report. We provided additional evidence related to nine recommendations and now believe we have addressed 94 of the 136 recommendations in the Draft Report. As discussed with your staff, we will be providing additional evidence that we have corrected the remaining weaknesses you identify in the draft report on a rolling basis until all findings are remediated. We appreciate your commitment to review the forthcoming evidence and provide feedback to us about it in a timely manner.

We plan to address the remaining number of open recommendations over the next 14 months with full implementation anticipated by April 2021. We developed this remediation time frame after considering our current resources, enterprise architecture, and communications needs. Some of the outstanding findings will be addressed in the course of system modernization and cloud transition efforts that we have already initiated. For example, the FCC is currently in the process of upgrading both ECFS and another system GAO reviewed in its study. The new versions of these applications will not have the security deficiencies that you have identified in their current versions.

Thank you again for the opportunity to respond to this draft report. Please do not hesitate to contact me if you have questions about this response.

Sincerely,

Mark Stephens Managing Director

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

Vijay A. D'Souza, (202) 512-6240, dsouzav@gao.gov
Seto J. Bagdoyan, (202) 512-4749, bagdoyans@gao.gov
Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Gary Austin, David Bruno, Tammi Kalugdan, Duc Ngo, and Christopher Warweg (assistant directors); David Hong (analyst-in-charge); Breanne Cave; Chris Businsky, Jr.; Saar Dagani; Marshall Williams, Jr.; Corey Evans; Andrew Howard; Elizabeth Kowalewski; Priscilla Smith; Henry Sutanto; and April Yeaney made significant contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548