United States Government Accountability Office

Report to the Chairman, Committee on the Budget, U.S. Senate

September 2020

TELECOMMUNICATIONS

FCC Should Take Action to Better Manage Persistent Fraud Risks in the Schools and Libraries Program

GAO Highlights

Highlights of GAO-20-606, a report to Chairman of the Committee on the Budget, U.S. Senate

Why GAO Did This Study

In 2017, the FCC's Office of Inspector General (OIG) reported that FCC's ability to deter and detect alleged E-rate program fraud has been severely limited since the program's inception due to a lack of certain controls. Also, as recently as February 2020, a number of E-rate program participants pled guilty to defrauding the program by billing for equipment and services that were not provided, and obtaining more than $2.6 million in program funds to which they were not entitled.

GAO was asked to review fraud risk management in the E-rate program. This report addresses: (1) the E-rate program's key fraud risks; (2) the extent to which FCC and USAC are managing fraud risks in accordance with leading practices; and (3) the extent to which FCC and USAC face challenges in effectively employing data analytics to support fraud risk management activities. GAO reviewed cases of fraud, OIG reports, and risk assessments, among other things. GAO assessed FCC's and USAC's procedures against leading practices in the Fraud Risk Framework. GAO interviewed FCC and USAC officials responsible for the E-rate program and fraud risk management.

What GAO Recommends

GAO makes three recommendations, including that FCC and USAC comprehensively assess fraud risks to the E-rate program and follow leading practices when designing and implementing data analytics to prevent and detect fraud. FCC agreed with the recommendations and outlined actions to address them.

View GAO-20-606. For more information, contact Seto J. Bagdoyan at (202) 512-6722 or bagdoyans@gao.gov.

September 2020

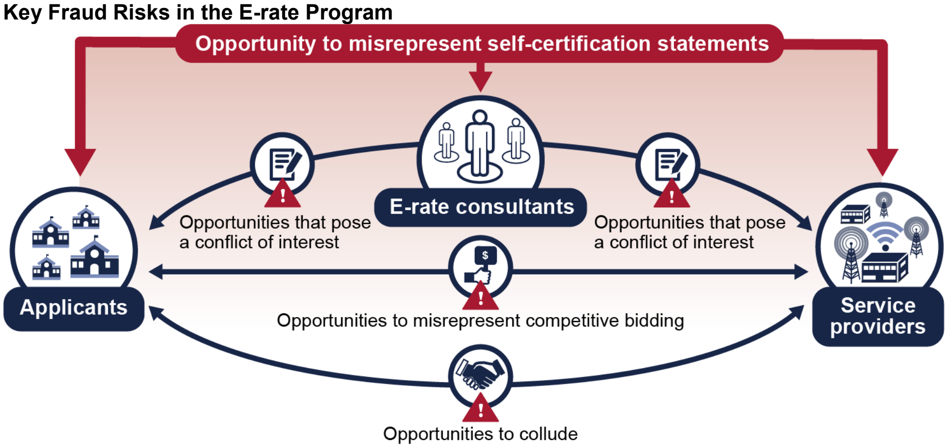
TELECOMMUNICATIONS

FCC Should Take Action to Better Manage Persistent Fraud Risks in the Schools and Libraries Program

What GAO Found

Since 1998, the Federal Communications Commission's (FCC) E-rate program has been a significant source of technology funding for schools and libraries (applicants) to obtain affordable broadband and telecommunications services. Other program participants include service providers and E-rate consultants that assist applicants and service providers with the application and funding processes. GAO identified several key fraud risks affecting the E-rate program, as shown below, including a reliance on self-certification statements. This inherent overarching key fraud risk presents opportunities for participants to misrepresent dozens of self-certification statements on various FCC forms.

Key Fraud Risks in the E-rate Program


Opportunity to misrepresent self-certification statements
E-rate consultants
Opportunities that pose a conflict of interest
Opportunities that pose a conflict of interest
Applicants
Service providers
Opportunities to misrepresent competitive bidding
Opportunities to collude

Source: GAO analysis of court documents. | GAO-20-606

FCC and the Universal Service Administrative Company (USAC) that administers the E-rate program have not yet implemented plans to comprehensively assess fraud risks, as called for in GAO's Fraud Risk Framework. Leading practices include tailoring fraud risk assessments to the program and examining the suitability of existing controls. FCC and USAC have established time frames for comprehensively assessing the E-rate program's fraud risks by the end of 2021. However, past fraud risk management initiatives have been delayed. Ensuring that such an assessment is completed as scheduled could help ensure FCC and USAC are prioritizing key fraud risks that persist in the E-rate program, and provide greater assurance that control activities are efficiently and effectively addressing the most significant fraud risks.

FCC and USAC face challenges in effectively employing data analytics to support future fraud risk management activities. For example, officials said that they are or will be using data analytics for fraud risk management, but have not implemented leading practices for data-analytics activities nor documented their efforts or plans for doing so. GAO's Fraud Risk Framework calls for agencies to design and implement control activities, including data-analytics activities, to prevent and detect fraud. Having FCC and USAC implement leading practices for data analytics and document how data-analytics activities will be used in antifraud strategies could position the agency to better prevent, detect, and respond to fraud in the E-rate program.

Contents

Figures

Abbreviations

EPC	E-rate Productivity Center
ESA	Educational Service Agency
FCC	Federal Communications Commission
Fraud Risk Framework	*A Framework for Managing Fraud Risks in Federal Programs*
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Program Integrity Assurance
USAC	Universal Service Administrative Company
USF	Universal Service Fund

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

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

September 16, 2020

The Honorable Michael B. Enzi
Chairman
Committee on the Budget
United States Senate

Dear Mr. Chairman:

Since 1998, the Federal Communications Commission's (FCC) schools and libraries universal service support mechanism—commonly known as the "E-rate" program—has been a significant federal source of technology funding for K-12 schools and libraries across the nation to obtain affordable broadband and telecommunications services. Specifically, in funding year 2019, the E-rate program received more than 35,000 applications and committed (i.e., authorized) approximately $2.4 billion to roughly 99,000 eligible schools and 11,000 libraries, according to officials.[1] Schools and libraries apply each year for E-rate program funding to the Universal Service Administrative Company (USAC)—which is the not-for-profit company that FCC designated to administer the program and which is supported by the Universal Service Fund (USF).[2]

[1] The funding year for the E-rate program runs from July 1 to June 30 of the following calendar year. For funding year 2019, FCC set a funding cap of $4.2 billion, which is the maximum amount available for the E-rate program. Also, according to FCC officials, generally, only those schools and libraries (and consortia made up of eligible schools and libraries) that meet statutory definitions of an elementary or secondary school or a library may receive funding.

[2] USAC is the administrator for the four programs that receive financial support from the USF, including the E-rate program. The USF is funded through mandated payments by companies that provide interstate and international telecommunications services. The other three programs are: (1) the high-cost program, which assists telecommunications carriers serving high-cost, rural, or insular areas; (2) the Lifeline program, which provides discounted telephone and internet service to low-income consumers; and (3) the Rural Health Care Program, which provides support to eligible health-care providers through discounts for broadband and telecommunications services. On the basis of funding approved for disbursement in 2019, the high-cost program is the largest USF program and E-rate is the second largest program.

Once an application and invoice are approved, the program reimburses a portion of the cost of the eligible services or equipment.[3]

FCC has reported the E-rate program as susceptible to significant improper payments. Specifically, FCC-reported estimated improper payments increased from approximately $85 million to approximately $140 million total from fiscal years 2014 through 2019. Improper payments could suggest that a program may also be vulnerable to fraud, although it is important to note that fraud is one specific type of improper payment and that improper payment estimates are not intended to measure fraud in a particular program.[4] One of the most common root causes of these improper payments identified by FCC was lack of sufficient documentation to demonstrate program compliance. In this regard, when payments lack the appropriate supporting documentation, their validity cannot be determined and potentially fraudulent activities could be concealed.

In 2010, we found that USAC's efforts to assess risk were related to financial-reporting purposes, not to assess risk specifically in the E-rate program and recommended that FCC conduct a robust risk assessment of the E-rate program.[5] In response, in 2015, a USAC contractor completed a risk assessment of the E-rate program, which included an

[3] Throughout this report, we refer to schools and libraries that apply to the program as "applicants," whether or not they eventually receive any funding from the program. Also, according to FCC officials, eligible services include, but are not limited to, telecommunications services and internet access.

[4] An improper payment is defined as any payment that should not have been made or that was made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements. For the purpose of producing an improper payment estimate, when the executive agency cannot determine, due to lacking or insufficient documentation, whether a payment is proper or not, the payment shall be treated as an improper payment. In particular, improper payments can be attributed to financial fraud or financial fraud risks that include instances in which beneficiaries intentionally provide misinformation to obtain illegal payments for ineligible recipients; ineligible goods or services; or for goods or services not received. While improper payments may be caused by unintentional error, fraud involves obtaining something of value through willful misrepresentation. Whether an act is fraudulent is determined through the judicial or other adjudicative system. In this report, we use the term "fraud risk" to include existing circumstances that provide an opportunity to commit fraud.

[5] GAO, *Telecommunications: FCC Should Assess the Design of the E-rate Program's Internal Control Structure*, GAO-10-908 (Washington, D.C.: Sept. 29, 2010).

assessment of all risks, including fraud risks.[6] As of June 2020, USAC has not implemented its contractor's recommendation that an external entity conduct a fraud risk assessment to provide USAC and FCC with an independent, comprehensive assessment of fraud vulnerabilities to the E-rate program.

In 2017, the FCC Office of Inspector General (OIG) reported to Congress that FCC's ability to deter and detect alleged E-rate program fraud during the competitive-bidding process has been severely limited since the program's inception in 1998 due to a lack of certain upfront controls.[7] Also, as recently as February 2020, a group of seven individuals working for schools, service providers, and E-rate program consulting firms pled guilty to defrauding the E-rate program by billing for equipment and services that were not provided, and obtaining more than $2.6 million in program funds to which they were not entitled.

You asked us to review fraud risk management in the E-rate program. This report addresses:

- the key fraud risks identified in the E-rate program;[8]

[6] Fraud and "fraud risk" are distinct concepts. Fraud relates to obtaining something of value through willful misrepresentation. Fraud risk exists when individuals have an opportunity to engage in fraudulent activity. Fraud risk factors are highlighted in federal internal control standards. See GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014). In particular, principle 8 requires federal managers to consider the potential for fraud when identifying, analyzing, and responding to risks; this can include considering types of fraud risk factors to agency programs which can provide, among others, opportunities, such as circumstances that exist, such as the absence of controls, ineffective controls, or the ability of management to override controls, that provide an opportunity to commit fraud. Also, according to GAO's Fraud Risk Framework, a "fraud risk factor" describes what conditions or actions are most likely to cause or increase the chances of a fraud risk occurring. See GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015). Although the existence of fraud risk factors does not necessarily indicate that fraud exists or will occur, they are often present when fraud does occur.

[7] Federal Communications Commission, Office of Inspector General, *Semiannual Report to Congress*, October 1, 2016-March 31, 2017 (Washington, D.C.: May 2017). Competitive bidding is a formal process in which the applicant identifies and requests the products and services it needs so that potential service providers can review those requests and submit bids for them.

[8] We define "key fraud risks identified" to mean recurring financial fraud risk factors identified multiple times across three sources of information that we reviewed from calendar years 2014 through 2019. Additional details on the three sources of information we reviewed are described below.

- the extent to which FCC is managing fraud risks (including through USAC) for the E-rate program in accordance with selected leading practices in fraud risk management; and
- the extent to which FCC and USAC face any challenges in effectively employing data analytics to support fraud risk management activities.

To identify key fraud risks in the E-rate program, we first reviewed three sources that spanned from calendar years 2014 through 2019.[9] These sources were: (1) documented cases of fraud and suspected fraud;[10] (2) the results of FCC's OIG audits and investigations; and (3) documented risk assessments of the E-rate program provided by FCC and USAC.[11] We then catalogued and described the identified key fraud risks from the three sources we reviewed.[12] We also reviewed various FCC forms that E-rate program applicants and service providers must submit to USAC during the application and funding phases. In addition, we met with officials from the FCC OIG to inquire about any possible fraud risks affecting the E-rate program. Next, we prepared and presented the list of key fraud risks identified and the sources of those fraud risks to FCC and USAC program officials and managers to determine whether they

[9] We chose this time period to include E-rate program transactions that occurred approximately within the last 5 funding years. Also, in 2014, FCC began taking steps to modernize and streamline the E-rate program and expand funding for wireless networks in elementary and secondary schools across the United States. Although we attempted to identify all the cases from calendar years 2014 through 2019, it is possible that there are some cases that we did not locate or receive. For this reason, the universe of cases we identified may not be exhaustive and thus cannot be generalizable to all cases. We present examples of cases, fraud risks, or dollar losses as illustrative examples in the report.

[10] The documented cases we reviewed included: (1) adjudicated and settled federal district court cases identified through review of the Department of Justice's online press releases or received from FCC or FCC OIG and then reviewed further through court documents obtained from the Public Access to Court Records system; (2) cases of alleged E-rate program violations of FCC's rules that appear as standalone FCC orders or notices on FCC's website and those we requested from FCC that FCC administratively adjudicated or settled; and (3) whistleblower complaint cases and referred cases of alleged E-rate program fraud we requested from the FCC OIG, USAC, and FCC's Enforcement Bureau.

[11] These sources may have involved facts and circumstances that occurred or existed prior to our audit scope.

[12] During the course of our audit, we learned of a recent federal court case that was adjudicated subsequent to our planned audit scope. We reviewed the facts and circumstances of this case and determined that we would include it in our review as an illustrative example since the case's fraud scheme occurred during our audit scope and involved the key fraud risks we describe in this report.

consider such risks to be key fraud risks that currently affect the E-rate program. In this report, we do not detail all the fraud risks we identified so that potential perpetrators of fraud do not become aware of their existence or exploit potential control weaknesses.

To determine the extent to which FCC is managing fraud risks (including through USAC) for the E-rate program in accordance with selected leading practices in fraud risk management, we reviewed FCC's and USAC's rules, policies, processes, tools, responsibilities, and guidance related to fraud risk management. We also analyzed documentation related to FCC's and USAC's risk assessment processes, including any assessment of fraud risks, and interviewed FCC and USAC officials about their efforts to manage fraud risks. In addition, we reviewed fraud and other risk assessments completed by or for FCC and USAC from calendar years 2014 through 2019. We assessed the information gathered to determine the extent to which FCC had implemented selected leading practices contained in *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework).[13] Our assessment focused on the leading practices contained in the second component related to assessing fraud risks.[14] We selected the leading practices within the assess component because the identification and assessment of fraud risks are an important step in determining whether FCC's and USAC's actions identify and address areas at risk for fraud. To the extent we found that FCC's or USAC's actions were inconsistent with leading practices, we conducted further interviews with program managers from FCC and USAC to determine the rationale. We also inquired about the

[13] GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015). The Fraud Risk Framework contains four components: (1) commit; (2) assess; (3) design and implement; and (4) evaluate and adapt. Within the four components, there are overarching concepts and leading practices.

