May 16, 2024

FCC FACT SHEET*

Schools and Libraries Cybersecurity Pilot Program

Report and Order – WC Docket No. 23-234

Background: Schools and libraries have been subject to increased cyberattacks by malicious actors to steal personal information, compromise online accounts, cause online personal harm or embarrassment, and otherwise disable critical networks that provide broadband connectivity. This item would establish the Schools and Libraries Cybersecurity Pilot Program (Pilot Program), modeled after the Connected Care Pilot Program, to study the effectiveness of using universal service funding to support cybersecurity services and equipment to protect school and library broadband networks.

What the Report and Order Would Do:

- Adopt final rules for a three-year Pilot Program.
- Provide up to $200 million in Universal Service Fund support available to participating eligible schools and libraries to defray the costs of eligible cybersecurity services and equipment.
- Allow a diverse array of eligible schools and libraries to apply to be selected as participants in the Pilot Program. Applications will be evaluated and participants will be selected on the basis of applicant type, discount rate, and the strength of the proposed projects contained in the applications.
- Leverage many of the existing forms, rules, and processes from the E-Rate, Emergency Connectivity Fund (ECF), and Connected Care Pilot programs. These rules and procedures cover all aspects of the Pilot, including seeking competitive bids, requesting eligible services and equipment, and submitting requests for reimbursement.
- Adopt robust program integrity protections, including competitive bidding, document retention, audits, restrictions on gifts, and suspension and debarment of bad actors.
- Designate the Universal Service Administrative Company (USAC) as the Administrator of the Pilot Program.
- Establish performance goals and data reporting requirements to track and measure the effectiveness of the Pilot Program.

* This document is being released as part of a "permit-but-disclose" proceeding. Any presentations or views on the subject expressed to the Commission or its staff, including by email, must be filed in WC Docket No. 23-234, which may be accessed via the Electronic Comment Filing System (https://www.fcc.gov/ecfs/). Before filing, participants should familiarize themselves with the Commission's *ex parte* rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. *See* 47 CFR § 1.1200 *et seq.*

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Schools and Libraries Cybersecurity Pilot Program	)	WC Docket No. 23-234
	)	

REPORT AND ORDER*

Adopted: [] **Released: []**

By the Commission:

TABLE OF CONTENTS

* This document has been circulated for tentative consideration by the Commission at its June open meeting. The issues referenced in this document and the Commission's ultimate resolution of those issues remain under consideration and subject to change. This document does not constitute any official action by the Commission. However, the Chairwoman has determined that, in the interest of promoting the public's ability to understand the nature and scope of issues under consideration, the public interest would be served by making this document publicly available. The FCC's *ex parte* rules apply and presentations are subject to "permit-but-disclose" *ex parte* rules. *See, e.g.*, 47 C.F.R. §§ 1.1206, 1.1200(a). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. *See* 47 CFR §§ 1.1200(a), 1.1203.

I. INTRODUCTION

1. As broadband connectivity and Internet access have become essential for K-12 students and adults alike, the security and safety of that access has likewise become paramount. Whether for online learning, job searching, or connecting with peers and the community, high-speed broadband is critical to educational, professional, and personal success in the modern world. Although broadband connectivity and Internet access can simplify and enhance the education and daily lives of K-12 students, school staff, and library patrons, they can also be used by malicious actors to steal personal information, compromise online accounts, and cause online personal harm or embarrassment. In response to the growing importance of cybersecurity to broadband connectivity and Internet access for K-12 schools and libraries, and in light of the increase in cyberattacks to disrupt or disable these critical networks, the Federal Communications Commission (Commission or FCC) adopts a three-year pilot program within the Universal Service Fund (USF or Fund) to provide up to $200 million to support cybersecurity services and equipment for eligible schools and libraries.

2. The Schools and Libraries Cybersecurity Pilot Program (Pilot or Pilot Program) is a critical next step to evaluate whether, and to what extent, the Commission should leverage the USF to support the cybersecurity needs of schools and libraries. By proceeding via a short-term Pilot Program, the Commission can gather key data on the types of cybersecurity services and equipment that K-12 schools and libraries need to protect their broadband networks and securely connect students, school staff, and library patrons to advanced communications that are integral to education. The Pilot Program will evaluate whether supporting cybersecurity services and equipment with universal service funds advances the key universal service principles of providing quality Internet and broadband services to K-12 schools and libraries at just, reasonable, and affordable rates; and ensuring schools' and libraries' access to advanced telecommunications. Importantly, the Pilot Program will also enable the Commission to better estimate the costs of supporting cybersecurity services and equipment via the USF, which will help inform future decisions on how to best utilize the USF to support the connectivity and network security needs of K-12 schools and libraries. Data and information collected through this Pilot Program may also aid in the considerations of broader efforts across the government to help schools and libraries address their cybersecurity concerns. In this regard, we note that other federal partners, including the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Department of Education (Education Department), have jurisdiction and deep expertise on cybersecurity matters, and we expect continued interagency coordination will enable us to leverage their knowledge and resources to explore how the Commission can contribute to addressing the cybersecurity needs of K-12 schools and libraries.

3. Eligible schools and libraries will be able to request and receive support through the Pilot Program to purchase a wide range of qualifying cybersecurity services and equipment that best suit their particular needs. To ensure that we are able to select a large number of participants for the Pilot Program, we adopt per-student and per-library budgets, subject to a minimum funding floor, as well as an overall funding cap. Additionally, we expect to select a diverse cross-section of schools, libraries, and consortia to participate in the Pilot Program, with a focus on selecting applicants with the greatest need. By selecting a participant pool that reflects large, small, urban, rural, and Tribal schools and libraries, we

expect to gain a better understanding about the cybersecurity needs of a wide range of schools and libraries.

4. In adopting this Pilot Program, we are also mindful of the E-Rate program's longstanding goal of promoting connectivity, as well as our obligation to be a mindful and prudent steward of the Commission's limited universal service funds. To that end, we must balance our actions in this proceeding against competing priorities, bearing in mind that the universal service funds are obtained through assessments collected from telecommunications carriers that are typically passed on to and paid for by U.S. consumers. We acknowledge that, as a limited-term Pilot Program, only a subset of K-12 schools and libraries will likely be selected and receive support to defray their cybersecurity-related costs. And, with a $200 million budget, the Pilot Program will not be able to fund all of the cybersecurity-related needs of the selected Pilot participants. We note that the estimated costs for all types of cybersecurity services may exceed the funding available for this Pilot Program, and we further note that the Pilot participants will not receive 100% reimbursement as they will be required to pay their non-discount share of the costs of the eligible services and equipment. Within this framework, we find that the Pilot Program will serve a vital role in informing the Commission, and broader federal government, as to the most pressing cybersecurity needs of K-12 schools and libraries, and the associated costs, which will enable the Commission and other stakeholders to best address these needs on a long-term basis.

II. BACKGROUND

5. The ongoing proliferation of innovative digital learning technologies, and the need to connect students, teachers, and library patrons to information, jobs, and life-long learning have led to a steady rise in the demand for bandwidth in schools and libraries.[1] However, the shift to modern connectivity has brought with it increased cyber threats and attacks, particularly for K-12 schools and libraries.[2] Recent information shows that such schools and libraries are vulnerable to increased cyber threats and attacks, often leading to the disruption of school and library operations, loss of learning, reductions in available bandwidth, significant monetary losses, and the leaking and theft of students', school staff members', and library patrons' personal information and confidential data.[3] K-12 schools

[1] FCC, *E-Rate: Universal Service Program for Schools and Libraries* (Sept. 15, 2021), https://www.fcc.gov/consumers/guides/universal-service-program-schools-and-libraries-e-rate; *see also* U.S. Department of Education, Office of Educational Technology, K-12 Digital Infrastructure Brief: Adequate and Future Proof (2023), https://tech.ed.gov/files/2023/08/FINAL_Adequate_FutureProof.pdf (ED Adequate and Future Proof Brief) ("The future will keep coming, and with it will be greater demands for bandwidth, devices, and digital learning resources.").

[2] *See, e.g.*, U.S. Government Accountability Office (GAO), Critical Infrastructure Protection Additional Federal Coordination is Needed to Enhance K-12 Cybersecurity at 3-4, 12-16, & n.8 (2022), https://www.gao.gov/assets/gao-23-105480.pdf (GAO K-12 Cybersecurity Report) (discussing detailed research regarding downtime for schools that were victims of ransomware attacks, how lack of financial resources can contribute to a school being targeted for a cyberattack, DDoS and cyberattacks that disrupted student learning and resulted in school closures, and ransomware attacks that resulted in the release of sensitive personal data for more than 500,000 students and school staff members and resulted in significant ransomware payments); *see also* Joe Warminsky, DC-Area School System Says Data of 100,000 People Affected in Ransomware Attack (Feb. 20, 2024), https://therecord.media/md-school-system-says-people-affected-ransomware (noting that the same ransomware attack that breached the personal information of 100,000 people, including the individuals' names, financial account information, and social security numbers, also resulted in a network outage for the Maryland district, which serves about 130,000 students).