[14] GAO issued a report in October 2019 recommending that the Chairman of FCC ensure that FCC's Office of Managing Director follows the leading practices in GAO's Fraud Risk Framework related to a dedicated entity's management of its antifraud activities, such as serving as the repository of knowledge on fraud risks and coordinating antifraud initiatives. Therefore, in this report we did not review the first component of the framework, which focuses on committing to an organizational structure to combat fraud. See GAO, *Telecommunications: FCC Should Take Additional Action to Manage Fraud Risks in Its Program to Support Broadband Service in High-Cost Areas*, GAO-20-27 (Washington, D.C.: Oct. 23, 2019). Additionally, we did not review the third or fourth components of the framework, which focus on: (1) designing and implementing an antifraud strategy and (2) evaluating outcomes using a risk-based approach and then adapting activities to improve fraud risk management because we ultimately found, as discussed in this report, that FCC had not fully adopted fraud risk management activities from the second component that trigger related activities in the third and fourth components.

related antifraud controls, if any that FCC or USAC reported could help address the identified key fraud risks.[15] In this report, we do not detail all the mitigating antifraud controls FCC or USAC officials told us they can use to address the key fraud risks we identified, so that potential perpetrators of fraud do not become aware of their existence or exploit potential control weaknesses.

To determine the extent to which FCC and USAC face challenges in effectively employing data analytics in support of fraud risk management activities, we interviewed FCC and USAC officials to determine how they use the E-rate program data and what type of data analytics, if any, they perform. We also reviewed USAC's data dictionaries to try to gain an understanding of the E-rate program data available for the purpose of performing data analytics. In addition, we interviewed FCC OIG officials about their experience using E-rate program data. As appropriate, we assessed the information gathered to determine the extent to which FCC and USAC's fraud risk management data-analytics activities align with federal internal control standards and the Fraud Risk Framework.[16]

We conducted this performance audit from April 2019 to September 2020 in accordance with generally accepted government auditing standards.[17] 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

[15] We did not evaluate the extent to which FCC's or USAC's designed controls were implemented or operating effectively or efficiently as this was outside the scope of our audit and premature for us to do as this is an unmet requirement for FCC and USAC to perform under the third component of the Fraud Risk Framework (i.e., "examine the suitability of existing controls"). Further, we did not interview officials from schools, libraries, or service providers to inquire about the controls they use to address any of the key fraud risks identified, as they were outside the scope of our audit.

[16] GAO-14-704G and GAO-15-593SP. While we did not review the third component of the framework, which focuses on designing and implementing an antifraud strategy, for purposes of our review of FCC's and USAC's challenges in effectively employing data analytics in support of fraud risk management activities, we selected relevant leading practices for data-analytics activities.

[17] We designed our audit prior to March 2020, when the Coronavirus Disease 2019 was declared a global pandemic and when Congress enacted the Coronavirus Aid, Relief, and Economic Security Act. As a result, this report predates changes, if any, to the E-rate program application or funding process that may have occurred as result of this global pandemic. Further, this report does not include an assessment of FCC's or USAC's fraud risk management efforts as it relates to any emerging E-rate program fraud risks that may stem from these events.

the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Overview of the E-rate Program and Participating Entities

The E-rate program provides eligible schools, school districts, and libraries, as well as consortia that include eligible schools and libraries, discounts on eligible broadband and telecommunications services or equipment.[18] The E-rate program was mandated by Congress in the Telecommunications Act of 1996.[19] In July 2014 and December 2014, FCC adopted the 2014 First and Second E-rate Orders, which cited three goals for the program:

- ensuring affordable access to high-speed broadband sufficient for schools and libraries;
- maximizing the cost-effectiveness of spending for E-rate program-supported purchases; and
- making the E-rate program's application process and other E-rate program's processes fast, simple, and efficient.

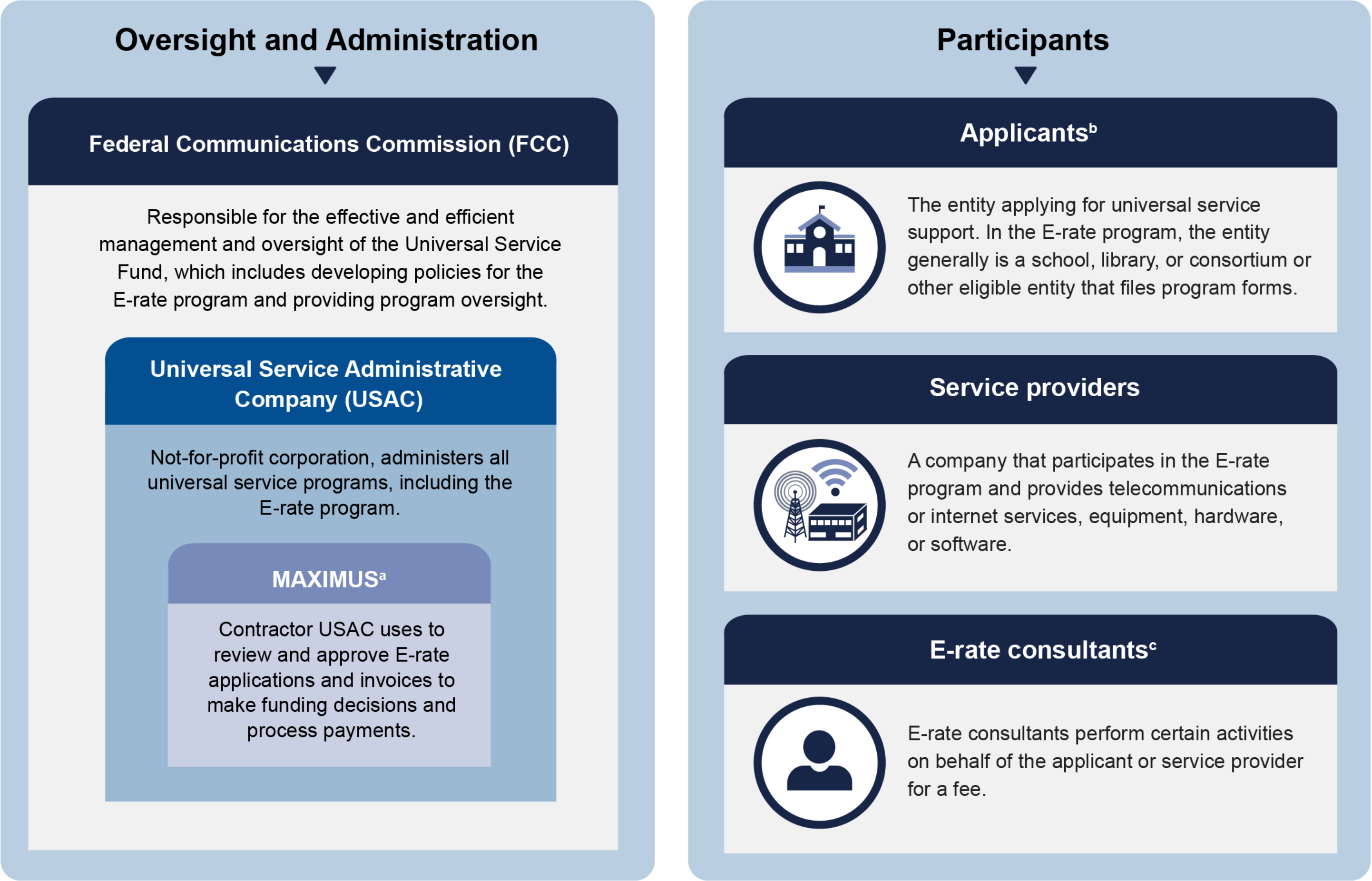
As illustrated in figure 1 below, FCC is responsible for developing the E-rate program's policies and oversight. FCC designated USAC, a not-for-profit entity, to administer the E-rate program through its Schools and Libraries Division. As part of this designation, since 2019, USAC has used a contractor, MAXIMUS, a for-profit company, to carry out certain key aspects of the program, such as reviewing and approving

[18] E-rate program funds can be used for internet access, internal connections, managed internal broadband services, basic maintenance of internal connections, telecommunications, and telecommunications services. Internal connections services are products—such as routers, switches, hubs, and wiring—needed to bring broadband into, and provide it throughout, schools and libraries.

[19] In section 254 of the Communications Act of 1934, as added by the Telecommunications Act of 1996, Congress instructed FCC to establish support mechanisms with the goal of ensuring the delivery of affordable telecommunications service to all Americans, including consumers in high-cost areas, low-income consumers, eligible schools and libraries, and rural health care providers. The 1996 Act instructed FCC to establish a universal service mechanism to ensure that schools and libraries have affordable access to advanced telecommunications and information services to use for educational purposes at discounted rates. See 47 U.S.C. § 254(h).

applications and invoices.[20] The participants in the E-rate program include school and library applicants; service providers; and E-rate program consultants. To receive E-rate program support, schools and libraries must apply each funding year.

Figure 1: Entities Overseeing, Administering, and Participating in E-rate Program



Oversight and Administration

Federal Communications Commission (FCC)

Responsible for the effective and efficient management and oversight of the Universal Service Fund, which includes developing policies for the E-rate program and providing program oversight.

Universal Service Administrative Company (USAC)

Not-for-profit corporation, administers all universal service programs, including the E-rate program.

MAXIMUS[a]

Contractor USAC uses to review and approve E-rate applications and invoices to make funding decisions and process payments.

Participants

Applicants[b]

The entity applying for universal service support. In the E-rate program, the entity generally is a school, library, or consortium or other eligible entity that files program forms.

Service providers

A company that participates in the E-rate program and provides telecommunications or internet services, equipment, hardware, or software.

E-rate consultants[c]

E-rate consultants perform certain activities on behalf of the applicant or service provider for a fee.

Source: GAO analysis of USAC information. | GAO-20-606

[a] USAC selected MAXIMUS to provide business process outsourcing services in support of the E-rate program. Invoices are processed by USAC. Payments are certified by FCC and processed by the Department of the Treasury.

[b] Applicant eligibility is determined by statute and FCC's rules for the E-rate program.

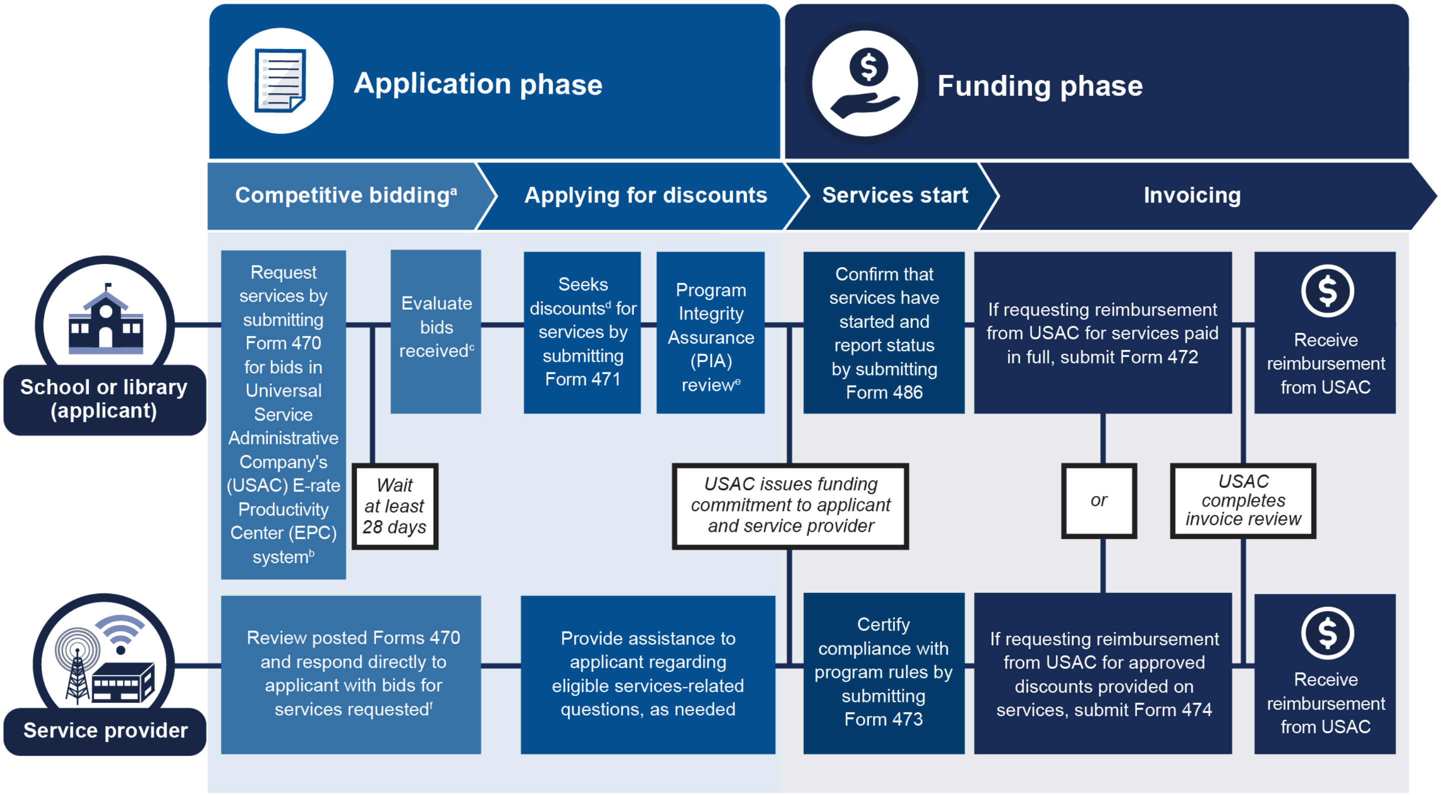
[20] As a contractor, MAXIMUS performs these reviews on the basis of FCC- and USAC-approved procedures and with USAC oversight. For purposes of this report, we use "USAC" to refer to activities that either USAC or MAXIMUS performs. Prior to contracting with MAXIMUS in 2019, SOLIX was USAC's vendor for these services.

[c] E-rate program applicants must identify any consultant that assists with the application or funding process.

E-rate Program Application and Funding Processes

The E-rate program provides applicants discounts ranging from 20 to 90 percent based on indicators of need and the category of service requested.[21] Applicants use the E-rate Productivity Center (EPC) system to submit applications to USAC. Figure 2 illustrates USAC's application and funding processes and phases.

Figure 2: USAC E-rate Program Application and Funding Processes and Phases


Application phase
Funding phase
Competitive bidding[a]
Applying for discounts
Services start
Invoicing
School or library (applicant)
Service provider
Request services by submitting Form 470 for bids in Universal Service Administrative Company's (USAC) E-rate Productivity Center (EPC) system[b]
Evaluate bids received[c]
Wait at least 28 days
Seeks discounts[d] for services by submitting Form 471
Program Integrity Assurance (PIA) review[e]
USAC issues funding commitment to applicant and service provider
Confirm that services have started and report status by submitting Form 486
If requesting reimbursement from USAC for services paid in full, submit Form 472
or
USAC completes invoice review
Receive reimbursement from USAC
Review posted Forms 470 and respond directly to applicant with bids for services requested[f]
Provide assistance to applicant regarding eligible services-related questions, as needed
Certify compliance with program rules by submitting Form 473
If requesting reimbursement from USAC for approved discounts provided on services, submit Form 474
Receive reimbursement from USAC

Source: GAO analysis of USAC information. | GAO-20-606

[a] Competitive bidding is a formal process in which the applicant identifies and requests the products and services it needs so that potential service providers can review those requests and submit bids for them. To begin the competitive-bidding process, the applicant must complete and certify an FCC

[21] These indicators include: (1) the percentage of students eligible for free or reduced-price lunches through the National School Lunch Program or a federally approved alternative mechanism and (2) whether the entity is located in a rural area. See 47 C.F.R. § 54.505.

Form 470. After applicants file Forms 470, the forms are available on USAC's public website for any service provider to see and to bid on.