[3] *See* CISA, *Cyber Threats to K-12 Remote Learning Education,* https://www.cisa.gov/stopransomware/cyber-threats-k-12-remote-learning-education (last visited Feb. 20, 2024) (discussing the rise in cyber threats and cyberattacks against K-12 educational entities and describing some of the more onerous actions employed by malicious actors); GAO, *As Cyberattacks Increase on K-12 Schools, Here is What's Being Done* (Dec. 1, 2022), https://www.gao.gov/blog/cyberattacks-increase-k-12-schools-here-whats-being-done (noting that the scale and number of cyberattacks against K-12 educational entities increased during COVID-19 and providing examples of how schools are being attacked); K12 Security Information eXchange, *The K-12 Cyber Incident Map*,

(continued….)

and libraries will continue to be prime targets for malicious actors, primarily because they are data-rich environments that tend to lack resources and advanced cybersecurity protections.[4]

6. *Cybersecurity Act of 2021, and Actions by Federal Partners to Address K-12 Cybersecurity Concerns.* In October 2021, the President signed into law the K-12 Cybersecurity Act of 2021, which directed CISA to conduct a study of K-12 cybersecurity risks.[5] In particular, the act directed CISA to evaluate and report on the specific cybersecurity risks that were impacting K-12 educational institutions; the cybersecurity challenges that K-12 educational institutions were facing; cybersecurity challenges related to remote learning; and the most accessible ways to communicate cybersecurity recommendations and tools.[6] CISA published its report in January 2023,[7] recommending that K-12 schools invest in the most impactful security measures;[8] recognize and actively address resource

(Continued from previous page)
https://www.k12six.org/map (last visited Feb. 20, 2024) (categorizing the 1,619 cyberattacks that occurred between 2016 and 2022 by type of attack using an interactive map); Career Charge, *Top 5 K-12 Cybersecurity Threats Schools are Facing* (Jan. 17, 2023), https://corporatetraining.usf.edu/blog/top-5-k-12-cybersecurity-threats-schools-are-facing (explaining that according to the 2019 State of Malware report, education is consistently among the top 10 industries targeted by attackers because schools are data-rich environments, lack IT funding for their infrastructure, provide few cybersecurity professional development opportunities for school staff, and are comprised of students who are tech savvy but lack good cyber hygiene practices); Center for Internet Services, *New MS-ISAC Report Details Cybersecurity Challenges of K-12 Schools* (Nov. 14, 2022), https://www.cisecurity.org/about-us/media/press-release/new-ms-isac-report-details-cybersecurity-challenges-of-k-12-schools (stating that 29% of K-12 MS-ISAC member organizations reported being victims of a cyber incident in the 2021-2022 school year); Will Caverly, Ransomware Attacks at Libraries: How They Happen, What to Do (May 10, 2021), https://publiclibrariesonline.org/2021/05/ransomware-attacks-at-libraries-how-they-happen-what-to-do/ (describing a ransomware attack at the Northampton Public Library that resulted in a two-week closure while the library's IT firm sorted out the malware problems); Kevin Regan, Cyber Risks No Longer Science-Fiction for Libraries (July 19, 2021), https://www.insurancejournal.com/magazines/mag-features/2021/07/19/623028.htm (explaining that the names and addresses stored by libraries may be all attackers need to invade patrons' privacy, and pose a threat to their finances and identity).

[4] Frederick Hess, The Top Target for Ransomware? It's Now K-12 Schools (Sept. 20, 2023), https://www.forbes.com/sites/frederickhess/2023/09/20/the-top-target-for-ransomware-its-now-k-12-schools/?sh=594b9b8a563f (discussing the increase of cyber threats and attacks on schools and characterizing them as "number one on the cybercrime hit list"); Center for Internet Security, *New MS-ISAC Report Details the Cybersecurity Challenges of K-12 Schools* (Nov. 14, 2022), https://www.prnewswire.com/news-releases/new-ms-isac-report-details-cybersecurity-challenges-of-k-12-schools-301675262.html (predicting that "cyber threat actors are highly likely to target K-12 school districts in the remainder of the 2022-2023 school year"); Will Caverly, *Ransomware Attacks at Libraries: How They Happen, What to Do* (May 10, 2021), https://publiclibrariesonline.org/2021/05/ransomware-attacks-at-libraries-how-they-happen-what-to-do/ (noting that "malicious hacking attacks of institutions are on the rise, particularly after the onset of the COVID-19 pandemic" and "[c]orporations, including nonprofits like public libraries, face greater dangers from these attacks").

[5] K-12 Cybersecurity Act, 2021, H.R. 17-122, Pub. L. No. 117-47, 117th Cong., (2021) (enacted), available at https://www.govinfo.gov/content/pkg/BILLS-117s1917enr/pdf/BILLS-117s1917enr.pdf.

[6] *Id*. at § 3(b)(A)-(D).

[7] *See generally* Press Release, CISA, CISA Releases Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats (Jan. 24, 2023), https://www.cisa.gov/news-events/alerts/2023/01/24/cisa-releases-protecting-our-future-partnering-safeguard-k-12; CISA, Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats at 12-18 (2023), https://www.cisa.gov/sites/default/files/2023-01/K-12report_FINAL_V2_508c_0.pdf (CISA K-12 Cybersecurity Report).

[8] CISA K-12 Cybersecurity Report at 1, 3, 12-14. Specifically, the Report recommended that "[i]n an environment of limited resources, [K-12] leaders should leverage security investments to focus on the most impactful steps. K-12 entities should begin with a small number of prioritized investments: deploying multi-factor authentication (MFA), mitigating known exploited vulnerabilities, implementing and testing backups, regularly exercising an incident

(continued….)

constraints;[9] and focus on collaboration and information-sharing by joining groups like the Multi-State Information Sharing and Analysis Center (MS-ISAC)[10] and K-12 Security Information Exchange (K12 SIX),[11] and building long-term relationships with CISA and the Federal Bureau of Investigation (FBI) regional security personnel.[12] Contemporaneously with the report, CISA also released an online toolkit that delved further into the three recommendations, linking each recommendation with key actions and related free or low-cost tools and resources to help K-12 school entities take actions to immediately reduce their cybersecurity risks and mitigate possibilities of cyber-attacks.[13]

7. While CISA's work was underway, the U.S. Government Accountability Office (GAO) was asked by Congress "to (1) determine what is known about the cost impact of cyber incidents on school districts and (2) determine the extent to which key federal agencies coordinate with other federal and nonfederal entities to help K-12 schools combat cyber threats."[14] In October 2022, GAO published its report, which found that additional federal coordination was needed to enhance K-12 school cybersecurity posture,[15] and recommended that the Secretary of Education establish a collaborative mechanism to coordinate cybersecurity efforts among federal agencies and with the K-12 school community; develop metrics to obtain feedback to measure the effectiveness of its cybersecurity products and services for school districts; and coordinate with federal and nonfederal stakeholders to determine how best to help school districts overcome the identified challenges and consider the identified opportunities for addressing cyber threats, as appropriate.[16] Although the GAO report did not recommend any action by the Commission, it discussed the E-Rate program generally, described interviews with FCC officials about the funding of basic firewall services, and named the FCC as a key federal agency that supports the education subsector.[17] More recently, the Education Department released three K-12 Digital

(Continued from previous page)
response plan, and implementing a strong cybersecurity training program. K-12 entities should then progress to fully adopting CISA's Cybersecurity Performance Goals (CPGs) and mature to building an enterprise cybersecurity plan aligned around the NIST Cybersecurity Framework (CSF)." CISA K-12 Cybersecurity Report at 3.

[9] By, for example, leveraging federal, state, and local grant programs; utilizing free or low-cost services; and requiring technology providers to enable strong security controls at no additional charge. *Id.* at 3, 12, 16-17.

[10] Per the GAO, "MS-ISAC is an independent, nonprofit organization that DHS designated in 2010 as the cybersecurity ISAC for state, local, tribal, and territorial governments. It provides services and information sharing to enhance state, local, tribal, and territorial governments' ability to prevent, protect against, respond to, and recover from cyberattacks and compromises." GAO K-12 Cybersecurity Report at 8, n.19.

[11] Per the GAO, "K12 SIX is a national nonprofit information-sharing organization that assists its members from the K-12 community in protecting from cybersecurity threats." GAO K-12 Cybersecurity Report at 2, n.7.

[12] CISA K-12 Cybersecurity Report at 3, 12, 18. Specifically, the CISA report recommended "[i]nformation sharing and collaboration with peers and partners . . . to build awareness and sustain resilience. K-12 entities should participate in an information sharing forum such as the Multi-State Information Sharing and Analysis Center (MS-ISAC) and/or K12 SIX and establish a relationship with CISA and FBI field personnel." *Id.* at 3.

[13] *See generally* CISA, *Online Toolkit: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats*, https://www.cisa.gov/online-toolkit-partnering-safeguard-k-12-organizations-cybersecurity-threats (last visited Nov. 9, 2023) (organizing the toolkit by recommendation, with each recommendation containing a description, applicable actions, and additional resources). CISA derived the toolkit from its broader list of cybersecurity performance goals. *Id.*

[14] *See* GAO K-12 Cybersecurity Report at 1-2.

[15] *See generally* GAO K-12 Cybersecurity Report.

[16] GAO K-12 Cybersecurity Report at 32. GAO did not direct any recommendations to the FCC.

[17] *Id.* at 7-8, 20-21, 28-30, 38, 40, 42-43. The report also notes that in fall 2021 there were in discussions between CISA and the FCC about creating a portfolio of CISA cybersecurity resources that the FCC could direct school districts to use to address their cybersecurity risks and in July 2022 the FCC initiated coordination with the U.S. Department of Education (Education Department), the FBI, and other independent and executive branch regulators (continued….)

Infrastructure Briefs,[18] one of which it co-authored with CISA,[19] to provide K-12 school districts across the country with a starting place to understand the importance of securing their digital infrastructure and the immediate steps they can take to keep their networks and systems safe from cyber threats. In March 2024, the Education Department, in coordination with CISA, launched the Government Coordinating Council (GCC) for the Education Facilities Subsector and appointed the Commission as an ex-officio member.[20]

8. *The E-Rate Program.* The E-Rate program was authorized by Congress as part of the Telecommunications Act of 1996 (1996 Act), and created by the Commission in 1997 to provide connectivity to and within schools and libraries.[21] Through the E-Rate program, eligible schools, libraries, and consortia (comprised of eligible schools and libraries) may request universal service discounts for eligible services and equipment, such as telecommunications services, Internet access, and internal connections.[22] The Commission can designate services eligible for E-Rate support as part of its authority to enhance, to the extent technically feasible and economically reasonable, access to advanced telecommunications and information services for all public and nonprofit elementary and secondary classrooms and libraries.[23]

9. The E-Rate program currently allows reimbursement for some cybersecurity services. The program funds basic firewall service[24] as a category one service but only if the firewall service is

(Continued from previous page)
regarding the E-Rate program. *Id.* at 20. FCC officials also noted that "the cost of covering advanced cybersecurity services for school districts would likely exceed the funding allocations for the [E-Rate] program" noting that a report from the Consortium for School Networking "found it would cost the E-Rate program $2.389 billion annually to fund all K-12 schools with funding for advanced security services." *Id*. at 20. However, the E-Rate program also currently funds over $3 billion for connectivity services to and within eligible schools and libraries, which is the primary purpose of the program. *Id*.