[b] EPC is the account- and application-management portal for the E-rate program.

[c] Before selecting a service provider, applicants must wait at least 28 days after the FCC Form 470 is certified in EPC and consider all bids that were received. The applicant must select the most cost-effective service offering and use the price of the eligible goods and services as the primary factor. Eligible goods and services include internet access, internal connections, managed internal broadband services, basic maintenance of internal connections, telecommunications, and telecommunications services.

[d] The E-rate program provides discounts to schools and libraries for eligible products and services.

[e] USAC, or its contractor, MAXIMUS, conducts the PIA review—the compliance review process of Forms 471 that must be completed before funding commitments are made by USAC.

[f] USAC does not receive the bids the service providers send to the applicant. Also, service providers cannot assist applicants regarding competitive bidding.

The E-rate program is funded through statutorily mandated payments into the USF by companies that provide interstate and international telecommunication services. Many of these companies, in turn, pass on their contribution costs to their subscribers through a line item on subscribers' telephone bills. E-rate program funding is disbursed by USAC either to service providers or directly to schools and libraries.

Funding to service providers. Reimbursements for the discounted amount are made to the service provider when the service provider has charged the school or library the non-discounted amount of the eligible services delivered by the service provider. For example, if an applicant is eligible for an 80 percent discount on a bill amounting to $100, then the applicant pays the non-discounted share (e.g., $20) and the service provider then seeks a reimbursement from USAC for the discounted share (e.g., $80).

Funding directly to a school or library. Reimbursements for the discounted amount are made to the school or library if it paid in full to the service provider for the eligible services delivered by the service provider. For example, if an applicant is eligible for an 80 percent discount on a bill amounting to $100, the applicant pays 100 percent of the service provider's bill (e.g., $100) and then seeks a reimbursement from USAC for the discounted share (e.g., $80).

Fraud Risk Management

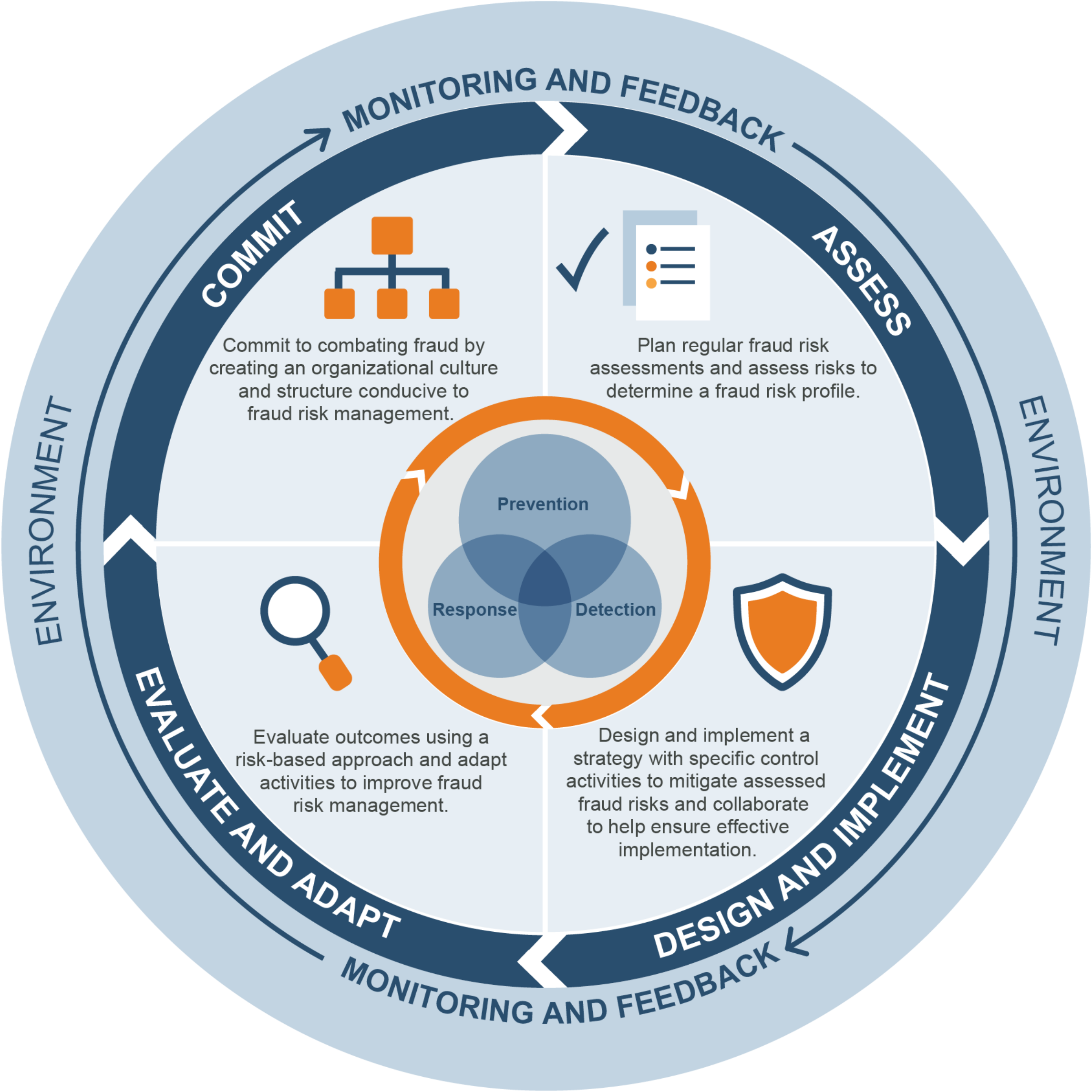
As mentioned earlier in this report, fraud and "fraud risk" are distinct concepts. Fraud—obtaining something of value through willful misrepresentation—can be challenging to detect and adjudicate because of its deceptive nature. Fraud risk exists when individuals have an opportunity to engage in fraudulent activity, have an incentive or are under pressure (e.g., financial pressures) to commit fraud, or are able to rationalize committing fraud. When fraud risks can be identified and mitigated, fraud may be less likely to occur. Although the occurrence of fraud indicates there is a fraud risk, a fraud risk can exist even if actual fraud has not yet been identified or adjudicated.

Executive-branch agency managers are responsible for managing fraud risks and implementing practices for combating those risks. Federal internal control standards state that as part of an overall risk assessment, management should consider the potential for fraud when identifying, analyzing, and responding to risks.[22] In July 2015, GAO issued the Fraud Risk Framework, which provides a comprehensive set of key components, overarching concepts, and leading practices that serve as a guide for agency managers to use when developing efforts to combat fraud in a strategic, risk-based way.[23] In particular, as shown in figure 3 below, the framework contains four components: (1) commit, (2) assess, (3) design and implement, and (4) evaluate and adapt.

[22] GAO-14-704G.

[23] GAO-15-593SP.

Figure 3: GAO's Fraud Risk Management Framework


MONITORING AND FEEDBACK
COMMIT
Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.
ASSESS
Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.
ENVIRONMENT
Prevention
Response
Detection
ENVIRONMENT
EVALUATE AND ADAPT
Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.
DESIGN AND IMPLEMENT
Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.
MONITORING AND FEEDBACK

Source: GAO. | GAO-20-606

The Fraud Reduction and Data Analytics Act of 2015, enacted in June 2016, required the Office of Management and Budget (OMB) to establish guidelines for federal agencies to create controls to identify and assess fraud risks and to design and implement antifraud control activities. The act further required OMB to incorporate the leading practices from the

Fraud Risk Framework in the guidelines. Although the Fraud Reduction and Data Analytics Act of 2015 was repealed in March 2020, the Payment Integrity Information Act of 2019 requires these guidelines to remain in effect, subject to modification by OMB as necessary and in consultation with GAO.[24]

Following a 2019 GAO recommendation, FCC and USAC have recently begun to establish dedicated entities to lead fraud risk management efforts for the USF programs, including E-rate.[25] Having such an entity is consistent with the leading practices contained in the Fraud Risk Framework's commit component. Specifically, according to FCC officials, FCC's Enterprise Risk Management Group will be the dedicated entity for conducting fraud risk assessment efforts for all of the USF programs. Further, according to USAC officials, in June 2019, USAC created the Office of General Counsel Fraud Risk Group, which will be USAC's dedicated entity responsible for coordinating with FCC to develop a USAC fraud risk assessment of factors affecting all of FCC's USF programs. In partnership with Schools and Libraries Division Program staff, the Fraud Risk Group assists in managing fraud risks affecting all USF programs, including E-rate. It is also responsible for assessing fraud-specific internal controls, identifying fraud vulnerabilities, and implementing safeguards. In addition, the Fraud Risk Group monitors whistleblower complaints received through USAC's hotline, audit findings, and internal observations of potential program fraud and improperly disbursed funds.

FCC's Enforcement Bureau and the FCC OIG also have roles in fraud risk management. FCC's Enforcement Bureau is the primary FCC unit responsible for, among other items, enforcing the provisions of the Communications Act and FCC's rules. For example, it receives referrals from USAC's Fraud Risk Group and others, and its mission is to investigate and respond to potential unlawful conduct. FCC OIG provides independent investigations, audits, and reviews of FCC's programs and operations. The OIG refers criminal matters to the U.S. Department of Justice and other law enforcement entities for prosecution.

[24] Pub. L. No. 116-117, § 2(a), 134 Stat. 113, 131 - 132 (2020), codified at 31 U.S.C. § 3357.

[25] According to FCC officials, FCC and USAC plan to have these entities coordinate with each other to execute their distinct roles in fraud risk management efforts.

Key Fraud Risks Identified in the E-rate Program Include Self-Certifications

Several key fraud risks have persistently affected the E-rate program since at least 2014. Specifically, based on our review of various sources, including federal court cases and FCC violations, we identified self-certifications as an inherent overarching key fraud risk that has affected the E-rate program.[26] We also identified underlying key fraud risks that involved opportunities to willfully self-certify misrepresented information and circumvent competitive-bidding requirements, collude, and engage in conflicts of interest.[27]

Reliance on Self-Certifications Is an Inherent Overarching Key Fraud Risk

Reliance on self-certification statements used on FCC's forms is an inherent overarching key fraud risk affecting the E-rate program application and funding phases.[28] This key fraud risk presents opportunities for applicants, service providers, or consultants to misrepresent dozens of self-certification statements on various application and funding FCC forms (see sidebar).[29]

[26] For the purposes of this report, we define "inherent overarching key fraud risk" to mean a key fraud risk that by its nature exists across a program (i.e., across the E-rate program application and funding phases) regardless of the controls in place. "Underlying key fraud risk" refers to specific examples of opportunities to defraud the E-rate program as a result of the inherent overarching fraud risk we identified.

[27] The key fraud risks identified in this report are not an exhaustive list of all fraud risks affecting the E-rate program.

[28] As illustrated in figure 2 above, the E-rate program's application phase consists of USAC determining the amount of program funds it could commit based on its review of various eligibility information that is self-reported and self-certified on various FCC forms submitted by schools and libraries, as well as additional information USAC may request during PIA reviews. According to USAC officials, this additional information is used to verify the completeness and accuracy of the information submitted on FCC 471 forms and to ensure compliance with the program's rules and requirements. Such self-reported and self-certified information includes information pertaining to: competitive bids solicited, E-rate program discounts calculated, and types of services being delivered, among other information. The funding phase consists of USAC reviewing various self-reported and self-certified invoice information that the schools, libraries, or service providers provide on FCC forms requesting the actual disbursement of E-rate program funding.

[29] According to FCC officials, the self-certification statements are required under penalty of perjury and applicants could be subject to fines for providing false information or making false statements. Nevertheless, relying on these self-certification statements can create opportunities for E-rate program participants to misrepresent or falsely certify: the certification statements themselves; E-rate program participants' adherence to program requirements and rules; or the veracity of the information inputted on the FCC forms or documentation maintained elsewhere.

Illustrative examples of E-rate program violations involving the key fraud risks associated with opportunities to misrepresent self-certifications

In July 2014, FCC found that a service provider and applicant misrepresented self-certification statements and violated FCC's rules during funding year 2003 by seeking E-rate program reimbursement for an approved wireless network, but instead purchasing and installing servers and fiber optic cables.

- **Amount improperly disbursed:** $33,894.

In October 2018, FCC found that a service provider misrepresented self-certification statements and violated FCC rules for funding years 1998, 1999, and 2000 by failing to bill the applicant's non-discounted share for internet access and seeking E-rate program reimbursements for services never approved by USAC and billed the schools for services that it never provided, over-billed for services that it did provide, and billed for ineligible services.

- **Amount improperly disbursed:** $5,021,070.

Source: GAO analysis of FCC program violations. | GAO-20-606

As we have previously reported, relying on program participants to self-report and self-certify information on agency forms, instead of verifying such information independently, could cause an agency to miss opportunities to prevent program fraud and abuse.[30] FCC designed the E-rate program to allow it to be administered as a self-certifying program. As such, in any given transaction throughout the E-rate program's application and funding process, USAC relies on the truthfulness of dozens of different self-certification statements provided by the applicants and service providers on various FCC forms. In particular, applicants and service providers must self-certify to several actions taken or information provided during the application and funding phases. This self-certifying includes information pertaining to compliance with application and funding requirements. According to FCC officials, while providing documentation to support these certifications may not be required in all cases, FCC's rules do not prevent USAC from requesting documentation from E-rate program participants to verify compliance with the statutory or regulatory requirements of the E-rate program, at any time, including in the course of reviewing a funding request prior to issuing a funding commitment. For example, according to FCC officials, USAC conducts various reviews and audits during the application and funding phases that can involve requesting documentation and may help determine the veracity of the self-certification statements made during these phases.