[18] *See* U.S. Department of Education, Office of Educational Technology, Adequate and Future Proof Brief, https://tech.ed.gov/files/2023/08/FINAL_Adequate_FutureProof.pdf; U.S. Department of Education, Office of Educational Technology, K-12 Digital Infrastructure Brief: Privacy Enhancing, Interoperable, and Useful (2023), https://tech.ed.gov/files/2023/08/FINAL_Privacy_Interop_Useful.pdf. *See also* Press Release, U.S. Department of Education, U.S. Department of Education Announces Key K-12 Cybersecurity Resilience Efforts (Aug. 7, 2023), https://www.ed.gov/news/press-releases/department-of-education-announces-k-12-cybersecurity-resilience-efforts.

[19] *See* U.S. Department of Education, Office of Educational Technology & CISA, K-12 Digital Infrastructure Brief: Defensible and Resilient (2023), https://tech.ed.gov/files/2023/08/DOEd-Report_20230804_-508c.pdf.

[20] *See* Press Release, U.S. Department of Education, U.S. Department of Education Launches Government Coordinating Council to Strengthen Cybersecurity in Schools (Mar. 28, 2024), https://www.ed.gov/news/press-releases/us-department-education-launches-government-coordinating-council-strengthen-cybersecurity-schools. Along with several other federal agencies, the Commission is an ex-officio member of the GCC.

[21] Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified at 47 U.S.C. § 151 *et seq.*).

[22] 47 U.S.C. § 254(c)(1), (c)(3), (h)(1)(B), (h)(2)(A). Congress charged the Commission with establishing competitively neutral rules to enhance access to advanced telecommunications and information services for all public and nonprofit elementary and secondary classrooms and libraries, and also provided the Commission with the authority to designate "additional" services eligible for universal service support for schools and libraries. 47 U.S.C. § 254(c)(3), (h)(2)(A).

[23] *Federal-State Joint Board on Universal Service*, CC Docket No. 96-45, Report and Order, 12 FCC Rcd 8776, 9008-15, paras. 436-49 (1997) (*Universal Service First Report and Order*); *see also* 47 U.S.C. § 254(h)(2)(A).

[24] In the E-Rate program, "firewall" is currently defined as a "hardware and software combination that sits at the boundary between an organization's network and the outside world, and protects the network against unauthorized access or intrusions." USAC, *Schools and Libraries (E-Rate) Program Eligible Services List (ESL) Glossary*, https://www.usac.org/wp-content/uploads/e-rate/documents/ESL-Glossary.pdf (last visited Apr. 1, 2024).

provided as part of the vendor's Internet service.[25] In addition, the E-Rate program funds separately-priced basic firewall services and components as a category two service, subject to the applicants' five-year category two budget.[26] Based on funding year (FY) 2023 data, the E-Rate program funded over $179 million in category one requests for data transmission and Internet access services that included basic firewall services, and over $16.5 million in category two requests for basic firewall services and components.[27]

10. The Commission, however, has previously declined to expand E-Rate support for additional cybersecurity services and equipment.[28] For example, in the 2010 *Schools and Libraries Sixth Report and Order*, the Commission declined to extend basic firewall services to include anti-virus and anti-spam software, and intrusion protection and prevention devices that prevent unauthorized access to a school's or library's network.[29] In doing so, the Commission explained that it "must balance the benefits of such protections with the cost of augmenting [the] list of supported services" and "[a]lthough [the Commission] agree[s] that protection from unauthorized access is a legitimate concern, the funds available to support the E-Rate program are constrained."[30] Thus, on balance, the Commission found at the time that "the limited E-Rate funds should not be used to support these services."[31] Next, in the *First 2014 E-Rate Order* the Commission declined to designate network security services, such as intrusion

[25] *See, e.g., Modernizing the E-Rate Program for Schools and Libraries*, WC Docket No. 13-184, Order, DA 22-1313, 37 FCC Rcd 14615, 14625 (WCB Dec. 14, 2022) (*FY 2023 ESL Order*). Category one services include services and equipment needed to support broadband connectivity to schools and libraries. *Modernizing the E-rate Program for Schools and Libraries*, WC Docket No. 13-184, Report and Order and Further Notice of Proposed Rulemaking, 29 FCC Rcd 8870, 8898-8900, paras. 77-78 (2014) (*First 2014 E-Rate Order*).

[26] *See, e.g., FY 2023 ESL Order*, 37 FCC Rcd at 14622. Category two services include services and equipment needed to support broadband connectivity *within* schools and libraries. *First 2014 E-Rate Order*, 29 FCC Rcd at 8898-8899 (designating the services needed to support broadband connectivity *to* schools and libraries as "category one" services and those needed for broadband connectivity *within* schools and libraries as "category two" services).

[27] *See* Letter from Tom Nesbitt, Director of Program Management, E-Rate/ECF Analytics, Appeals, Customer Service, & Risk/Audits, USAC to Trent B. Harkrader, Chief, FCC Wireline Competition Bureau at Attachment (Apr. 15, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/104150165207077.

[28] *See, e.g., Schools and Libraries Universal Support Mechanism, A National Broadband Plan for Our Future*, CC Docket No. 02-6, GN Docket No. 09-51, Sixth Report and Order, 25 FCC Rcd 18762, 18808-18809, para. 105, n.317 (2010) (*Schools and Libraries Sixth Report and Order*) (providing list of the commenters that requested the Commission expand the eligibility of basic firewall services to include other services and devices necessary to protect their broadband networks).

[29] *See, id.*, para. 105.

[30] *See, e.g., id*.

[31] *See, e.g., id*. The Commission reviews several factors when considering adding services to the ESL. Generally, under the Commission's implementation of the statute for the E-Rate program, the Commission considers whether the service serves an educational purpose. *See* 47 U.S.C. § 254(h)(1)(B); *see also Schools and Libraries Sixth Report and Order*, 25 FCC Rcd at 18805, para. 99. Additionally, the Commission considers whether the service is primarily or significantly used to facilitate connectivity. *See Schools and Libraries Sixth Report and Order*, 25 FCC Rcd at 18805, para. 99; 47 U.S.C. § 254(h)(2)(A). And, due to the program's limited funds, the Commission must balance the benefits of particular services with the costs of adding them to the list of supported services. *See* 47 U.S.C. § 254(h)(2)(A); *Schools and Libraries Sixth Report and Order*, 25 FCC Rcd at 18805, para. 99. Section 254(h)(2)(A) of the Communications Act of 1934, as amended, authorizes the Commission to designate services eligible for E-Rate support as part of its authority to enhance, to the extent technologically feasible and economically reasonable, access to advanced telecommunications and information services. 47 U.S.C. § 254(h)(2)(A). Thus, the E-Rate program is not able to fund every service that potentially serves an educational purpose, and for that reason the Commission evaluates the potential impact of funding a particular service on the E-Rate program and the USF when considering whether to add new services to the eligible services list. *See Schools and Libraries Sixth Report and Order*, 25 FCC Rcd at 18805, para. 99.

protection, intrusion detection, and malware protection as eligible for category two support to ensure that such support was targeted efficiently to equipment necessary for broadband connectivity.[32] And in the *2019 Category Two Budget Order*, the Commission again declined E-Rate stakeholder requests to make advanced firewalls and services eligible as part of the category two budget proceeding.[33]

11. *COVID-19 and Cybersecurity Petitions, Eligible Services List Filings, and Public Notice.* During the coronavirus (COVID-19) pandemic, several E-Rate stakeholders requested that the Commission reconsider the eligibility of advanced firewall and network security services. For example, Cisco Systems, Inc. (Cisco) submitted a petition for waiver asking the Commission to raise applicants' category two budgets by 10% and allow category two funding to be used for advanced network security services during the COVID-19 pandemic (i.e., for FYs 2020 and 2021).[34] On February 8, 2021, the Commission received a petition for declaratory ruling and petition for rulemaking from a group of E-Rate program stakeholders[35] requesting that the definition of "firewall" be modified to include all firewall and related features (e.g., next-generation firewall protection, endpoint protection, and advanced security), and that the definition of broadband be updated to include cybersecurity.[36] The petitioners also asked the Commission to increase the current category two budgets to include additional funding for advanced firewall and other network security services.[37] As part of the FY 2023 ESL proceeding, many E-Rate stakeholders requested that the Commission reconsider its earlier eligibility decisions and clarify that advanced or next-generation firewalls and services, as well as other network security services, are eligible for E-Rate support.[38] On November 15, 2022, the Commission also received a proposal from Funds For

[32] *First 2014 E-Rate Order*, 29 FCC Rcd at 8917-18, paras. 120-21 (removing VPNs and all other services under "Data Protection" other than basic firewalls and uninterruptible power supply/battery backup from the FY 2015 Eligible Services List to refocus E-Rate support on internal connections necessary for deploying LANs/WANs); *see also Modernizing the E-Rate Program for Schools and Libraries*, WC Docket No. 13-184, Order, 30 FCC Rcd 9923, 9929, para. 18 (WCB 2015) (*Funding Year 2016 ESL Order*) (declining to expand eligibility of basic firewall services or to add additional network security services to the FY 2016 E-Rate ESL).

[33] *See Modernizing the E-Rate Program for Schools and Libraries*, WC Docket No. 13-184, Report and Order, 34 FCC Rcd 11219, 11236-37, para. 46 & n.123 (2019) (*2019 Category Two Budget Order*) (relying on the *First 2014 E-Rate Order* and explaining that it was focusing "category two funding on the internal connections that are truly necessary to deliver high-speed broadband to students and library patrons via local area networks and wireless local area networks").