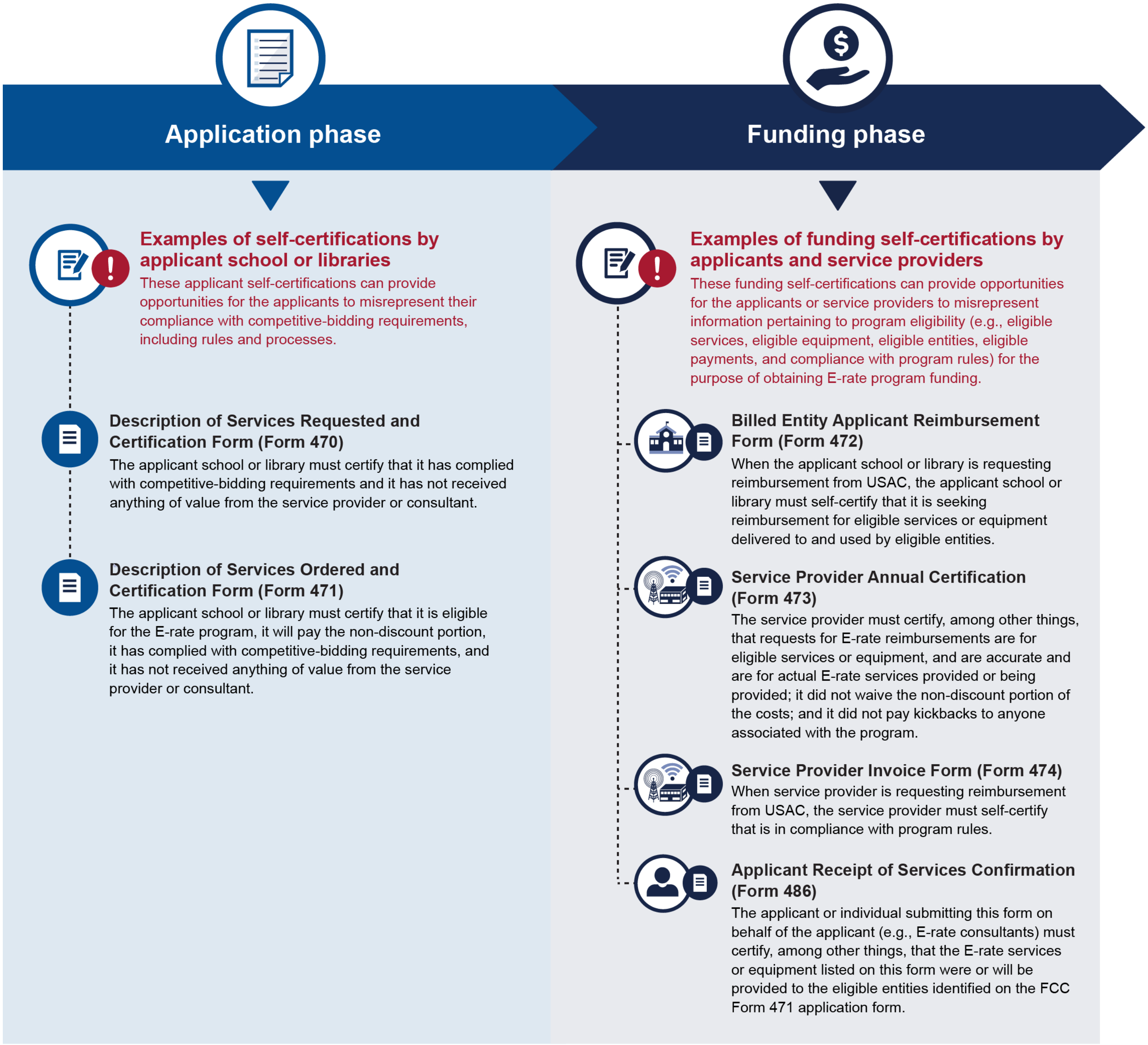
Further, and as described earlier this report, FCC has identified one of the most common root causes of the E-rate program's improper payments to be lack of sufficient application, invoicing, and funding documentation to demonstrate program compliance.[31] Without appropriate supporting documentation, the validity of information self-reported and self-certified cannot be determined. Although it is possible that these payments were for valid purposes, it is also possible that improper payments could reveal indicators of potential fraudulent activities, but the lack of sufficient documentation to demonstrate program compliance could further conceal such fraudulent activities. Thus, reliance on these self-certifications can provide opportunities for applicants or service providers to misrepresent these statements and defraud the E-rate program and obtaining improper E-rate program funding. As illustrated in figure 4, there are a number of

[30] GAO, *Export-Import Bank: EXIM Should Explore Using Available Data to Identify Applicants with Delinquent Federal Debt*, GAO-19-337 (Washington, D.C.: Mar. 23, 2019); and GAO, *Aviation: FAA Needs to Better Prevent, Detect, and Respond to Fraud and Abuse Risks in Aircraft Registration*, GAO-20-164 (Washington, D.C.: Mar. 25, 2020).

[31] Federal Communications Commission, *Agency Financial Report: Fiscal Year 2019* (Nov. 19, 2019).

opportunities for E-rate program participants to misrepresent a variety of self-certification statements, including those statements pertaining to compliance with competitive-bidding rules; discount rates calculated; invoices provided and paid; E-rate program services or equipment provided and received; and E-rate program funding requested.

Figure 4: Examples of Opportunities for Applicants and Service Providers to Self-Certify Misrepresented Application and Funding Information



Application phase

Examples of self-certifications by applicant school or libraries

These applicant self-certifications can provide opportunities for the applicants to misrepresent their compliance with competitive-bidding requirements, including rules and processes.

Description of Services Requested and Certification Form (Form 470)

The applicant school or library must certify that it has complied with competitive-bidding requirements and it has not received anything of value from the service provider or consultant.

Description of Services Ordered and Certification Form (Form 471)

The applicant school or library must certify that it is eligible for the E-rate program, it will pay the non-discount portion, it has complied with competitive-bidding requirements, and it has not received anything of value from the service provider or consultant.

Funding phase

Examples of funding self-certifications by applicants and service providers

These funding self-certifications can provide opportunities for the applicants or service providers to misrepresent information pertaining to program eligibility (e.g., eligible services, eligible equipment, eligible entities, eligible payments, and compliance with program rules) for the purpose of obtaining E-rate program funding.

Billed Entity Applicant Reimbursement Form (Form 472)

When the applicant school or library is requesting reimbursement from USAC, the applicant school or library must self-certify that it is seeking reimbursement for eligible services or equipment delivered to and used by eligible entities.

Service Provider Annual Certification (Form 473)

The service provider must certify, among other things, that requests for E-rate reimbursements are for eligible services or equipment, and are accurate and are for actual E-rate services provided or being provided; it did not waive the non-discount portion of the costs; and it did not pay kickbacks to anyone associated with the program.

Service Provider Invoice Form (Form 474)

When service provider is requesting reimbursement from USAC, the service provider must self-certify that is in compliance with program rules.

Applicant Receipt of Services Confirmation (Form 486)

The applicant or individual submitting this form on behalf of the applicant (e.g., E-rate consultants) must certify, among other things, that the E-rate services or equipment listed on this form were or will be provided to the eligible entities identified on the FCC Form 471 application form.

Source: GAO analysis of FCC information. | GAO-20-606

In addition, in 2004, the FCC Inspector General testified at a congressional committee hearing about the concerns he and the U.S. Department of Justice had with FCC's heavy reliance on self-certifications. Specifically, the FCC Inspector General testified that these self-certifications expose the E-rate program to fraud, waste, abuse, and improper funding.[32] The following year, in 2005, a congressional committee's investigation report found that the E-rate program self-certifications seemed to have little effect in deterring some school officials and service providers from taking advantage of the program's weaknesses.[33] Today, the reliance on self-certifications persists as a key fraud risk to the E-rate program. If not sufficiently assessed and addressed from the fraud risk management approach, as we describe later in this report, the E-rate program self-certification statements will continue to provide opportunities for applicants and service providers to misrepresent a variety of self-certified applicant or funding information, which can create the fraud risk of applicants or service providers receiving fraudulent and improper E-rate program funding.

Underlying Key Fraud Risks Identified

In addition to the inherent overarching key fraud risk of self-certifications, we identified three underlying and related key fraud risks.

[32] *The Universal Service E-rate Program,* Before the S. Committee on Commerce, Science, Transportation, 108th, Cong. 108-962 (2004) (statement of Inspector General of the Federal Communications Commission H. Walker Feaster III).

[33] *Waste, Fraud, and Abuse Concerns with the E-rate Program,* Before the H. Subcommittee on Oversight and Investigations, 109th Cong. (2005) (statement of Chairman Ed Whitfield).

Underlying Key Fraud Risk: Opportunity to Misrepresent Competitive Bidding

Opportunities to misrepresent compliance with competitive-bidding requirements, such as competitive-bidding rules and processes, is a key underlying fraud risk (see sidebar). This risk involves self-certification statements during the E-rate program application phase. For example, applicants could misrepresent self-certification statements regarding competitive bidding by circumventing or violating competitive-bidding rules or processes, unbeknownst to FCC or USAC. Such an opportunity exists because neither entity has visibility into the competitive bids that the applicant says it receives. Figure 5 presents examples of the types of self-certifications that are required during the application phase and that are potentially vulnerable to misrepresentations.

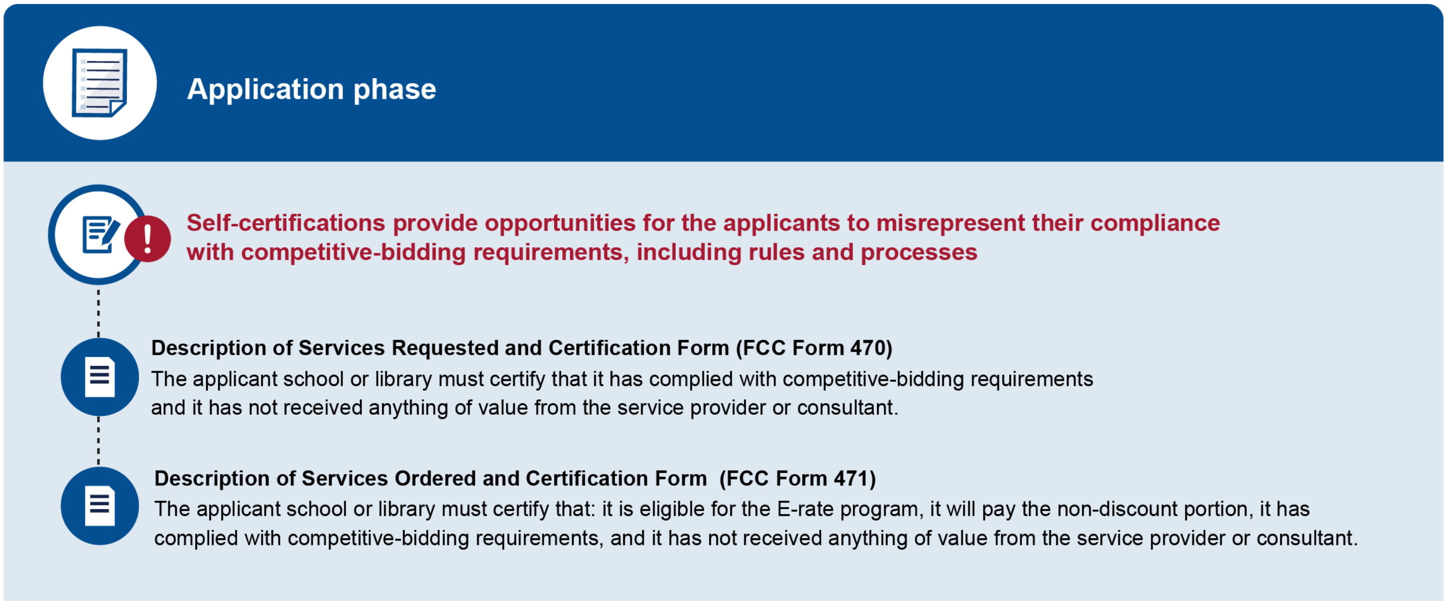
Illustrative example of E-rate program violations involving the key fraud risks associated with opportunities to circumvent competitive bidding and misrepresent self-certifications

In April 2015, FCC found that a service provider misrepresented self-certification statements by providing “grants” through an affiliated nonprofit to pay for the applicants’ non-discounted share for distance-learning services for funding years 2004 to 2008, in violation of FCC rules. FCC also found that the provider’s ability to provide grants to the schools for the non-discounted share created an unfair advantage during the competitive-bidding processes

- Amount improperly disbursed: $1,089,702.

Source: GAO analysis of FCC program violations. | GAO-20-606

Figure 5: Examples of Self-Certifications Required during the Application Phase



Application phase

Self-certifications provide opportunities for the applicants to misrepresent their compliance with competitive-bidding requirements, including rules and processes

Description of Services Requested and Certification Form (FCC Form 470)
The applicant school or library must certify that it has complied with competitive-bidding requirements and it has not received anything of value from the service provider or consultant.

Description of Services Ordered and Certification Form (FCC Form 471)
The applicant school or library must certify that: it is eligible for the E-rate program, it will pay the non-discount portion, it has complied with competitive-bidding requirements, and it has not received anything of value from the service provider or consultant.

Source: GAO analysis of FCC information. | GAO-20-606

Currently, USAC does not have direct access, through a repository or otherwise, to obtain and monitor bidding information submitted by bidders without requesting such information from the applicants or service providers. According to the FCC OIG, an open competitive-bidding process lies at the heart of the E-rate program and is key to ensuring that USAC does not pay more than it should for supported E-rate program services or products and helps deter fraud, waste, and abuse during the competitive-bidding process and during pre-commitment phase.

In 2015, the USAC contractor that conducted a risk assessment of the E-rate program recommended that USAC develop a central document repository where applicants would be required to upload and store key documents (e.g., service contract, billed invoices) at the time an application was filed. The contractor also noted that existing controls would need to be modified to require review of these documents. Similarly, since 2017, the FCC OIG has recommended that FCC direct USAC to implement an online competitive-bidding repository that focused on the E-rate program's requirements for a fair and open competitive-bidding process. Such a portal could strengthen program controls by allowing USAC direct access to obtain and monitor bidding information submitted by bidders without having to request such information from the applicants or service providers. According to the FCC OIG, "[S]ince the program's inception in 1998, the ability to deter and detect fraud, waste, and abuse, during the competitive-bidding process has been severely limited by the lack of upfront collection of competitive bids."

Additionally, FCC itself has identified one of the most common root causes of E-rate program improper payments to include E-rate program participants violating or circumventing the E-rate program's competitive-bidding rules due to a lack of sufficient documentation to demonstrate compliance with the competitive-bidding rules.[34] FCC officials explained that developing the competitive-bidding portal was initially deferred until the E-rate Productivity Center (EPC) system and associated information technology challenges were resolved and applicants were familiar with its use. As of May 2020, FCC officials told us that in response to the FCC OIG recommendation with regard to strengthening program controls for competitive bidding, they recently provided approval for USAC to move forward with planning and developing the portal. They said they are continuing to work with USAC officials to gather information about the level of effort involved in terms of timing, cost, and other aspects of implementation. Also, current FCC rules do not require that bids be put into a portal, so this situation will need to be addressed through a rulemaking. FCC officials said they expect that competitive-bidding portal to be open and available by July 1, 2022, for funding year 2023.

Underlying Key Fraud Risk: Collusion Opportunities for Applicants and Service Providers

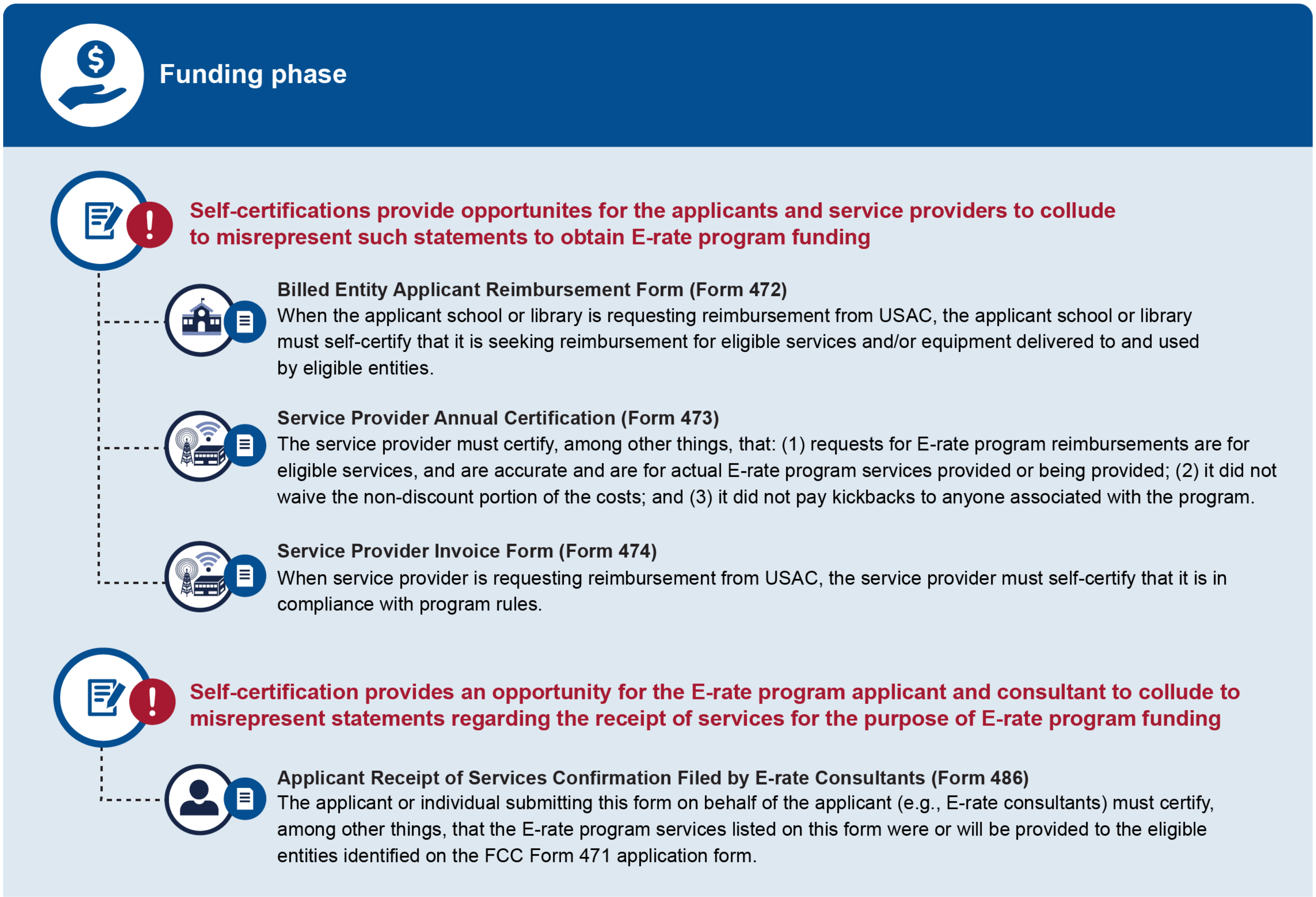
Opportunities for various E-rate program participants to collude was another underlying key fraud risk we identified. For example, we identified opportunities to include misrepresentations on forms requiring self-certification during the application and funding phases through the collusion of E-rate program applicants (i.e., schools and libraries) and service providers. Specifically, such opportunities include E-rate program applicants and service providers colluding to submit bogus or inaccurate application or funding information that they can then falsely self-certify for the purpose of defrauding the E-rate program or obtaining ineligible program funding. Such collusion may not be discovered due to the self-certifying nature of the program.[35] For example, as illustrated in figure 6, several FCC forms provide opportunities for applicants and service

[34] Federal Communications Commission, *Agency Financial Report: Fiscal Year 2019* (Nov. 19, 2019).

[35] For example, during the funding phase, such self-certifications include applicants self-certifying invoice information regarding eligible goods or services that applicants requested and received. Such invoice information is self-reported to USAC, and USAC reviews it before disbursing E-rate program funding.

providers to collude to make misrepresentations on a number of self-certifications during the funding phase.

Figure 6: Examples of Applicant and Service Provider Self-Certifications Required during the Funding Phase



Funding phase

Self-certifications provide opportunites for the applicants and service providers to collude to misrepresent such statements to obtain E-rate program funding

Billed Entity Applicant Reimbursement Form (Form 472)
When the applicant school or library is requesting reimbursement from USAC, the applicant school or library must self-certify that it is seeking reimbursement for eligible services and/or equipment delivered to and used by eligible entities.

Service Provider Annual Certification (Form 473)
The service provider must certify, among other things, that: (1) requests for E-rate program reimbursements are for eligible services, and are accurate and are for actual E-rate program services provided or being provided; (2) it did not waive the non-discount portion of the costs; and (3) it did not pay kickbacks to anyone associated with the program.

Service Provider Invoice Form (Form 474)
When service provider is requesting reimbursement from USAC, the service provider must self-certify that it is in compliance with program rules.

Self-certification provides an opportunity for the E-rate program applicant and consultant to collude to misrepresent statements regarding the receipt of services for the purpose of E-rate program funding

Applicant Receipt of Services Confirmation Filed by E-rate Consultants (Form 486)
The applicant or individual submitting this form on behalf of the applicant (e.g., E-rate consultants) must certify, among other things, that the E-rate program services listed on this form were or will be provided to the eligible entities identified on the FCC Form 471 application form.

Source: GAO analysis of FCC information. | GAO-20-606

Underlying Key Fraud Risk: Opportunity for E-rate Consultants or Educational Service Agencies to Engage in Roles That Misrepresent Conflicts of Interest and Other Information

As mentioned above, fraud involves obtaining something of value through willful misrepresentation. According to USAC, a conflict of interest can exist when an E-rate consultant or Educational Service Agency represents both the applicant and service provider in the same transaction. Such relationships can provide further opportunities for these participants to willfully misrepresent these relationships or application and funding information.

E-rate consultants. Private consultant firms (i.e., E-rate consultants) may assist many E-rate program applicants or service providers with the application and funding processes and complex program requirements. According to FCC officials, E-rate consultants can be hired by and paid on commission by the applicant or service provider. These consultants are typically paid a fee or a commission for their services. However, FCC has noted that a consultant can exert great influence on an applicant's competitive-bidding process and should not have a financial relationship with a service provider that it selects (or recommends) on behalf of the applicant. According to FCC, such a financial relationship can constitute a prohibited conflict of interest and impairs the applicant's ability to hold a fair and open competitive-bidding process.[36] According to USAC, a consultant is any non-employee of the entity that assists the entity in applying for funding by filling out the application materials for a fee. Consulting firms, for purposes of being identified in EPC, may be organizations with multiple employees or they may be individuals.[37] Although E-rate consultants can help applicants and service providers navigate complex E-rate program requirements, according to officials from FCC's OIG, in some cases such relationships can also create opportunities for the consultants to engage in roles that pose conflicts of interest.

E-rate program rules require that all applicants conduct a fair and open competitive-bidding process and do not allow a consultant (acting on behalf of an applicant) to have an ownership interest, sales commission arrangement, or other financial stake with respect to a service provider it selects or recommends on behalf of the applicant. However, USAC

[36] *Akisha Networks, Inc. Order*, 27 FCC Rcd 8294, para. 2 (2012).

[37] As described earlier, during the application and funding phases, applicants and service providers use multiple E-rate program systems, including EPC to submit the FCC forms, which USAC reviews during the application and funding process. Later in this report, we describe other fraud risk management issues pertaining data maintained in USAC's data systems, including EPC.

officials told us that the rules do not expressly prohibit a consultant from representing both an applicant and a service provider in the same transaction in all instances.[38] This can create a conflict of interest opportunity for the consultant and give rise to a competitive-bidding violation if, for example, the consultant is paid on commission and is involved in the vendor selection process. The potential for this kind of conflict, coupled with the EPC account access an applicant may have granted to its consultant, provides the E-rate consultant with an opportunity to misrepresent and falsely self-certify application and funding information for the purpose of defrauding the E-rate program, obtaining improper funding, or facilitating the selection of a service provider that may not be the most cost-effective. While consultants can assist with applications, based on EPC system user rights, they do not certify applications or receive funding on behalf of school and library applicants.[39]

Further, although E-rate consultants are expected to be independent of the applicants, and service providers, neither FCC nor USAC have direct oversight or monitoring responsibility over E-rate consultants' activities. As a result, this absence of direct oversight can increase the likelihood and impact of the opportunities E-rate consultants have to misrepresent self-reported application or funding information and do so with or without the applicants' or service providers' knowledge as illustrated in figure 7 below. This scenario can include additional opportunities for E-rate consultants to collude with schools, libraries, or service providers to include misrepresentations in dozens of self-certification statements on the various FCC application and funding forms pertaining to the veracity

[38] While the rule does not expressly prohibit such conduct, FCC has noted that "[a] consultant, acting on behalf of the applicant, exerts great influence on an applicant's bidding process and thus, should not have a financial relationship with a service provider which it selects (or recommends) on behalf of the applicant." Akisha Networks, Inc. Order, 27 FCC Rcd 8294, para. 2 (2012).

[39] Although FCC officials stated that consultants can assist with application forms in EPC, the consultants do not certify them. However, as we described earlier, if granted these rights by an applicant, an E-rate consultant can complete and self-certify the FCC application forms in EPC on behalf of the applicant, which creates opportunities for the consultant to independently or collude to misrepresent a number of self-reported and self-certified information on FCC application and funding forms for the purpose of defrauding the E-rate program and obtaining improper funding.

of eligible discount rates, entitled E-rate program services or equipment received, or E-rate program funding reimbursed.[40]

Educational Service Agencies (ESA). Federal law defines an ESA as a regional public multiservice agency authorized by state statute to help develop, manage, and provide services or programs to local educational agencies, including services and equipment funded by the E-rate program.[41] ESAs can concurrently serve as E-rate program applicants, consultants, and service providers. Specifically, according to USAC, ESAs may perform concurrently as many as three roles in the E-rate program that should be independent, including applying for E-rate program discounts for schools and libraries; providing E-rate program consulting assistance to their school districts; and serving as the service providers of eligible E-rate program services and equipment. Thus, ESAs also have opportunities to create conflicts of interest, which, in turn, create opportunities to misrepresent various self-reported and self-certified application and funding information. FCC rules do not specifically define or address ESAs, according to USAC. However, USAC officials acknowledged that there is no prohibition on an ESA fulfilling the role of an E-rate program applicant, service provider, or consultant. Such structures, if not assessed and addressed from a fraud risk-based approach described later in this report, can increase the likelihood and impact of any related conflict-of-interest opportunities that ESAs can pose.

The key overarching and underlying fraud risks we identified continue to persist throughout the E-rate program. For example, FCC's annual agency financial reports from 2014 through 2019 highlight a number of these key fraud risks as recurring management challenges affecting the E-rate program. Further, as illustrated in the court case from February 2020 in figure 7 below, such opportunities persist and thus continue to enable applicants, service providers, and consultants to misrepresent self-certification statements, misrepresent competitive bidding, collude, and engage in roles that pose conflicts of interest.

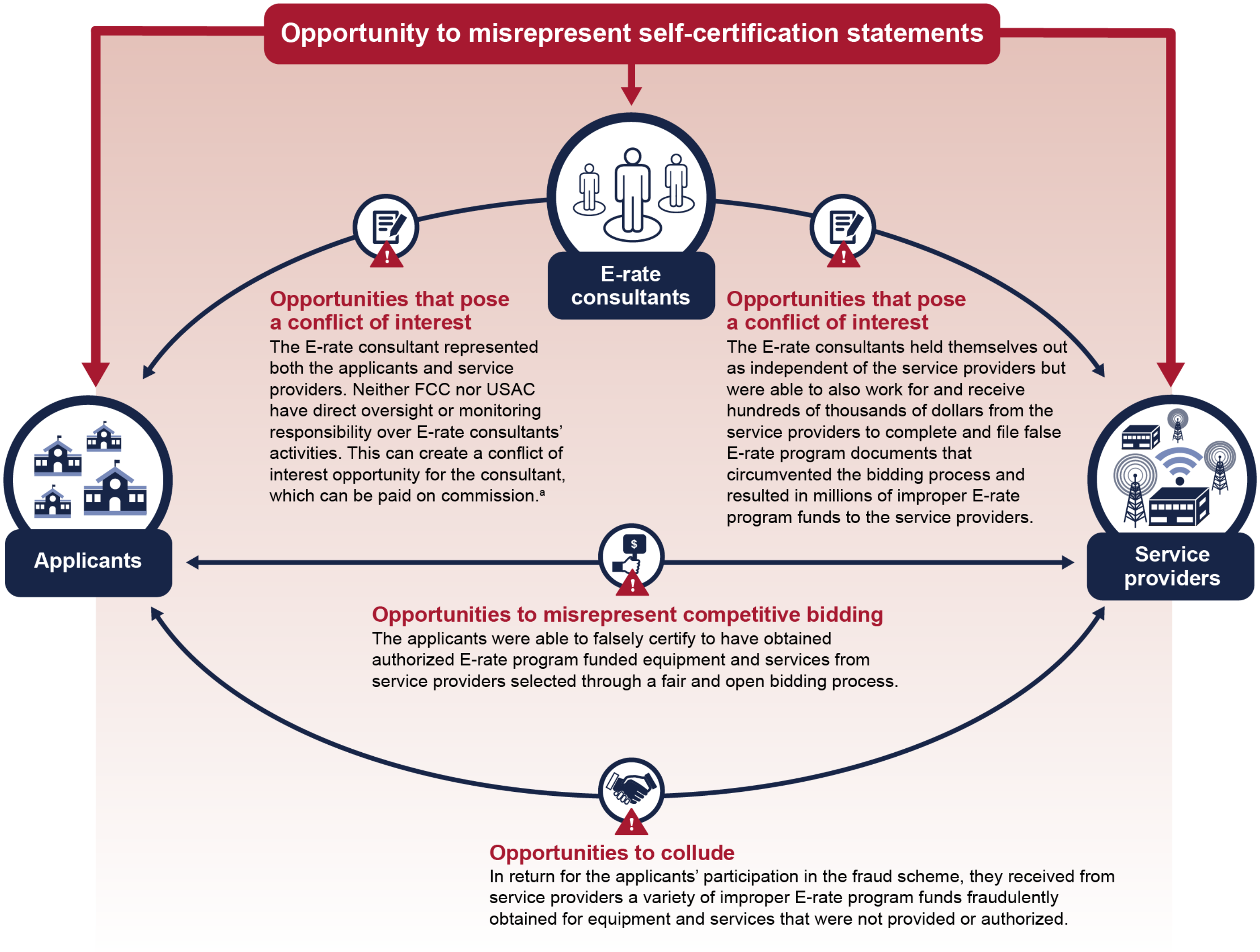
[40] As we describe later in this report, E-rate consultants can also be an Educational Service Agency (ESA), which can create conflicts of interest and opportunities to misrepresent self-certifications if the ESA also serves as an E-rate program applicant or E-rate program service provider, or both roles.

[41] 20 U.S.C. § 1401(5).

Figure 7: Recent Court Case Illustrating Overarching and Underlying Key Fraud Risks

A recent court case that illustrates overarching and underlying key fraud risks

In February 2020, a number of E-rate program applicants, service providers, and consultants pled guilty to conspiring to defraud the program between 2010 and 2016 based on the submission of false certifications, which is an inherent overarching key fraud risk affecting the E-rate program. This resulted in the disbursement of millions of dollars in fraudulent and improper E-rate program funding to support services or equipment that were purposeless, inflated, unauthorized, or not provided. As part of their plea agreements, these E-rate program participants agreed to pay a total of more than $2.6 million in restitution. The following underlying key fraud risks were also apparent in this court case:



Opportunities that pose a conflict of interest
The E-rate consultant represented both the applicants and service providers. Neither FCC nor USAC have direct oversight or monitoring responsibility over E-rate consultants' activities. This can create a conflict of interest opportunity for the consultant, which can be paid on commission.[a]

Opportunities that pose a conflict of interest
The E-rate consultants held themselves out as independent of the service providers but were able to also work for and receive hundreds of thousands of dollars from the service providers to complete and file false E-rate program documents that circumvented the bidding process and resulted in millions of improper E-rate program funds to the service providers.

Opportunities to misrepresent competitive bidding
The applicants were able to falsely certify to have obtained authorized E-rate program funded equipment and services from service providers selected through a fair and open bidding process.