[34] Petition of Cisco Systems, Inc. for Waiver, WC Docket No. 13-184, at 1-2, 6 (filed Aug. 20, 2020), https://www.fcc.gov/ecfs/search/search-filings/filing/10820400607480. The Commission did not grant Cisco's Petition for Waiver. Rather, it sought comment on the underlying issues raised in the petition. *See infra* para. 12.

[35] The E-Rate stakeholders included the Consortium for School Networking (CoSN), Alliance for Excellence in Education, State Educational Technology Directors Association (SETDA), Council of the Great City Schools (Council GCS), State E-Rate Coordinators' Alliance (SECA), and Schools, Health & Libraries Broadband Coalition (SHLB Coalition).

[36] Petition of CoSN et al. for Declaratory Relief and Rulemaking Allowing Additional Use of E-Rate Funds for K-12 Cybersecurity, WC Docket No. 13-184, at 2 (filed Feb. 8, 2021) (CoSN 2021 Petition). CoSN, along with Funds For Learning, LLC (FFL), provided a study and the costs associated with adding advanced firewall and other network security services to the E-Rate program and estimated that it would cost the program about $2.389 billion annually to fund these advanced firewall and other network security services for all K-12 schools. *Id.* at 14, Attach. at 4.

[37] *Id.* at 13.

[38] *See Wireline Competition Bureau Seeks Comment on Requests to Allow the Use of E-Rate Funds for Advanced or Next-Generation Firewalls and Other Network Security Services*, WC Docket No. 13-184, Public Notice, DA 22-1315, 2022 WL 17886490, at *7, Appendix A (WCB Dec. 14, 2022) (*December 2022 Public Notice*). During that proceeding, AASA, The School Superintendents Association (AASA) along with 19 other national educational organizations, requested that the Commission take a measured approach in deciding whether to expand the eligibility of advanced firewalls and services, as well as other cybersecurity services. These stakeholders urged the (continued….)

Learning, LLC (FFL) for the Commission to establish a three-year pilot program to fund advanced firewalls and services as a category two service.[39] FFL also proposed that a funding cap of at least $60 million to $120 million be used for each of the three years.[40] FFL further proposed that in the event demand exceeds available funds, the pilot funding be prioritized to the applicants with the highest discount rates, and that the Commission deny funding for the remaining applicants with lower discount rates when the capped pilot funds are exhausted.[41]

12. In response to the cybersecurity petitions, FY 2023 ESL filings, and the proposed FFL pilot cybersecurity program, and in light of the increasing number of cybersecurity threats targeting K-12 schools, the Wireline Competition Bureau (Bureau) issued a Public Notice on December 14, 2022. In the Public Notice, the Bureau sought comment on a variety of topics, including the definition of advanced or next-generation firewalls and services, the specific cybersecurity services and equipment the E-Rate program should fund as advanced or next-generation firewalls and services, the appropriate categorization of the firewalls and services, the Commission's legal authority to extend E-Rate eligibility to the firewalls and services, and the impact that funding the firewalls and services may have on the E-Rate program's longstanding goal of supporting connectivity.[42]

13. Based on the record developed in response to that Public Notice, on November 13, 2023, the Commission released a Notice of Proposed Rulemaking (*Cybersecurity NPRM*), which proposed and sought comment on establishing the Pilot we adopt today.[43] In particular, the *Cybersecurity NPRM* considered whether expanding universal service support to protect schools and libraries from cyber threats and attacks could advance the key universal service principles of providing quality Internet and broadband services to eligible schools and libraries at just, reasonable, and affordable rates and ensure schools' and libraries' access to advanced telecommunications services.[44] It also sought comment on a variety of topics related to the Pilot, including the Pilot application requirements and processes, eligibility

(Continued from previous page)
Commission to work collaboratively with other federal agencies to "determine the products and services that are available and effective in responding to and preventing cyberattacks[;] . . . schools should not be driving the response to cyberattacks, nor should E-Rate, the only federal funding stream supporting connectivity in schools, be repurposed/redirected for this important effort." *See* Letter from AASA, The School Superintendents Association, et al., to Jessica Rosenworcel, Chairwoman, Brendan Carr, Geoffrey Starks, and Nathan Simington, Commissioners, FCC, CC Docket No. 02-6, at 1 (filed Sept. 23, 2022), https://www.fcc.gov/ecfs/document/10923187101919/1 ("E-Rate alone cannot defray the costs of technology and training necessary to secure school and library networks and data.").

[39] *See, e.g.*, Letter from John D. Harrington, Chief Executive Officer, Funds For Learning, LLC to Jessica Rosenworcel, Chairwoman, Brendan Carr, Geoffrey Starks, Nathan Simington, Commissioners, FCC, CC Docket No. 02-6, WC Docket No. 13-184 (filed Nov. 15, 2022), https://www.fcc.gov/ecfs/document/111630719929/1 (FFL Nov. 15 *Ex Parte* Letter); Letter from John D. Harrington, Chief Executive Officer, Funds For Learning, LLC to Marlene H. Dortch, Secretary, FCC, CC Docket No. 02-6, WC Docket No. 13-184 (filed Nov. 21, 2022), https://www.fcc.gov/ecfs/document/1122304899639/1 (FFL Nov. 21 *Ex Parte* Letter); Letter from John D. Harrington, Chief Executive Officer, Funds For Learning, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 02-6, WC Docket No. 13-184 (filed Nov. 23, 2022), https://www.fcc.gov/ecfs/document/112325067454/1 (FFL Nov. 23 *Ex Parte* Letter) (collectively, FFL *Ex Parte* Letters).

[40] FFL Nov. 23 *Ex Parte* Letter at 1.

[41] *Id*. at 2-3.

[42] *See generally December 2022 Public Notice*.

[43] *Schools and Libraries Cybersecurity Pilot Program*, WC Docket No. 23-234, Notice of Proposed Rulemaking, FCC 23-92, 2023 WL 8605080 (Nov. 13, 2023) (*Cybersecurity NPRM*).

[44] *Cybersecurity NPRM,* 2023 WL 8605080 at *1, para. 2.

considerations for Pilot participants,[45] the eligible services and equipment to be funded by the Pilot, the data reporting requirements associated with the Pilot, and the Commission's legal authority to conduct the Pilot and expand E-Rate program support to include cybersecurity services and equipment.[46] Comments were due on January 29, 2024, and replies were due on February 27, 2024. The Commission received approximately 70 filings from a wide array of interested parties, nearly all of whom supported the Pilot Program.

III. DISCUSSION

14. In this Report and Order, we establish a three-year Pilot Program to evaluate whether supporting cybersecurity services and equipment with universal service support could advance the key universal service principles of providing quality Internet and broadband services to K-12 schools and libraries at just, reasonable, and affordable rates; and ensuring schools' and libraries' access to advanced telecommunications as provided by Congress in the 1996 Act.[47] Specifically, we first adopt a three-year Pilot timeframe and $200 million cap to support cybersecurity services and equipment, including advanced firewalls, for eligible schools and libraries, using the Connected Care Pilot Program as a model.[48] Second, we establish per-student and per-library budgets to specify the amount of funding that Pilot participants can receive and ensure funding can be widely disbursed. Next, we confirm that all eligible schools and libraries, including those that do not currently participate in the E-Rate program, are eligible to apply to participate in the Pilot Program. We then adopt a Pilot eligible services list that specifies the cybersecurity services and equipment that will be eligible for Pilot funding, and an application process that mirrors the E-Rate program and through which we can select a broad pool of participants. In addition, we establish Pilot Program rules and procedures for all phases of the Pilot, including competitive bidding, requesting funding, and invoicing/reimbursement. These Pilot rules and procedures draw on our experience administering the E-Rate and ECF programs and will promote efficient program administration and reduce burdens on Pilot participants. We also appoint an Administrator of the Pilot, and adopt program integrity protections, including document retention and production, gift, certification, audit, and suspension and debarment rules, consistent with our responsibility to be a careful steward of limited USF dollars. We then adopt Pilot performance goals and data reporting requirements to help us assess the costs and benefits of using the limited universal service funds to support the cybersecurity needs of K-12 schools and libraries, and establish appeal and waiver request rules to provide recourse for parties aggrieved by decisions of the Pilot Program Administrator. Lastly, we conclude that the Commission has legal authority to establish a Pilot Program that provides USF support for cybersecurity services and equipment to eligible schools and libraries and that the requirements of the Children's Internet Protection Act (CIPA) are triggered by the purchase of eligible services or equipment through the Pilot.

A. Pilot Timeframe and Overall Cap

15. *Pilot Program Timeframe.* We first adopt a Pilot Program duration of three years. In the

[45] For purposes of the Pilot program, we refer to "participants" as those entities selected to be included in the Pilot program. We use the term "applicants" to refer to the entire pool of entities that apply for the Pilot. In this regard, the nomenclature for the Pilot program will differ slightly from the E-Rate program, which traditionally refers to schools and libraries collectively as "applicants."

[46] *See generally Cybersecurity NPRM.*

[47] *See, e.g.*, *Promoting Telehealth for Low-Income Consumers; COVID-19 Telehealth Program*, WC Docket Nos.18-213, 20-89, Report and Order, 35 FCC Rcd 3366, 3375, para. 13 (2020) (*Connected Care Pilot Order*) (stating that the Connected Care Pilot Program would evaluate "whether and how the USF can help defray health care providers' costs of providing connected care services, particularly to low-income Americans and veterans").

[48] *Id.* at para. 38 (making available $100 million over a three-year funding period through a pilot program separate from the budgets of existing universal service programs).