Opportunities to collude
In return for the applicants' participation in the fraud scheme, they received from service providers a variety of improper E-rate program funds fraudulently obtained for equipment and services that were not provided or authorized.

Source: GAO analysis of court documents. | GAO-20-606

[a] According to FCC officials, such conduct is prohibited under FCC rules and precedent. E-rate program rules require that an applicant conduct a fair and open competitive-bidding process. 47 CFR §54.503. FCC has stated that "[a] consultant, acting on behalf of the applicant, exerts great influence

on an applicant's bidding process and thus, should not have a financial relationship with a service provider which it selects (or recommends) on behalf of the applicant." Akisha Networks, Inc. Order, 27 FCC Rcd 8294, para. 2 (2012). In these instances, FCC has found that the consultant's relationship with the service provider and applicant constitutes a prohibited conflict of interest and impairs the applicant's ability to hold a fair and open competitive-bidding processes. Id.

FCC and USAC Have Not Yet Implemented Plans to Comprehensively Assess E-rate Program's Fraud Risks

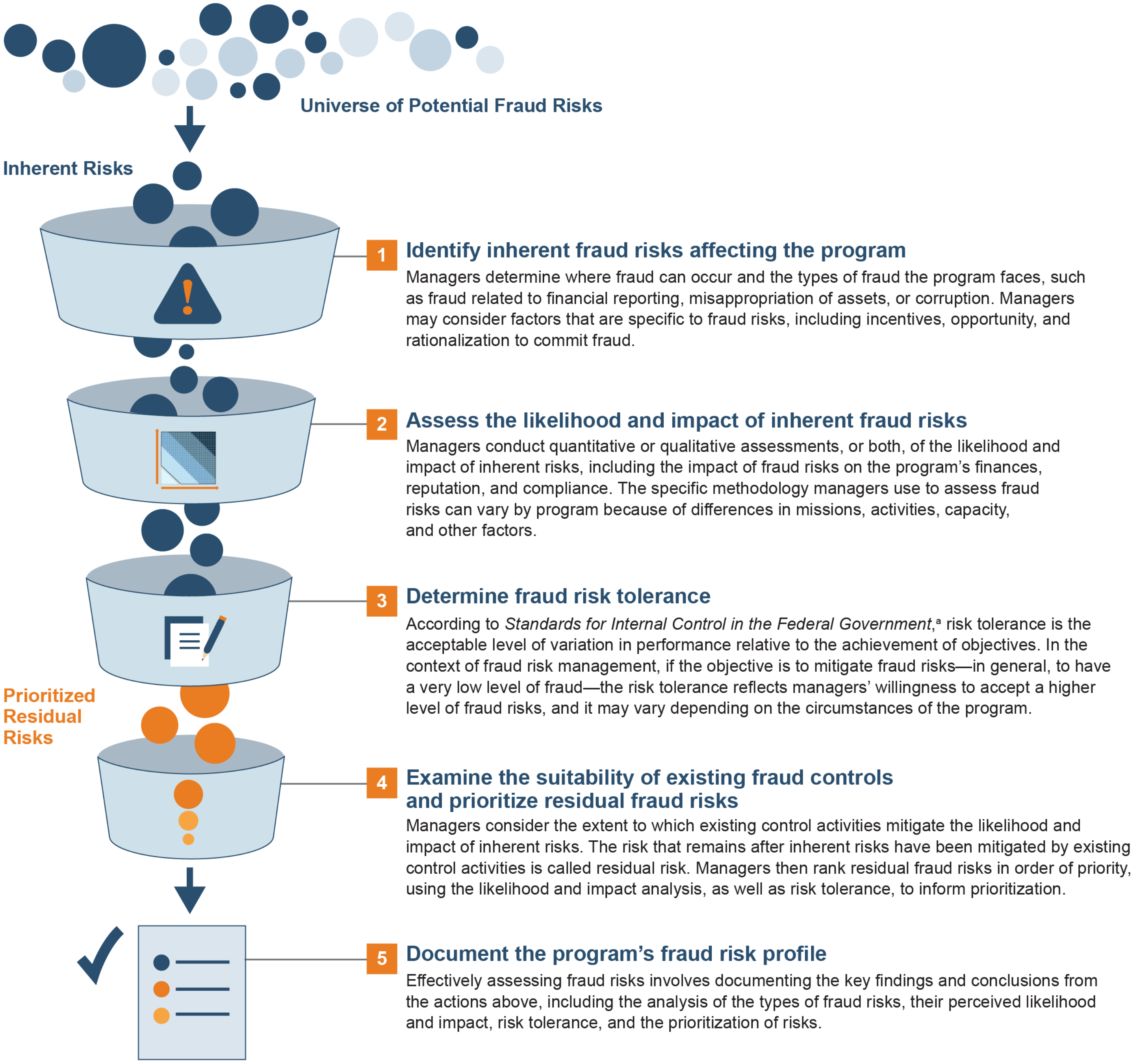
Fraud risk framework component:

Plan regular fraud risk assessments and assess risks to determine a fraud risk profile

Source: GAO. | GAO-20-606

The second component of GAO's Fraud Risk Framework—assess—calls for federal managers to plan regular fraud risk assessments, and to assess risks to determine a fraud risk profile. It also calls for federal managers to examine the suitability of existing controls. Figure 8 below summarizes the key elements of the fraud risk assessment process.

Figure 8: Key Elements of the Fraud Risk Assessment Process



1 **Identify inherent fraud risks affecting the program**

Managers determine where fraud can occur and the types of fraud the program faces, such as fraud related to financial reporting, misappropriation of assets, or corruption. Managers may consider factors that are specific to fraud risks, including incentives, opportunity, and rationalization to commit fraud.

2 **Assess the likelihood and impact of inherent fraud risks**

Managers conduct quantitative or qualitative assessments, or both, of the likelihood and impact of inherent risks, including the impact of fraud risks on the program's finances, reputation, and compliance. The specific methodology managers use to assess fraud risks can vary by program because of differences in missions, activities, capacity, and other factors.

3 **Determine fraud risk tolerance**

According to *Standards for Internal Control in the Federal Government*,[a] risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. In the context of fraud risk management, if the objective is to mitigate fraud risks—in general, to have a very low level of fraud—the risk tolerance reflects managers' willingness to accept a higher level of fraud risks, and it may vary depending on the circumstances of the program.

4 **Examine the suitability of existing fraud controls and prioritize residual fraud risks**

Managers consider the extent to which existing control activities mitigate the likelihood and impact of inherent risks. The risk that remains after inherent risks have been mitigated by existing control activities is called residual risk. Managers then rank residual fraud risks in order of priority, using the likelihood and impact analysis, as well as risk tolerance, to inform prioritization.

5 **Document the program's fraud risk profile**

Effectively assessing fraud risks involves documenting the key findings and conclusions from the actions above, including the analysis of the types of fraud risks, their perceived likelihood and impact, risk tolerance, and the prioritization of risks.

Source: GAO. | GAO-20-606

In 2014 (i.e., prior to GAO's release of the Fraud Risk Framework), FCC developed a fraud risk assessment that included an assessment of fraud risks that could affect the financial operations of the USF programs as a whole. However, this assessment was not tailored to the E-rate program or E-rate program fraud risks specifically. Also, as described above, in 2015, a USAC contractor completed a risk assessment of the E-rate program, which included an assessment of all risks, including fraud risks. However, since 2015, FCC and USAC have not fully implemented key leading practices in the Fraud Risk Framework or responded to the contractor's recommendation to conduct a fraud risk assessment that provides an independent, comprehensive assessment of fraud vulnerabilities to the E-rate program. Specifically, according to FCC and USAC officials, neither FCC nor USAC have yet performed regular standalone fraud risk assessments or determined fraud risk profiles that are tailored to the E-rate program and include a full assessment of fraud risks affecting the E-rate program, including the key fraud risks we describe above.

FCC and USAC officials said that although neither entity has developed a formal comprehensive fraud risk assessment tailored to the E-rate program since GAO issued the Fraud Risk Framework, FCC and USAC perform program and entity level risk assessments that could identify fraud risks. For example:

- According to FCC officials, FCC performs a program-level risk assessment of the E-rate program each year.
- FCC officials also said that USAC conducts an annual entity-level risk assessment as well as a program and processes level risk assessment, which analyze risk at the USF program level, including E-rate. In addition, USAC has been using general risk assessments to annually measure the likelihood of some key fraud risks identified between calendar years 2014 and 2019.
- FCC officials told us that their focus in the past has been Enterprise Risk Management, which involved performing Enterprise Risk Assessments of E-rate program risks, including fraud risks, as required by OMB A-123 guidance.[42] USAC officials said that in the past, USAC included fraud risks in its broader Enterprise Risk Assessment. FCC and USAC officials noted that fraud risk is part of

[42] Office of Management and Budget, *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*, OMB Memorandum M-16-17 (Washington, D.C.: July 2016).

overall enterprise risk, and there are fraud aspects included in the risk assessments that they have conducted. The Fraud Risk Framework acknowledges that agencies may use initiatives like Enterprise Risk Management efforts to assess their fraud risks, but it does not eliminate the separate and independent fraud risk management requirements.

These efforts, however, do not encompass the key elements of the fraud risk assessment process, as we previously discussed. Additionally, in its fiscal year 2019 agency financial report, FCC reported that it is aware more needs to be done to improve fraud risk management of the E-rate program, including developing a program-specific fraud risk assessment and fraud risk profile. FCC officials said that they are currently developing an entity-wide fraud risk assessment and fraud risk profile of all USF programs, and will then move on to program-specific fraud risk assessments and fraud risk profiles tailored to each of the USF programs, including E-rate. FCC officials also said they have plans to conduct a fraud risk assessment and develop a fraud risk profile tailored to the E-rate program by the end of 2021. In addition, FCC officials told us that they plan to incorporate USAC's E-rate program fraud risk assessment, which USAC will develop, into FCC's fraud risk assessment, tailoring it as appropriate. FCC officials said that because USAC's function (i.e., program administration) is different than FCC's (i.e., policy-making and oversight), the fraud risk assessments should be tailored to reflect those differences.

USAC officials told us that they plan to use GAO's Fraud Risk Framework as a set of criteria to complete program-specific fraud risk assessments for all USF programs on a rolling basis. USAC officials informed us that, as of May 2020, they have posted a Request for Proposal to engage an outside vendor to complete a fraud risk assessment for FCC's high-cost program, which is their pilot program for this effort.[43] Once the contract is awarded to a vendor, the vendor is expected to take 6 months to complete the fraud risk assessment and fraud risk profile for the high-cost program. USAC expects this to be completed in 2021. Following this work on the high-cost program, USAC plans to complete a fraud risk assessment and determine a fraud risk profile tailored to the E-rate

[43] USAC officials said that the outside vendor is expected to have fraud risk assessment experience, including experience with implementing leading practices from the Fraud Risk Framework. USAC posted this Request for Proposal in May 2020. Offers are due in June 2020 and USAC expects to award a contract in August 2020.

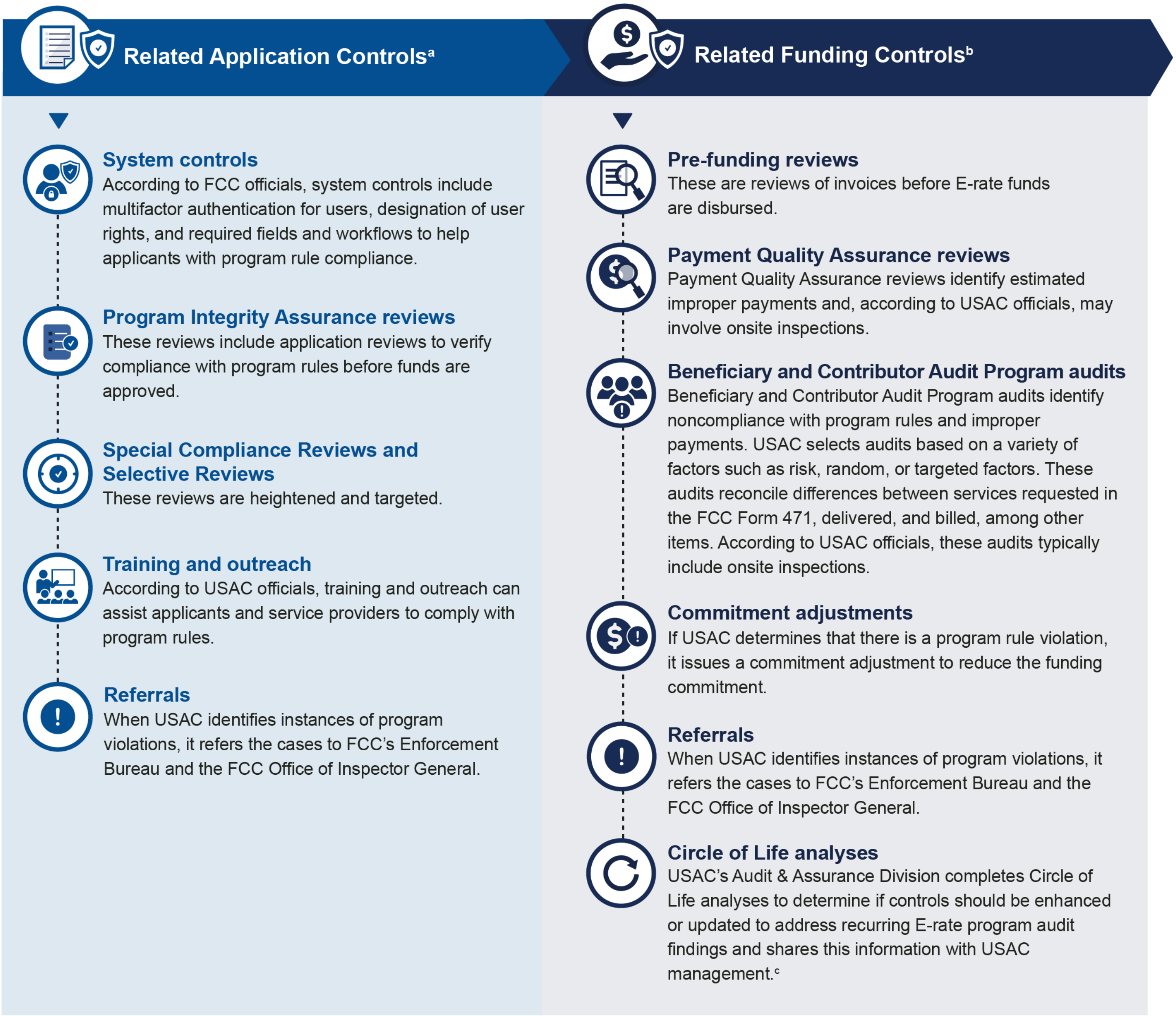
program by the end of 2021. As of March 2020, USAC's Fraud Risk Group plans on completing the E-rate program's fraud risk assessment process using the high-cost program's fraud risk assessment as a guide and pulling information from other sources, including FCC's Enforcement Bureau.[44]

Although FCC and USAC have yet to conduct a fraud risk assessment tailored to the E-rate program, according to USAC officials, the controls (policies and procedures) listed in figure 9 below, among others, were designed to ensure compliance with FCC rules, but they can also help address key fraud risks affecting the application or funding phases.[45]

[44] Depending on their experience with the vendor's completion of the high-cost program fraud risk assessment, USAC officials said that they may continue to engage the outside vendor for the E-rate program fraud risk assessment.

[45] This is not an exhaustive list of policies or procedures that FCC or USAC designed to ensure compliance with E-rate program application or funding rules and address key fraud risks we describe in this report. We did not independently evaluate the extent to which these related controls were effectively and efficiently addressing fraud risks during the application or funding phases as such work was outside the scope of our review.

Figure 9: Examples of Related E-rate Program Application and Funding Controls



Related Application and Funding Controls

Related Application Controls[a]

System controls
According to FCC officials, system controls include multifactor authentication for users, designation of user rights, and required fields and workflows to help applicants with program rule compliance.

Program Integrity Assurance reviews
These reviews include application reviews to verify compliance with program rules before funds are approved.

Special Compliance Reviews and Selective Reviews
These reviews are heightened and targeted.

Training and outreach
According to USAC officials, training and outreach can assist applicants and service providers to comply with program rules.

Referrals
When USAC identifies instances of program violations, it refers the cases to FCC's Enforcement Bureau and the FCC Office of Inspector General.

Related Funding Controls[b]

Pre-funding reviews
These are reviews of invoices before E-rate funds are disbursed.

Payment Quality Assurance reviews
Payment Quality Assurance reviews identify estimated improper payments and, according to USAC officials, may involve onsite inspections.

Beneficiary and Contributor Audit Program audits
Beneficiary and Contributor Audit Program audits identify noncompliance with program rules and improper payments. USAC selects audits based on a variety of factors such as risk, random, or targeted factors. These audits reconcile differences between services requested in the FCC Form 471, delivered, and billed, among other items. According to USAC officials, these audits typically include onsite inspections.

Commitment adjustments
If USAC determines that there is a program rule violation, it issues a commitment adjustment to reduce the funding commitment.

Referrals
When USAC identifies instances of program violations, it refers the cases to FCC's Enforcement Bureau and the FCC Office of Inspector General.

Circle of Life analyses
USAC's Audit & Assurance Division completes Circle of Life analyses to determine if controls should be enhanced or updated to address recurring E-rate program audit findings and shares this information with USAC management.[c]

Source: GAO analysis of FCC and USAC information. | GAO-20-606

[a] We define application controls to include controls related to the application process that can occur before E-rate program funds are committed.

[b] We define funding controls to include controls related to the funding process that can occur before or after E-rate program funds are disbursed.

[c] USAC officials said that the Circle of Life initiative is designed to improve program integrity by identifying common audit findings from the Payment Quality Assurance reviews and Beneficiary and Contributor Audit Program audits after funding is disbursed, identifying the root causes, and developing corrective action plans to address those root causes. Since 2014, many of these recurring audit findings have involved issues that pertain to some of key fraud risks described in this report, including issues pertaining to opportunities to violate or circumvent competitive-bidding requirements. USAC's corrective action plans aim to reduce future instances and improper payments and generally involve immediate improvements to address control gaps such as updated or implemented guidance, technology, and training. However, USAC officials acknowledged that this remains an area within the E-rate program that they are committed to taking additional steps to ensure the effectiveness of the developed corrective action plans.

While USAC officials told us that related controls used to ensure compliance with program rules can also be used to address some of the key fraud risks we identified, such controls were not developed from a fraud risk-based approach. According to USAC officials, once the fraud risk assessment of the E-rate program is completed, USAC plans to use the results to design and implement controls to address identified fraud risks, consistent with the Fraud Risk Framework's leading practices. Six months after these controls are implemented, USAC officials plan to evaluate how the controls, designed and implemented as a result of the fraud risk assessment, are working and then make any adjustments, if needed. USAC plans to repeat this process every one to 5 years.

Although both FCC and USAC have established plans with time frames for conducting fraud risk assessments of the E-rate program and determining the program's fraud risk profile, USAC has not consistently implemented recommendations related to fraud risk management in the past. As mentioned above, it has taken USAC 5 years to take preliminary steps to implement its contractor's recommendation to perform a comprehensive fraud risk assessment of the E-rate program. In addition, USAC has taken 3 years to begin to implement the FCC OIG's recommendation to develop a competitive-bidding portal for the E-rate program. Moreover, the key fraud risks identified continue to persist throughout the E-rate program and FCC's annual agency financial reports from 2014 through 2019 highlight a number of these key fraud risks as recurring management challenges affecting the E-rate program.

FCC and USAC could help ensure that they are prioritizing key fraud risks that persist in the E-rate program by implementing their respective plans, and following planned time frames, to conduct fraud risk assessments and determine fraud risk profiles for the E-rate program by the end of 2021. Also, by comprehensively assessing fraud risks, including examining the suitability of existing controls and prioritizing residual risks, FCC and USAC would have greater assurance as to whether current control activities are efficiently and effectively addressing the most significant E-rate program fraud risks within an established tolerable level, or whether additional fraud controls or adjustments are needed to help mitigate the disbursement of potentially fraudulent E-rate program funding. Such information is necessary to appropriately design and implement an antifraud strategy and evaluate and adapt the strategy and controls to improve fraud risk management in the E-rate program.

FCC and USAC Face Challenges in Effectively Employing Data Analytics to Support Future Fraud Risk Management Activities

GAO's Fraud Risk Framework calls for agencies to design and implement control activities, including data-analytics activities, to prevent and detect fraud.[46] These data-analytics activities can also help inform broader fraud risk management efforts including fraud risk assessments. Leading practices for data-analytics activities include:

- conducting data matching to verify key information, including self-reported data and information necessary to determine eligibility;
- conducting data mining to identify suspicious activity or transactions, including anomalies, outliers, and other red flags in the data; and
- automating data-analytic tests to monitor data for fraud indicators on a continuous, real-time basis.

FCC and USAC officials said that they are or will be using data analytics for fraud risk management. However, they have not implemented leading practices for data-analytics activities nor documented their efforts or plans for doing so. For example, USAC officials told us that they can currently perform certain data analytics to identify potential fraud and program violations. For instance, they said that they can mine the data to identify service providers who exhibit unique characteristics that may indicate higher fraud risk. USAC officials also said that they can analyze the data to identify outliers or to flag groups of applications, which can then be reviewed and investigated further. However, they have not automated these data-analytic tests to monitor data on a continuous, real-time basis, nor have they documented a plan that outlines their data-analytics strategy as part of their fraud risk management efforts. USAC officials said that as they develop their data analytics plans, they are exploring

[46] GAO-15-593SP.

how best to leverage their tools to support more robust data-analytic capabilities.

Additionally, FCC Enforcement Bureau officials told us that the agency is developing a data-based process to assist with investigations. FCC officials said that this process will enable the agency to access E-rate program data to obtain information on ongoing Enforcement Bureau cases. It will also allow the Enforcement Bureau to identify program violations and potential fraud. However, FCC has not specified the data-analytics tests that it will use with the data-based process, nor has it documented a plan that outlines its data-analytics strategy as part of its fraud risk management efforts. FCC officials said that their future plans include developing a predictive data-analytics tool, but they have not documented the analytics that the tool will perform or a time frame for developing it. According to GAO's Fraud Risk Framework, predictive-analytics can enable agencies to identify fraud before they make payments, rather than detecting fraudulent transactions and attempting to recover funds after payment.[47]

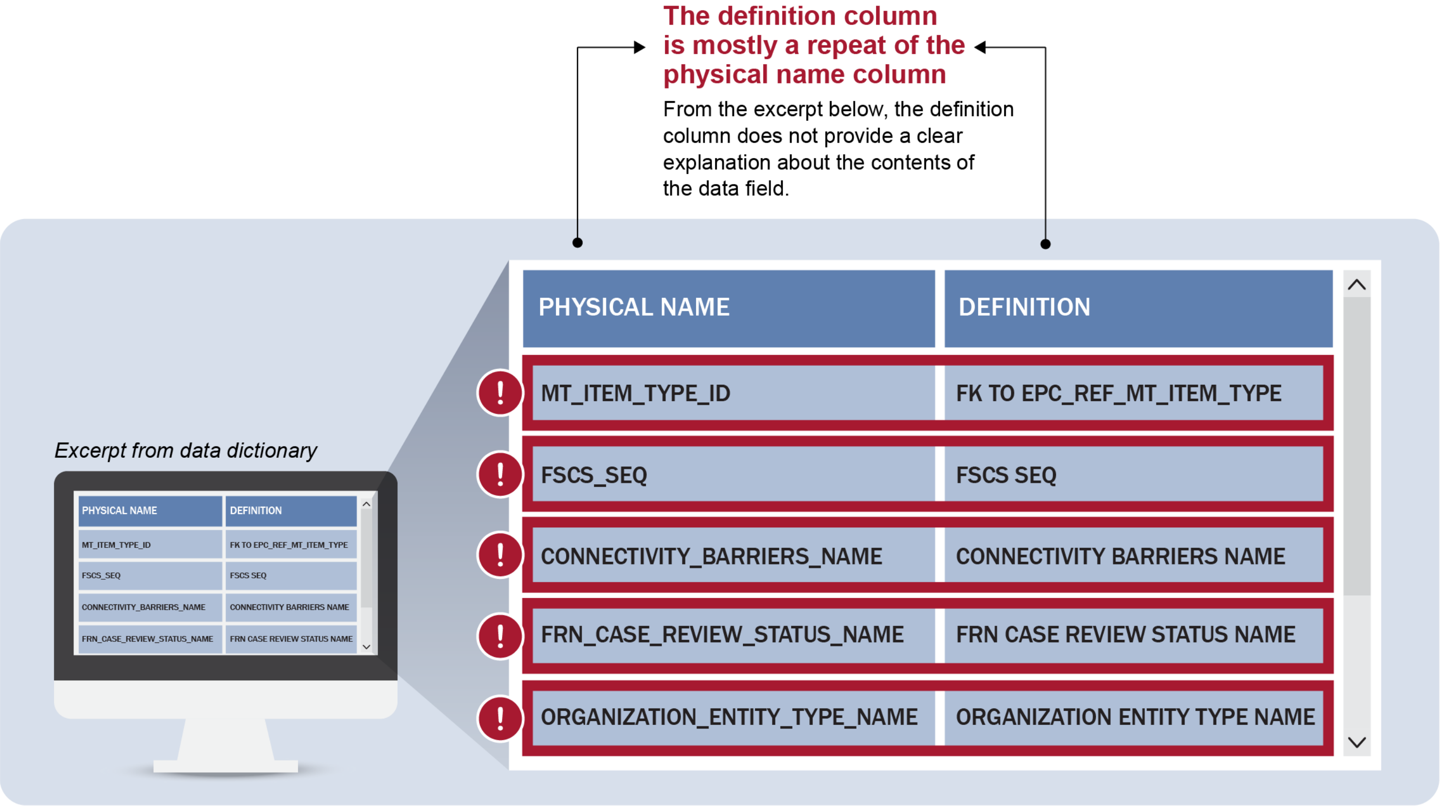
GAO's Fraud Risk Framework also calls for agencies to develop, document, and communicate an antifraud strategy to employees and stakeholders that describes the program's activities for preventing, detecting, and responding to fraud, as well as monitoring and evaluation. Having FCC and USAC implement leading practices for data analytics and document how data-analytics activities will be used in their antifraud strategies could position them to better prevent, detect, and respond to fraud in the E-rate program. For example, earlier in this report, we described key fraud risks associated with self-certification statements pertaining to the accuracy of application and funding information. This key fraud risk could potentially be mitigated by FCC and USAC developing and documenting plans for using data analytics to prevent and detect fraud. For example, USAC could conduct data matching with third-party data—such as National School Lunch Program data—to verify the applicant's self-reported information to determine program eligibility. USAC could also automate data-analytics tests to identify unusual patterns or outliers in the application or invoice data on a continuous, real-time basis; such patterns or outliers could then be investigated further.

[47] GAO-15-593SP.

In addition, FCC faces challenges in effectively and efficiently employing data analytics for fraud risk management activities in part because USAC does not have complete documentation related to the computer systems it uses to administer the E-rate program.[48] Computer system documentation can include data dictionaries. Data dictionaries generally contain information on the data fields in the system, their definitions, descriptions, and range of potential values. However, USAC's E-rate program data dictionaries do not provide clear definitions for all fields in its systems. For example, the system USAC uses for processing E-rate program applications contains over 10,000 data fields, including roughly 1,000 fields that USAC officials told us are key business fields that they use to administer the program. However, as illustrated in figure 10, this data dictionary does not provide an explanation about what the data fields should contain as part of the field definition.

[48] USAC primarily uses two systems to administer the E-rate program: (1) one system to process applications since 2016—EPC, and (2) another system to process invoices—the Invoice Streamlined Tracking and Application Review system. The latter system is also used to process actions related to applications submitted prior to 2016.

Figure 10: Example of Key Business Fields That Do Not Provide Clear Definitions, in an E-rate Program Data Dictionary


The definition column is mostly a repeat of the physical name column

From the excerpt below, the definition column does not provide a clear explanation about the contents of the data field.

PHYSICAL NAME	DEFINITION
MT_ITEM_TYPE_ID	FK TO EPC_REF_MT_ITEM_TYPE
FSCS_SEQ	FSCS SEQ
CONNECTIVITY_BARRIERS_NAME	CONNECTIVITY BARRIERS NAME
FRN_CASE_REVIEW_STATUS_NAME	FRN CASE REVIEW STATUS NAME
ORGANIZATION_ENTITY_TYPE_NAME	ORGANIZATION ENTITY TYPE NAME

Source: GAO analysis of USAC information. | GAO-20-606

FCC officials told us that the lack of data field definitions can make it difficult to fully understand and use the data to manage fraud risks in the program. For example, FCC officials did not know if there are data that USAC is not currently collecting or analyzing that would be helpful in managing fraud risks. FCC officials told us that as the agency is developing a data-based process and obtaining E-rate program data from USAC, officials have had to consult with USAC frequently to understand the data and get the data they need. In addition, an official from the FCC OIG's Office of Investigations told us that the lack of a comprehensive data dictionary has made reviewing the data more difficult and negatively affected the office's ability to work efficiently, as it has had to hold discussions with USAC to get answers to its questions about the data.

We also experienced challenges in using the data. We obtained the E-rate program data dictionaries from USAC because we initially planned to request data and perform data analytics to identify potential fraud risks. For example, we planned to analyze the data to identify applicants' consultants that consistently select the same service provider, a finding that could serve as indicators of potential conflicts of interest and misrepresentation regarding the true extent of representation the consultants were providing applicants and service providers within the same transactions. However, the lack of field definitions made it difficult to understand the contents of the fields, creating a challenge for us to formulate our data request in a timely manner without extensive coordination with USAC officials. Further compounding potential delays, the analytics we planned to perform would have required us to take an iterative approach and to continue to refine our analysis to identify potential red flags— a process that can take a considerable amount of time. Ultimately we determined that it would not be feasible to obtain and analyze the data within our reporting timeframe, so we elected to exclude this work from our audit scope.

USAC officials cited resource and capacity constraints and other priorities as the reasons for why they have not developed a data dictionary that details the contents of all data fields. They further told us that USAC has dedicated staff who are familiar with the data systems and can provide guidance and training to new users as needed. Nevertheless, having USAC document the definitions of the data fields in the E-rate program systems could help improve FCC's ability to understand and use the data to manage fraud risks. Federal internal control standards state that management develops and maintains documentation of its internal control system.[49] Effective documentation assists in management's design of internal control by establishing and communicating the "who, what, when, where, and why" of internal control execution to personnel. Documentation provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel, as well as a means to communicate that knowledge as needed to external parties, such as external auditors.