Cybersecurity NPRM, we sought comment on our proposed three-year term for the Pilot Program.[49] We sought comment specifically to understand whether (i) the proposed length of the program is sufficient to provide the Commission with ample data to evaluate how effective the Pilot funding is in protecting K-12 schools and libraries, and their broadband networks and data, from cyber threats and attacks; (ii) if it was feasible to shorten the Pilot without compromising the integrity of the data collected; and (iii) if we should provide additional time for participants to prepare for the Pilot or for the Commission to evaluate the data at the conclusion of the Pilot.[50]

16. While several commenters support the proposed Pilot duration of three years,[51] many advocated for a shortened Pilot duration of either one year or eighteen months.[52] Commenters supporting a shorter Pilot timeframe offered four main reasons for doing so. First, commenters argued that a three-year Pilot would render the data collected on cybersecurity services and equipment used to combat cybersecurity threats and attacks obsolete by the conclusion of the Pilot Program.[53] Second, commenters advocated that a shorter program would allow the Commission to evaluate Pilot data in time to align with the next E-Rate category two budget cycle (FY 2026 through FY 2030).[54] Third, commenters argued for a shorter duration on the grounds that applicants who were not selected to participate in the Pilot would be required to wait over three-years to potentially receive funding to combat cybersecurity threats and attacks.[55] Finally, commenters recommend a shorter Pilot term or, alternatively, a higher cap, in order to increase the number and diversity of participants.[56]

17. A three-year Pilot Program will give us the time to evaluate whether universal service

[49] *Cybersecurity NPRM,* 2023 WL 8605080 at *12, para. 28.

[50] *Id*.

[51] Cybersecurity Coalition and Information Technology Industry Council Comments at 2 (Cybersecurity Coalition/ITI) ("The Coalition and IT are broadly supportive of the proposed three-year pilot program within the Universal Service Fund (USF) to provide up to $200 million to support cybersecurity and advanced firewall services for eligible schools and libraries."); *see also* Illinois Office of Broadband Comments at 6 (IOB) ("IOB agrees that the . . . Pilot program should not exceed three years. That period will provide an ample opportunity for the Commission to gather a meaningful amount of data on the effectiveness of participants' chosen approaches to cybersecurity."); National Educational Organizations Reply at 3 (EdGroup); CTIA Reply at 10.

[52] *See e.g.,* ActZero Comments at 6 ("Instead of a three-year duration, the Commission should conduct the pilot program for one year. Allowing three months for the application and selection process and an additional three months to review data after the pilot concludes would allow the Commission to determine the best path forward within 18 months."); *see also* CoSN, American Library Association (ALA), SEDTA, SHLB Coalition et al. February 1 *Ex Parte* Letter at 2 (CoSN et al. February 1 *Ex Parte* Letter); Wisconsin Department of Public Instruction Reply at 2 (WI DPI); ALA Comments at 4; Local Education Agencies *Ex Parte* Letter at 1; Clear Creek Amana Express Comments.

[53] FFL Comments at 6; FFL Reply at 2-3; The Friday Institute for Education Innovation Comments at 2 (Friday Institute).

[54] Access, ALA, CoSN, SHLB Coalition et al. *Ex Parte* Letter, WC Docket No. 13-184, at 1-2 (rec. Aug. 7, 2023) (CoSN et al. August 7 *Ex Parte* Letter); Fortinet Inc. Reply at 2 (Fortinet).

[55] The Quilt Reply at 1 (Quilt); ALA Reply at 2; Council GCS at 3-4; Michigan Statewide Educational Network Comments at 3 (MISEN).

[56] Quilt Reply at 3-4 ("The Quilt agrees with NCTA – The Internet & Television Association (NCTA) that 'the Commission needs to have a sufficient sample of participants in order to create meaningful data about the Pilot Program's impact [but that] $200 million may not be enough to enable a wide cross-section of schools and libraries to participate and purchase the needed cybersecurity equipment and services for their networks.' Whether the Commission makes more funding available in the pilot, we note that concentrating funding in a one-year pilot period instead of three-years would make more funding available per participant per year."); *see also* Fortinet Reply at 1-2, n.7; ActZero Comments at 1; Dallas ISD Comments at 3; Association of California School Administrators and the California School Boards Association Reply at 3-4 (ASCA-CSBA Federal Partnership).

support should be used to fund cybersecurity services and equipment on a permanent basis and we adopt a program duration of three years for the Pilot. In establishing the Connected Care Pilot Program, the Commission concluded that a three-year pilot program was "reasonable and will allow the Commission to obtain sufficient, meaningful data from the selected pilot projects" and we find the same reasoning applies here.[57] As a responsible steward of the limited USF, we are obliged to carefully evaluate any actions that would expand demands on the Fund. This is particularly important where, as here, we are exploring whether to make funding available to support services and equipment not previously covered, and where other resources may be available. Given record estimates regarding what it could cost to fund a complete suite of cybersecurity services and equipment, we think it is imperative to carefully consider the potential benefits—and burdens—before deciding whether to move forward with such funding on a wider scale or permanent basis. We believe that a three-year term will enable us to gather the necessary information.

18. We recognize there is a tradeoff between learning more from the Pilot and moving quickly to potentially expand support to protect K-12 schools' and libraries' broadband networks and data from cybersecurity threats and attacks. While some commenters suggested setting a one-year-to-eighteen-month term, in part to align with the next category two budget cycle, we decline to do so. A shorter term would hamper the Commission's ability to evaluate the use of universal service funds to fund cybersecurity equipment and services, particularly given the expected lead time for schools and libraries to implement a cybersecurity solution and unknowns around the evolving threat of potential cybersecurity attacks.[58] Moreover, we note that it would be challenging to align the conclusion of the Pilot with the next category two budget cycle in any event, given the time needed to evaluate lessons learned from the Pilot and the proceedings needed to implement any permanent funding stream for cybersecurity services and equipment. Additionally, we disagree with commenters that a three-year term would render any potential solutions or analysis obsolete. Given the flexibility we provide to Pilot participants to select and modify the cybersecurity services and equipment they choose over the three-year period, we expect that participants will be able to quickly adapt to changes in cybersecurity threats or attacks, or the availability of new cybersecurity solutions. Additionally, given the reporting requirements we adopt herein, we expect to keep pace with lessons learned from the Pilot as data is provided which, in turn, will help facilitate our analysis and determination of next steps. Finally, we disagree with commenters who suggest we shorten the Pilot term or allocate additional funding in order to fund a greater or wider array of participants. As discussed below, we believe the $200 million cap will allow us to provide sufficient support to a wide cross-section of Pilot participants; thus, the benefits to retaining the proposed three-year time frame are greater than the benefits of a shorter duration.

19. *Pilot Program Cap*. We also adopt a Pilot Program funding cap of $200 million over three years for the Pilot Program.[59] In the *Cybersecurity NPRM*, we sought comment on whether (i) a cap of $200 million would be sufficient to obtain meaningful data about how this funding would help to protect schools' and libraries' broadband networks and data and improve their ability to address K-12 cyber risks; (ii) if a lower cap would be sufficient for these purposes (e.g., $100 million); and (iii) how the total Pilot Program cap should be distributed over the three-year funding period in a way that accounts for participants' spending needs while ensuring predictable funding over the three-year term.[60]

20. Several commenters agree that the proposed $200 million funding cap is sufficient to

[57] *See, e.g.*, *Connected Care Pilot Order*, 35 FCC Rcd at 3389-90, para. 46.

[58] *See, e.g.,* Dallas ISD Comments at 2 (asserting that a shorter time frame would accommodate a wider sample of participants and would provide sufficient data for the Commission to conduct its analysis).

[59] *Cybersecurity NPRM,* 2023 WL 8605080 at *12, para. 29.

[60] *Id*.

fund a wide range of Pilot participants over a three-year period.[61] Others suggested a higher amount in order to provide funding[62] to a larger number of E-Rate applicants. Having reviewed the record in its entirety, we adopt the proposed $200 million funding cap for the Pilot Program. For our goal of obtaining meaningful information on how this Pilot could help protect schools' and libraries' broadband networks and data, and improve their ability to address K-12 schools' and libraries' cybersecurity risks, as discussed later in this Order, we believe the proposed cap of $200 million over three years will be sufficient.

21. To provide funding for the Pilot, and to minimize the impact on the contribution factor, we will assign unused E-Rate funds from prior funding years to cover the full $200 million cap. In 2023, the Bureau found that unused funds from prior funding years were available for use in funding year 2023 and directed the USF Administrator, the Universal Service Administrative Company (USAC), to fully fund year 2023 demand, and to reserve an additional $190 million of carry forward funds for future use.[63] Similarly, in 2024, the Bureau directed USAC to reserve $10 million of the available $500 million of carry forward funds for future use.[64] With this Order, we assign that $200 million of carry forward funding to offset the collection requirements for the Pilot, thereby reducing any potential increase on the contribution factor. Making use of carry forward funding in this way is consistent with our responsibility to be a careful steward of the USF, while at the same time allows the Commission to respond to the need for additional cybersecurity funding for K-12 schools and libraries. This approach is consistent with how the E-Rate and other USF programs are administered.[65]

B. Pilot Participant Budgets

22. We next adopt fixed per-student and per-library budgets to determine the amount of funding that participants may receive during the Pilot. In the *Cybersecurity NPRM*, we sought comment on how to evaluate funding requests[66] and whether to establish a maximum amount of funding that an individual participant could receive.[67] Among other things, we sought comment on whether providing a larger amount of funding to a smaller number of participants, or a smaller amount of funding to a greater number of participants, would best enable us to assess the use of the USF for cybersecurity services and equipment.[68] In particular, we sought comment on whether we should establish a per-student budget, with a corresponding budget for libraries, as well as the data sources and cost information that would be appropriate to use in evaluating funding requests.[69] Additionally, we sought comment on whether we should require Pilot participants to contribute a portion of the eligible costs of cybersecurity services and equipment in order to receive funding.[70] We further proposed to apply a participant's category two discount rate to calculate the non-discounted share of costs for the Pilot Program, but also sought

[61] Cybersecurity Coalition/ITI Comments at 2 ("The Coalition and IT are broadly supportive of the proposed three-year pilot program within the Universal Service Fund (USF) to provide up to $200 million to support cybersecurity and advanced firewall services for eligible schools and libraries."); *see also* IOB Comments at 7; ALA Reply at 2-3.

[62] *See e.g.*, MISEN Comments at 5; EdGroup Reply at 4.

[63] *Wireline Competition Bureau Directs USAC to Fully Fund Eligible Category One and Category Two E-Rate Requests*, CC Docket No. 02-6, Public Notice, DA 23-425 (WCB 2023).

[64] *Wireline Competition Bureau Directs USAC to Fully Fund Eligible Category One and Category Two E-Rate Requests*, CC Docket No. 02-6, Public Notice, DA 24-457 (WCB 2024).

[65] *See* 47 CFR § 54.709(b) (specifying the treatment of carry forward funds).

[66] *Cybersecurity NPRM,* 2023 WL 8605080 at *13, para. 32.

[67] *Id*., para. 31.

[68] *Id*., para. 32.

[69] *Id*., para. 31.

[70] *Id*.

comment on requiring participants to instead contribute a fixed percentage of the costs of the cybersecurity services and equipment purchased.[71] Finally, we sought comment on whether a participant should receive its funding commitment in equal installments, or whether there may be reasons why a Pilot participant may need access to a greater amount earlier during the three-year term.[72]

23. A 2021 cost study submitted jointly by FFL, the Consortium for School Networking (CoSN), and others estimated it would cost approximately $13.60 per student annually to support advanced or next-generation firewall services, $16.20 per student annually to support endpoint security and protection, and $14.50 per student annually to support additional, advanced cybersecurity services and equipment.[73] Rubrik, Inc. (Rubrik), in its comments, stated it would be reasonable to establish a funding maximum for individual entities of $1 million to $2 million.[74]

24. Based on our review of the cost estimates submitted by commenters, and consistent with our goal to provide funding to a wide variety of participants, as discussed later in this Order, we adopt fixed budgets to determine the amount of funding that a Pilot participant can receive.[75] In establishing these budgets, which account for the estimated costs of different types of advanced cybersecurity solutions, we expect to provide meaningful benefit to a substantial number of schools, libraries, and consortia. In implementing this approach, we decline to award support based on a percentage of a participant's category one or category two budget, as suggested by some commenters.[76] We find that a more tailored approach, grounded in the estimated cost of implementing specific types of cybersecurity solutions, would best achieve our goals in a targeted and cost-effective manner. Furthermore, we note that because we do not limit Pilot participation to current E-Rate applicants, the suggested approach would therefore be difficult to implement. When implementing these budgets, we will categorize Pilot applicants and consider their funding needs in combination with their applicant type, as discussed in greater detail below.

25. *Schools and School Districts*. Schools and school districts will be eligible to receive up to $13.60 per student, on a pre-discount basis, to purchase eligible cybersecurity services and equipment over the three-year Pilot duration.[77] We find that a pre-discount budget of $13.60 per student strikes an

[71] *Id*.

[72] *Cybersecurity NPRM,* 2023 WL 8605080 at *12, para. 29.

[73] CoSN 2021 Petition, Attachment at 14 (CoSN et al 2021 E-Rate Cybersecurity Cost Estimate); *see also supra* note 36.

[74] Rubrik, Inc. Comments at 3 (Rubrik).

[75] *See, e.g.*, *Connected Care Pilot Order*, 35 FCC Rcd at 3388-89, para. 43 (observing that there are "significant advantages to providing a set support amount that requires participants to contribute a portion of the eligible costs, including being administratively simple, predictable, and equitable, as well as incentivizing participants to choose the most cost-effective services and equipment and refrain from purchasing a higher level of service or equipment than needed").

[76] Crown Castle Fiber LLC Comments at 4 (Crown Castle) (suggesting that the Pilot program's support be limited to "33% of the Internet Access service for the largest circuit of each applicant, excluding Wide Area Networking, MPLS, and site-to-site connectivity"); FFL Comments at 17 (asserting that "[c]yber security should also be funded by a certain overall percentage based on the overall funding available in a given 5 year [E-Rate] funding window").

[77] Because school and school district budgets are calculated on a per-student basis, and because the budget covers the three year Pilot program duration, we will use a participant's student count in the first year of the Pilot program as the applicable student count for the entirety of the Pilot. Participants will not update their student counts in subsequent years. For participants that do not currently participate in E-Rate, and therefore may not have a student count on file with USAC, USAC will determine the participant's student count and discount rate based on information provided during the eligibility review of the new participant. All Pilot participants who are not currently participating in the E-Rate program will have their eligibility verified by USAC as part of the FCC Form 484 review process.

appropriate balance between supporting the various types of cybersecurity services and equipment needed to protect school networks, and our desire to provide funding to as many schools and school districts as possible in the limited-term Pilot Program. Additionally, we note that this per-student budget is sufficient to support the majority of the total costs related to any one of the three types of security measures FFL and CoSN identified in their cost estimate,[78] and is also consistent with the Commission's analysis in the *First 2014 E-Rate Order* that established per-student budgets for category two equipment and services.[79]

26. We recognize that for many schools a pre-discount budget of $13.60 will not, by itself, be sufficient to fund all of the school's cybersecurity needs to achieve a fully mature cybersecurity posture, as doing so would typically require a school to implement multiple categories of technical solutions, often in a specific priority order.[80] Given the limited Pilot funding available, our approach instead ensures that each participating school will receive funding to prioritize implementation of solutions within one major technological category requested by commenters,[81] enabling the school to make meaningful progress toward its own cybersecurity goals and providing flexibility for schools with differing cybersecurity strengths and vulnerabilities.[82] We find that this approach ensures that each participant can make meaningful, incremental progress towards its own cybersecurity goals, and best positions the Commission to assess the benefits that accrue from funding individual cybersecurity solutions, consistent with a core objective of the Pilot. We also find that this approach represents a strategic and cost-effective way to spend limited Pilot funds in the context of considering future changes to the E-Rate program, as it creates incentives for each school to select the most impactful incremental solutions available to it in view of the school's specific cybersecurity vulnerabilities and strengths.[83]

27. Schools and school districts selected for the Pilot Program will be eligible to receive, at a minimum, $15,000 in support, on a pre-discount basis, over the three-year Pilot duration. We establish this funding floor to ensure that even the smallest schools and school districts can receive support sufficient to purchase a variety of cybersecurity services and equipment. We set the funding floor at $15,000, pre-discount, because it aligns with the cost estimate submitted by FFL and CoSN, which found that that the approximate per-site cost for advanced firewalls is $15,994.[84] We note that a pre-discount $13.60 per-student budget equates to approximately 1,100 students in a school or school district receiving $15,000 in support. As a result, schools and school districts with 1,100 students or fewer will be eligible to receive the $15,000 funding floor. We also establish a budget maximum of $1.5 million, pre-discount,

[78] CoSN et al 2021 E-Rate Cybersecurity Cost Estimate at 14. The cost estimate provides that the three categories of cybersecurity protections, next-generation or advanced firewall services, endpoint protection services, and advanced+ security services are "layered," in that they "build upon one another." *Id.* at 3. For the purposes of the Pilot, however, we seek to study each of these categories independently, along with the other categories included in Cybersecurity Pilot Eligible Services List at Appendix B, to better ascertain the incremental value each category of cybersecurity protections could bring in securing E-Rate-funded broadband networks and data.

[79] *See, e.g.*, *First 2014 E-Rate Order*, 29 FCC Rcd at 8904, 8216, paras. 91, 118.

[80] *See* CoSN et al 2021 E-Rate Cybersecurity Cost Estimate at 3 (opining that next-generation or advanced firewall services, endpoint protection services, and advanced+ security services are "layered," in that they "build upon one another").

[81] Namely, next-generation/advanced firewall services, endpoint protection services, and advanced+ security services. *See supra* para. 23 (citing CoSN et al 2021 E-Rate Cybersecurity Cost Estimate at 14).

[82] CoSN et al 2021 E-Rate Cybersecurity Cost Estimate at 15 (recommending that K-12 entities develop a "cybersecurity plan[]" tailored to its "technology and risk environment" that defines a "target maturity state" and implements a "maturation path" for the entity).

[83] *See* CISA K-12 Cybersecurity Report at 13 (noting that "[c]ybersecurity is not one size fits all" as "[s]chools and their districts have distinct strengths and weaknesses and a wide range of needs" even as there are some common actions that "every K-12 organization can take to significantly reduce the risk of a damaging instruction").

[84] CoSN et al 2021 E-Rate Cybersecurity Cost Estimate at 15.

which equates to approximately 110,000 students, using the pre-discount $13.60 per-student budget. As a result, schools and school districts with more than 1,100 students, and up to approximately 110,000 students, will calculate their budget using the pre-discount $13.60 per-student multiplier. Schools and school districts with more than 110,000 students will be subject to the budget maximum of $1.5 million, over the three-year Pilot duration. We find that a $1.5 million maximum reflects the greater purchasing power of larger schools, school districts, and consortia, and the associated reduction in the cost-per-student amount.[85] Additionally, we establish the budget maximum to best ensure that Pilot funds are able to support cybersecurity services and equipment for as many schools and libraries as possible, and also to ensure that a disproportionate amount of funding is not awarded to any one participant.

28. *Libraries and Library Systems.* Rather than adopt a per-user budget, as we have for schools and school districts, or a budget based on library square footage as we do for category two E-Rate funding requests, we adopt a budget that provides a set amount of funding per library. In particular, we establish a pre-discount budget of $15,000 per library, consistent with our analysis above regarding the minimum per-site funding amount needed to support advanced firewalls. Library systems with more than 11 sites will be eligible for support up to $175,000, which we note approximately reflects the cost of providing advanced firewalls to an entity with between 10 and 24 locations.[86] We believe a per-site methodology for calculating library budgets more appropriate than using library square footage, as we do for E-Rate category two funding requests, because costs for cybersecurity services and equipment do not scale with square footage in the same way as they do for building internal Wi-Fi networks. We also find that the pre-discount budgets established for libraries and library systems are generally consistent with how funding is allocated in the E-Rate program to cover the majority of the cost of supported services and equipment, and strike a balance between funding a baseline amount needed to procure cybersecurity services and equipment, and ensuring that the Pilot Program is able to support a significant number of schools and libraries.