Conclusions

The E-rate program provides a significant source of technology funding for schools and libraries to obtain affordable broadband and telecommunications services. Our review identified a number of key fraud risks in the E-rate program, some of which involved fraud documented in adjudicated court cases such as a case in which E-rate program participants pled guilty to conspiring to defraud the program based on the

[49] GAO-14-704G.

submission of false certifications and agreed to pay more than $2.6 million in restitution. FCC and USAC have not comprehensively assessed the E-rate program's fraud risks, consistent with the Fraud Risk Framework's leading practices, which potentially allowed these key fraud risks to impair FCC's oversight efforts and USAC's administration of the E-rate program for at least a half decade. Specifically, while both entities have plans to do so, neither FCC nor USAC have yet conducted regular fraud risk assessments of the E-rate program. Regular fraud risk assessments are a pivotal step in managing fraud risks and designing an antifraud strategy for addressing them, helping to ensure that FCC's and USAC's key oversight efforts and antifraud controls are targeted at areas at greatest risk for fraud in the E-rate program, and helping safeguard program resources and allocate them to legitimate recipients. Yet, as of June 2020, USAC has not implemented a contractor's 2015 recommendation that an external entity conduct a fraud risk assessment of the E-rate program. Furthermore, neither FCC nor USAC have sufficiently developed or documented plans for using data analytics to manage fraud risks, nor has USAC defined the data used to ensure compliance with program rules. The lack of definitions has created inefficiencies for FCC as it is developing a data-based process to assist with investigations and could lead to further inefficiencies as FCC continues developing a predictive data-analytics tool that will be used for oversight and antifraud efforts. Not taking timely corrective action to improve fraud risk management, including to address these long-standing, recurring fraud risks, could lead to missed opportunities to efficiently and effectively prevent, detect, and respond to potential E-rate program fraud and its financial impact of diverting funds to ineligible program participants.

Recommendations for Executive Action

We are making the following three recommendations to FCC:

The Chairman of FCC should direct and coordinate with the Chief Executive Officer of USAC to comprehensively assess fraud risks to the E-rate program, including implementing their respective plans for developing periodic fraud risk assessments, examining the suitability of existing fraud controls, and compiling fraud risk profiles following the timelines described in this report. The assessments should be informed by the key fraud risks identified in this report from closed court cases, prior risk assessments, and OIG reports, among other sources. (Recommendation 1)

The Chairman of FCC should ensure that FCC and USAC follow the leading practices in GAO's Fraud Risk Framework when designing and implementing data-analytics activities to prevent and detect fraud as part of their respective antifraud strategies for the E-rate program. (Recommendation 2)

The Chairman of FCC should direct the Chief Executive Officer of USAC to clearly define and fully document the data fields in all relevant E-rate program computer systems to help improve FCC's ability to understand and use data to manage fraud risks. (Recommendation 3)

Agency Comments

We provided a draft of this report to FCC for review and comment. In its comments, reproduced in appendix I, FCC agreed with our recommendations and described actions it would take to implement them. FCC also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Chairman of FCC, and other interested parties. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

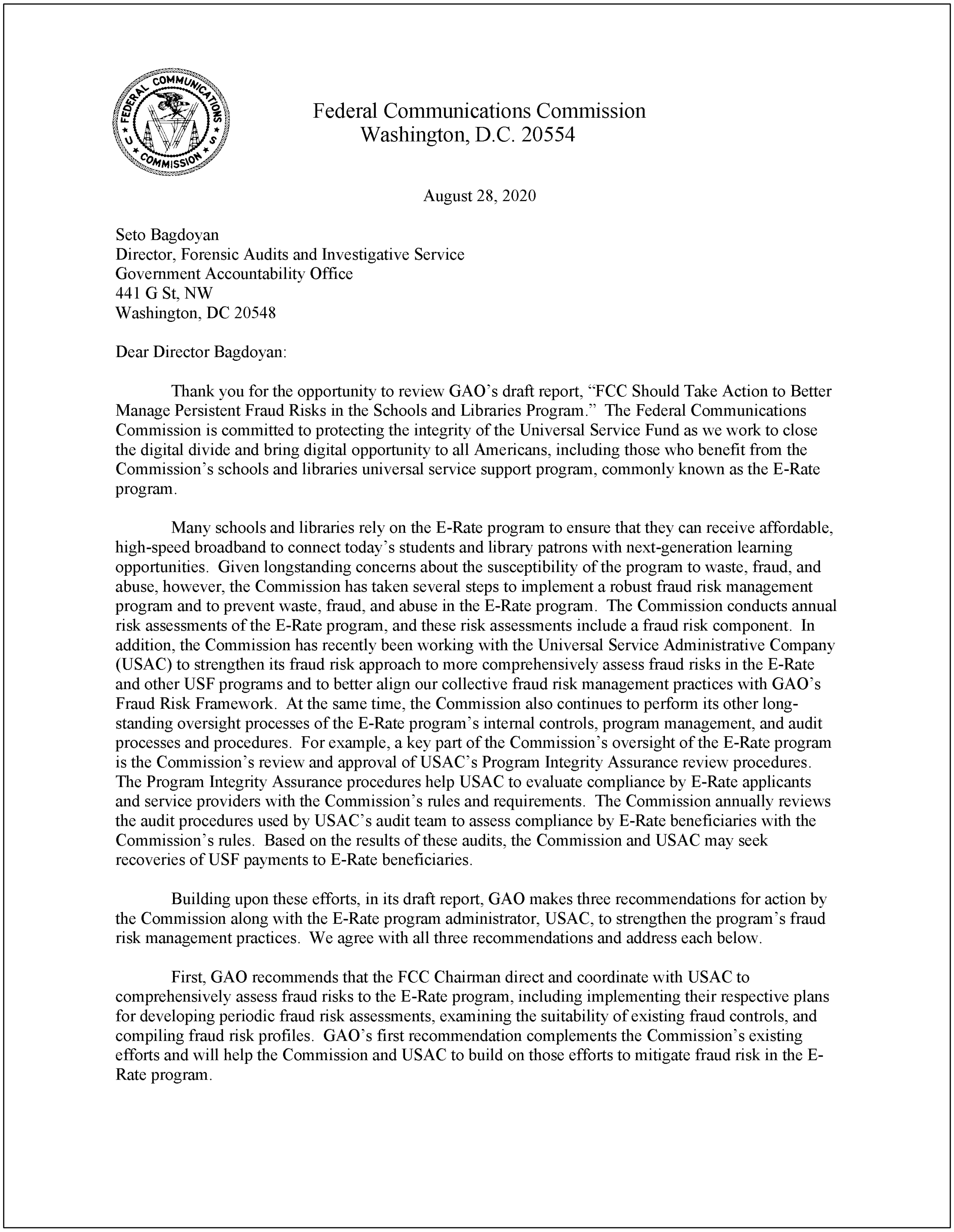
If you or your staff have any questions about this report, please contact me at (202) 512-6722 or bagdoyans@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs are on the last page of this report. GAO staff who made key contributions to this report are listed in appendix II.

Sincerely yours,

Seto J. B

Seto J. Bagdoyan
Director
Forensic Audits and Investigative Service

Appendix I: Comments from the Federal Communications Commission



Federal Communications Commission
Washington, D.C. 20554

August 28, 2020

Seto Bagdoyan
Director, Forensic Audits and Investigative Service
Government Accountability Office
441 G St, NW
Washington, DC 20548

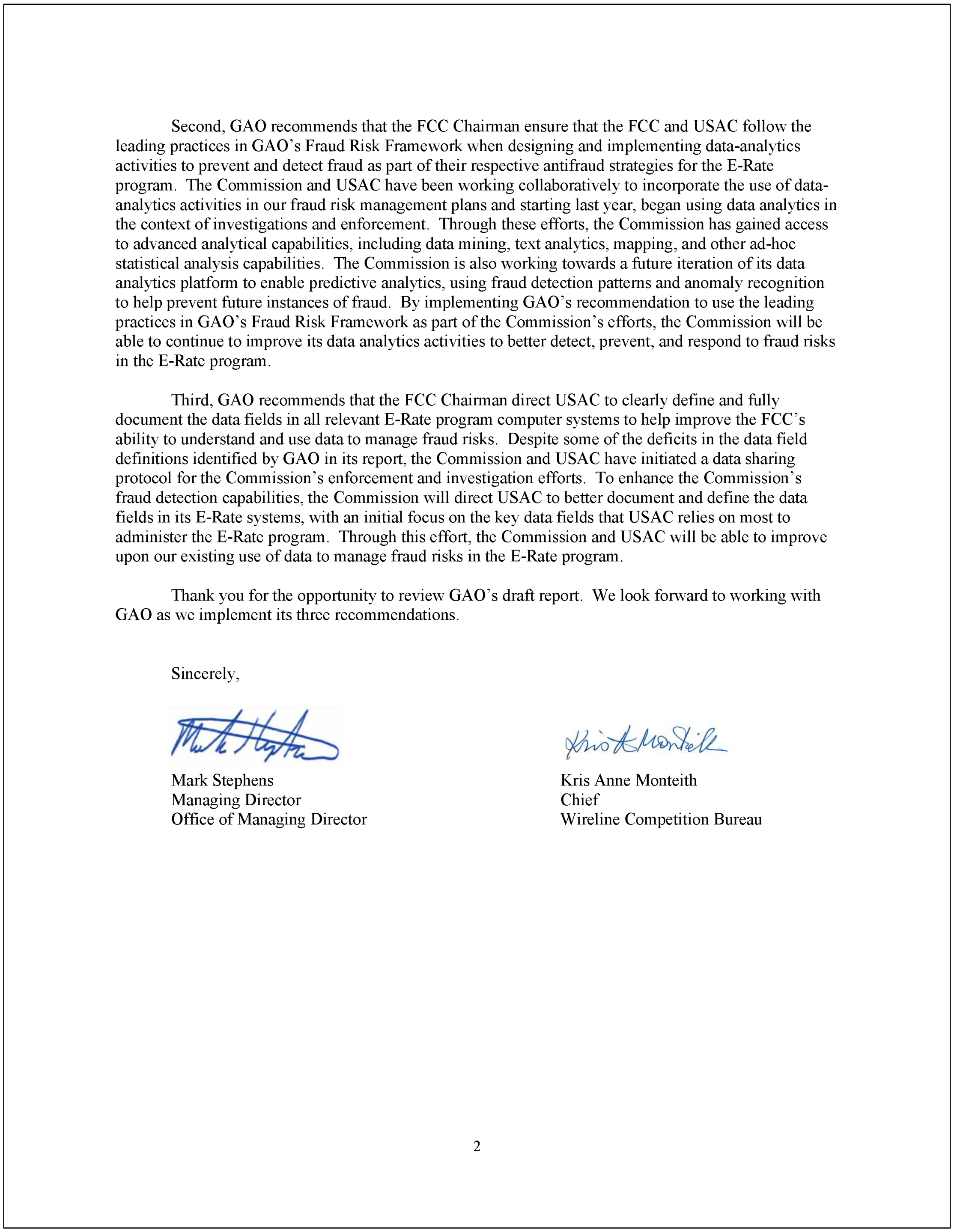
Dear Director Bagdoyan:

Thank you for the opportunity to review GAO's draft report, "FCC Should Take Action to Better Manage Persistent Fraud Risks in the Schools and Libraries Program." The Federal Communications Commission is committed to protecting the integrity of the Universal Service Fund as we work to close the digital divide and bring digital opportunity to all Americans, including those who benefit from the Commission's schools and libraries universal service support program, commonly known as the E-Rate program.

Many schools and libraries rely on the E-Rate program to ensure that they can receive affordable, high-speed broadband to connect today's students and library patrons with next-generation learning opportunities. Given longstanding concerns about the susceptibility of the program to waste, fraud, and abuse, however, the Commission has taken several steps to implement a robust fraud risk management program and to prevent waste, fraud, and abuse in the E-Rate program. The Commission conducts annual risk assessments of the E-Rate program, and these risk assessments include a fraud risk component. In addition, the Commission has recently been working with the Universal Service Administrative Company (USAC) to strengthen its fraud risk approach to more comprehensively assess fraud risks in the E-Rate and other USF programs and to better align our collective fraud risk management practices with GAO's Fraud Risk Framework. At the same time, the Commission also continues to perform its other long-standing oversight processes of the E-Rate program's internal controls, program management, and audit processes and procedures. For example, a key part of the Commission's oversight of the E-Rate program is the Commission's review and approval of USAC's Program Integrity Assurance review procedures. The Program Integrity Assurance procedures help USAC to evaluate compliance by E-Rate applicants and service providers with the Commission's rules and requirements. The Commission annually reviews the audit procedures used by USAC's audit team to assess compliance by E-Rate beneficiaries with the Commission's rules. Based on the results of these audits, the Commission and USAC may seek recoveries of USF payments to E-Rate beneficiaries.

Building upon these efforts, in its draft report, GAO makes three recommendations for action by the Commission along with the E-Rate program administrator, USAC, to strengthen the program's fraud risk management practices. We agree with all three recommendations and address each below.

First, GAO recommends that the FCC Chairman direct and coordinate with USAC to comprehensively assess fraud risks to the E-Rate program, including implementing their respective plans for developing periodic fraud risk assessments, examining the suitability of existing fraud controls, and compiling fraud risk profiles. GAO's first recommendation complements the Commission's existing efforts and will help the Commission and USAC to build on those efforts to mitigate fraud risk in the E-Rate program.



Second, GAO recommends that the FCC Chairman ensure that the FCC and USAC follow the leading practices in GAO's Fraud Risk Framework when designing and implementing data-analytics activities to prevent and detect fraud as part of their respective antifraud strategies for the E-Rate program. The Commission and USAC have been working collaboratively to incorporate the use of data-analytics activities in our fraud risk management plans and starting last year, began using data analytics in the context of investigations and enforcement. Through these efforts, the Commission has gained access to advanced analytical capabilities, including data mining, text analytics, mapping, and other ad-hoc statistical analysis capabilities. The Commission is also working towards a future iteration of its data analytics platform to enable predictive analytics, using fraud detection patterns and anomaly recognition to help prevent future instances of fraud. By implementing GAO's recommendation to use the leading practices in GAO's Fraud Risk Framework as part of the Commission's efforts, the Commission will be able to continue to improve its data analytics activities to better detect, prevent, and respond to fraud risks in the E-Rate program.

Third, GAO recommends that the FCC Chairman direct USAC to clearly define and fully document the data fields in all relevant E-Rate program computer systems to help improve the FCC's ability to understand and use data to manage fraud risks. Despite some of the deficits in the data field definitions identified by GAO in its report, the Commission and USAC have initiated a data sharing protocol for the Commission's enforcement and investigation efforts. To enhance the Commission's fraud detection capabilities, the Commission will direct USAC to better document and define the data fields in its E-Rate systems, with an initial focus on the key data fields that USAC relies on most to administer the E-Rate program. Through this effort, the Commission and USAC will be able to improve upon our existing use of data to manage fraud risks in the E-Rate program.

Thank you for the opportunity to review GAO's draft report. We look forward to working with GAO as we implement its three recommendations.

Sincerely,

Mark Stephens
Managing Director
Office of Managing Director

Kris Anne Monteith
Chief
Wireline Competition Bureau

2

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Seto J. Bagdoyan, (202) 512-6722 or bagdoyans@gao.gov

Staff Acknowledgments

In addition to the contact named above, Gabrielle M. Fagan (Assistant Director), Flavio Martinez (Analyst-in-Charge), Ranya Elias, and Tamera Lockley made key contributions to this report. Also contributing to the report were Pamela Davidson, Colin Fallon, Barbara Lewis, Maria McMullen, Sabrina Streagle, and Charles Truxillo.

(103480)

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