29. *Consortia.* Consortia participants comprised of eligible schools and libraries will be eligible to receive funding based on student count (using the pre-discount $13.60 per student multiplier) and the number of library sites (using the pre-discount $15,000 per library budget). Consortia that are solely comprised of schools will be subject to the $1.5 million budget maximum applicable to schools. Consortia that are solely comprised of libraries will be subject to the $175,000 budget maximum for library systems. Consortia comprised of both eligible schools and libraries will be subject to the $1.5 million budget maximum applicable to schools. We find these budget maximums are an important mechanism to ensure that Pilot funding is widely disbursed. We will also require each consortium to select a consortium leader.[87]

30. *Non-discount Share of Costs.* We will require participants to contribute a portion of the costs of the cybersecurity services and equipment they seek to purchase with Pilot Program support, similar to the non-discount share that E-Rate applicants are required to contribute to the cost of their eligible services and equipment.[88] We agree with the Dallas Independent School District (Dallas ISD) that requiring participants to contribute some portion of the costs of eligible services and equipment, as we have in E-Rate, will be "successful in aligning the interests of applicants to minimizing waste, fraud,

[85] *Id.* (finding that the cost of advanced firewall for a school district with 50+ sites is approximately $1.2 million); *see also, e.g.*, Cisco Comments at 13 (noting economies of scale for district-wide or state-wide purchases); Cybersecurity Coalition/ITI Comments at 6 (highlighting cost benefits that are driven by scale).

[86] CoSN et. al 2021 E-Rate Cybersecurity Cost Estimate at 15.

[87] *See* 47 CFR § 54.2002(c)(1) (as codified in Appendix A) (codifying the requirement to select a consortium leader). The requirement for consortia to select a leader is consistent with the similar requirement in the E-Rate program. *See* https://www.usac.org/e-rate/applicant-process/before-you-begin/consortia/.

[88] *See* 47 CFR § 54.523.

and abuse."[89] In the *Cybersecurity NPRM*, we proposed using a participant's category two discount rate to determine the portion of costs a participant will be required to contribute.[90] We establish today, instead, that participants will use their category one discount rate to determine the non-discount share of costs. Thus, participants with the students with the greatest need will be eligible for support for 90 percent of their costs, and will be required to contribute 10 percent of the cost of eligible cybersecurity services and equipment purchased with Pilot funds. By using the category one discount rate, the program's neediest schools and libraries will have greater flexibility in selecting eligible services and equipment, thus supporting our goal to evaluate the benefits of supporting advanced firewalls and cybersecurity services using the USF. Furthermore, the category one discount rate is appropriate, as Pilot funds will be used to enhance the protection of the broadband networks, including those funded from the E-Rate program's category one. We find that this approach is preferable to establishing a uniform contribution percentage like the one adopted for the Connected Care Pilot Program[91] because it equitably accounts for the relative need of the participant. Moreover, most, if not all, Pilot applicants and participants—including large state or regional consortia—are already familiar with the use of discount rates in the E-Rate program.[92]

31. *Disbursement of Support.* We will permit Pilot participants to request reimbursement as expenses are incurred, even if it means that a greater amount of funding may be drawn earlier in the three-year Pilot term. In doing so, we acknowledge that some participants may face greater up-front costs for the services and equipment needed to implement their cybersecurity plans, whereas others may have ongoing recurring costs,[93] or some combination of both. We agree with Cisco that we should not adopt a "static" [94] funding approach, as well as with Palo Alto Networks, Inc. (Palo Alto) that a flexible approach would "ensure a stronger runway for the deployment and configuration of eligible solutions and products under the Pilot."[95] However, we decline to adopt the recommendation of ATARC Cybersecurity Higher Education and Workforce Development Working Group (ATARC) that we abandon our traditional reimbursement structure to provide "seed" money at the outset of the Pilot.[96] This reimbursement process is consistent with the reimbursement processes used in the E-Rate and other universal service programs[97]

[89] Dallas ISD Comments at 3.

[90] *Cybersecurity NPRM,* 2023 WL 8605080 at *13, para. 31.

[91] *See, e.g.*, IOB Comments at 8; *see also Connected Care Pilot Order*, 35 FCC Rcd at 3388-89, para. 87 (establishing a uniform 85 percent discount rate for the Connected Care Pilot Program).

[92] As in the E-Rate program, discount rates for the Pilot program will be determined on the basis of the percentage of student enrollment that is eligible for a free or reduced price lunch under the National School Lunch Program. Libraires and consortia calculate a discount rate on the basis of the percentage of student enrollment that is eligible for the National School Lunch Program in the public school district in which they are located. *See* 47 CFR § 54.2007 (establishing discount methodology for the Pilot); *see also* 47 CFR § 54.505 (establishing discount methodology for the E-Rate program). These discount rate calculations will also apply for Pilot participants that do not currently participate in the E-Rate program. All Pilot participants who do not currently participate in the E-Rate program will have their eligibility verified during the FCC Form 484 review process. The discount rate for that participants will be determined as part of the eligibility review.

[93] *See* Center for Internet Security Comments at 9 (CIS) (noting that "[m]any of today's cybersecurity solutions are now licensed by a yearly subscription" with ongoing, recurring costs); Cisco Comments at 13; Zscaler, Inc. Reply at 2 (Zscaler).

[94] Cisco Comments at 13.

[95] Palo Alto Networks Comments at 2.

[96] ATARC Cybersecurity Higher Education and Workforce Development Working Group Reply at 1 (ATARC); *see also* EdGroup Reply at 3.

[97] *See, e.g.*, *Connected Care Pilot Order*, 35 FCC Rcd at 3387-88, para. 42 (stating that "requests for funding may vary year to year and therefore we will not require that Pilot Program funding be distributed evenly").

and, combined with the requirement that Pilot participants contribute some amount of their own money towards the cost of eligible services and equipment, serves as an important backstop for safeguarding the integrity of the Pilot Program. Moreover, while we are mindful of the importance of establishing a predictable cap that minimizes the contribution burden on consumers, we expect that the limited nature of the Pilot cap relative to the overall size of the Fund, as well as our planned use of the reserved $200 million in carry forward funding,[98] will minimize any burden to the overall Fund for any given quarter.

32. *Pilot Benefits will Exceed Costs.* We expect the benefits of the Pilot Program to exceed the costs. As a threshold matter, we note that program participation by applicants and service providers is voluntary, and we expect that Pilot participants will carefully weigh the benefits, costs, and burdens of participation to ensure that the benefits outweigh their costs. The Pilot will also enable us to evaluate the estimated economic benefits of using universal service support for cybersecurity services and equipment, compared to its cost to the Fund. In this regard, we note that, according to the Federal Bureau of Investigation's Internet Crime Complaint Center, the U.S. population, including U.S. territory residents, incurred an estimated $10.9 billion in losses from cybercrime in 2023.[99] Based on a 2023 U.S. population of 335 million, this equates to a per-capita loss of about $32.50 per person from cybercrime.[100] The Pilot Program caps support at $13.60 per student for most schools and school districts. If the Pilot can reduce the annual monetary cost of cyberattacks on participating K-12 schools by at least 42 percent, the expected economic benefits of increased cybersecurity would exceed the per-student funding costs.[101] We expect that there may be additional benefits that cannot be easily quantified, such as a reduction in learning downtime caused by cyberattacks,[102] reputational benefits from increased trust in school and library systems, increased digital and cybersecurity literacy among students and staff, and the safeguarding of intellectual property.[103] Despite these benefits, we are also concerned about the overall

[98] *See supra* para. 21.

[99] *See* FBI, FBI Internet Crime Report 2023, at 25 (2023), https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf. An estimated $10,924,447,718 of losses due to cybercrimes was reported in 2023. This is a 22 percent increase from losses reported in 2022.

[100] *See* Press Release, U.S. Census, US Population Trends Return to Pre-Pandemic Norms as More States Gain Population (Dec. 19, 2023), https://www.census.gov/newsroom/press-releases/2023/population-trends-return-to-pre-pandemic-norms.html (reporting a U.S. population of 334,914,895 in December 2023).

[101] $13.60 / ($10,924,447,718 / 334,914,895) = $13.60 / $32.62 = 41.7%. This assumes the per-student cost of cyberattacks is equivalent to the per-capita cost across the United States. However, it is likely that the per-student cost is higher than the U.S. per-capita average because schools are frequent and growing targets of cyberattacks. If so, then our estimates are a floor on potential benefits of the Pilot program to K-12 students.

[102] GAO K-12 Cybersecurity Report at 2. For example, the annual monetary cost of ransomware attacks does not include the downtime while the school district negotiates, lost instruction time, the cost of recovering lost data despite paying the ransom, the anxiety inflicted, and the harm to the general population's trust in schools. Attackers can publish sensitive data to retaliate for nonpayment of a ransom to scare future victims. Levin estimates that criminals, in retaliation for unpaid ransoms, exposed personal information of at least 560,000 current students and 56,000 staff in 2020, and likely former students and staff. Levin, Douglas A., The State of K-12 Cybersecurity: 2020 Year in Review at 6 & 9 (2021), https://k12cybersecure.com/wp-content/uploads/2021/03/StateofK12Cybersecurity-2020.pdf (2020 Levin Report).

[103] The Pilot program encourages participants to access tools and trainings to improve cybersecurity awareness among students and staff. For example, CISA provides free Federal Virtual Training Environment (Fed-VTE) online cybersecurity training to public K-12 school staff, and the National Initiative for Cybersecurity Careers and Studies provides classroom curricula and formal training for teachers to implement good cyber practices. *See* https://niccs.cisa.gov/education-training/federal-virtual-training-environment-fedvte & https://niccs.cisa.gov/education-training/cybersecurity-teachers. The National Institute of Standards and Technology (NIST) also has training resources at https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content. We further note that in the Cybersecurity Eligible Services List at Appendix B, cybersecurity training for students, school staff, and library patrons is not an eligible service and thus, Pilot participants are strongly

(continued….)

cost to the Fund, if we were to provide cybersecurity funding to all E-Rate participants, which CoSN estimates could cost the Fund $2.389 billion annually.[104] This limited Pilot Program will therefore enable the Commission to evaluate the benefits of using universal service funding to fund cybersecurity services and equipment against the costs before deciding whether to support it on a permanent basis.

C. Eligibility of Pilot Participants

33. We next make eligibility for participation in the Pilot Program open to all eligible schools and libraries,[105] including those that do not currently participate in the E-Rate program. In the *Cybersecurity NPRM*, we sought comment on the types of entities that should be eligible to participate in the Pilot Program.[106] We observed that a wide array of entities participate in the E-Rate program, and sought comment on how to ensure that the Pilot likewise has a diverse participant pool.[107] Specifically, we asked whether: (i) eligibility should be limited to schools and libraries currently participating in the E-Rate program; (ii) eligibility should be expanded to include schools and libraries that do not currently participate in the E-Rate program; or (iii) eligibility should include any entity that qualifies for funding through the E-Rate program.[108] We proposed to adopt the same definitions for schools and libraries as used in the E-Rate program, when determining the eligibility of Pilot participants.[109]

34. Commenters generally supported leveraging the E-Rate program rules to determine the types of entities that should be eligible to participate in the Pilot Program, with at least a few encouraging the Commission to limit eligibility to existing E-Rate applicants.[110] For example, NCTA – The Internet & Television Association (NCTA) argued that limiting eligibility to existing E-Rate participants was appropriate "since [Pilot] cybersecurity services will be integrated with the connectivity being purchased pursuant to the E-Rate program."[111] Several commenters urged the Commission to make consortia eligible, consistent with the E-Rate program.[112] These commenters noted that consortia "can provide valuable services at scale,"[113] which would allow the Commission to "stretch the limited proposed Pilot funding and increase the impact to more students and schools."[114] Others suggested that we expand

(Continued from previous page)
encouraged to use the free and low-cost cybersecurity training resources that are readily available to supplement the other cybersecurity equipment and services that are eligible through the Pilot.

[104] CoSN 2021 Petition at 14.

[105] 47 CFR § 54.2000 (defining elementary school, secondary school, library, and library consortium, for purposes of the Pilot); *id.* § 54.2002 (defining eligible recipients of Pilot program support).

[106] *Cybersecurity NPRM,* 2023 WL 8605080 at *13, para. 34.

[107] *Id*.

[108] *Id*. The Commission also sought comment on whether applicants should be selected based on their existing cybersecurity posture, including cyber readiness and resources, commitment to undertake cyber readiness activities, and past history of cyberattacks. *Cybersecurity NPRM* at *13-14, paras. 34-36. As discussed *infra* at para. 67, we decline to do so and focus instead on selecting participants by weighing objective considerations, such as discount rate, school size, and urban/rural status.

[109] *See Cybersecurity NPRM*, Appendix A (proposing to adopt the E-Rate definitions for elementary school, secondary school, library, and library consortium). The proposed definitions for these terms at section 54.2000 are the same definitions adopted and codified at section 54.500. *See* 47 CFR §§ 54.500, 54.2000.

[110] NCTA Comments at 5; Palo Alto Network Comments at 1; Lumen Reply at 6.

[111] *Id*.

[112] K12 SIX Comments at 6; MISEN Comments at 11; Allendale Public Schools Reply at 2 (Allendale), Wayne RESA Reply at 2.

[113] K12 SIX Comments at 6.

[114] MISEN Comments at 11.

eligibility to include local and other government entities[115] and Educational Service Agencies (ESAs).[116]

35. We have determined that we will permit all eligible schools and libraries, including those that do not currently participate in the E-Rate program, to apply to participate in the Pilot.[117] We adopt the definitions of elementary school, secondary school, library, and library consortium contained in Appendix A of this Report and Order, which mirror the definitions that we use for the E-Rate program.[118] In taking these steps, we decline to adopt suggestions from commenters that we limit Pilot eligibility to only those schools and libraries that currently participate in the E-Rate program.[119] We observe that all schools and libraries currently face increased cybersecurity threats and attacks regardless of whether they receive E-Rate funding and opening the Pilot Program to all eligible schools and libraries will allow us to gather data from the widest range of eligible participants. While we appreciate the concern raised by NCTA and others that the Pilot should focus on protecting E-Rate-funded networks, we believe that, on balance, opening the Pilot Program to a wider pool of participants would best ensure that we have sufficient data to evaluate the impact of universal service support on the purchase of cybersecurity services and equipment both now and in the future. Given the large percentage of eligible schools that participate in the E-Rate program, we anticipate that the overwhelming majority of Pilot participants will also be E-Rate participants.

36. Consistent with our E-Rate rules, we further clarify that we will also permit eligible schools and libraries that apply as a consortium to participate in the Pilot. We agree with commenters that consortia have buying power that can help bring down costs[120] and that including consortia in the Pilot would allow larger, better resourced schools and libraries to partner with smaller, less technically savvy participants. We decline to extend eligibility to local and other governmental entities, including ESAs, or other entities that are not an eligible school or library as defined in section 54.2000 of the

[115] *See* The City of New York Office of Technology and Innovation Reply at 2 (City of NY OTI) ("When listing eligible recipients in Section 54.2002, no allowance is made for local government entities that provide cyber security services for schools and libraries, centrally. The City believes that government entities that provide cyber security services to schools and libraries should be included in the list of eligible recipients. In many instances, these entities are the sole providers of cyber security services to schools and libraries. Precluding their eligibility would put schools and libraries in the position of having to implement separate technologies, with which they are unfamiliar with (*increasing* the risk of misconfigurations) or declining to take advantage of the grant."); IOB Comments at 9.

[116] City of NY OTI Reply at 2. Federal law defines an Educational Service Agency as a "regional public multiservice agency authorized by state statute to develop, manage, and provide services or programs to local educational agencies." The E-Rate rules do not specifically define or address ESAs. To determine whether an ESA is eligible to receive E-Rate support, USAC must verify that the ESA provides elementary or secondary education as determined under state law (whether the entity provides elementary or secondary education to its student population and whether the ESA facility is eligible for support because elementary or secondary education, as defined in state law, is provided at that facility). USAC asks state and territory officials to describe the programs served by ESAs and whether ESAs operate facilities that they either own or lease that contain classrooms. The officials are also asked to provide legal support for the information they supply to USAC and to certify the accuracy of their determinations. The results from these reviews are included in the Eligibility Table for Educational Service Agencies and can be found at https://www.usac.org/e-rate/applicant-process/before-you-begin/educational-service-agencies/.

[117] As discussed above, selected Pilot participants that do not currently participate in the E-Rate program will have their eligibility verified, and their discount rate calculated, during the FCC Form 484 review process. *See supra* paras. 25, 30.

[118] *See supra* note 109.

[119] Palo Alto Networks Comments at 1; NCTA Comments at 5.

[120] *See, e.g.*, Allendale Reply at 2.

Commission's rules adopted today.[121] However, non-eligible entities, including local, state and Tribal governmental entities, and other not-for-profit organizations may serve as a consortium leader for a consortium participant in the Pilot, but like in the Rural Health Care, E-Rate, and Connected Care Pilot programs, would be ineligible to receive Pilot benefits, discounts, and funding, and therefore must pass through the benefits, discounts, and support to the eligible school and library consortium members.[122] While we recognize that local governmental entities may provide economies of scale or cybersecurity expertise that would benefit schools and libraries, the E-Rate and Rural Health Care programs direct USF support to schools, libraries, and health care providers, pursuant to sections 254(c)(3) and 254(h) of the Communications Act of 1934, as amended (the Act).[123] As our legal authority for the Pilot stems from the same source,[124] we decline to expand Pilot eligibility to include governmental and other entities that would be ineligible under the E-Rate or Rural Health Care programs; however, we recognize the expertise and value of these entities by allowing them to serve as ineligible consortium leaders and passing through the benefits, discounts, and support of the Pilot Program to the eligible school and library consortium members. We direct the Bureau and USAC to provide additional training and guidance on creating a Pilot consortium and serving as a consortium leader in the Pilot. We also direct the Bureau and USAC to establish measures to prevent eligible schools and libraries from receiving duplicative Pilot support as an individual Pilot participant and as a Pilot consortium member.

D. Eligible Services and Equipment/Security Measures

1. Eligible Services and Equipment

37. We adopt a Pilot Eligible Services List (P-ESL) which specifies eligible cybersecurity services and equipment for the Pilot.[125] In the *Cybersecurity NPRM*, we sought comment on the "equipment and services . . . that should be made eligible to participants in the Pilot" and on whether we should specify eligible services and equipment using "general criteria" or rather as a "list of specific technologies."[126] Based on the record, we adopt a flexible approach for the P-ESL as we deem services and/or equipment eligible if they "constitute a protection designed to improve or enhance the cybersecurity of a K-12 school, library or consortia."[127] At the same time, we provide applicants with specificity and clarity in practical terms in the P-ESL, as it enumerates as eligible, in a non-limiting manner, four general categories of technology raised by commenters as effective in combatting cyber

[121] We clarify that to the extent that an ESA meets the eligibility requirements set forth in our rules, it will be eligible to participate in and receive Pilot support. *See e.g.*, USAC, *Eligibility Table for Educational Service Agencies (ESAs)*, https://www.usac.org/wp-content/uploads/e-rate/documents/Tools/ESA-Eligibility-Table.pdf (last visited Apr. 3, 2024) (providing information on whether an ESA is eligible for E-Rate support as determined by state law).

[122] *See, e.g.*, 47 CFR § 54.609 (providing that an ineligible entity that serves as the Consortium Leader must pass on the full value of any discounts, funding, or other program benefits secured to the consortium members that are eligible"); 47 CFR § 54.500 (noting that consortia can include public sector (governmental) entities but such entities are not eligible for support); *Connected Care Pilot Order,* 35 FCC Rcd at 3411-12, para. 75 & n.198 (adopting 47 CFR § 54.609 in the Connected Care Pilot Program). However, such entities can serve as the consortium leader. *See* USAC, Consortia, https://www.usac.org/e-rate/applicant-process/before-you-begin/consortia/ (last visited Apr. 2, 2024) (noting that the consortium leader can be one of the E-Rate eligible entities, or an outside entity, such as the organization that established the consortium). *See also* 47 CFR § 54.2002(c)(1) (explaining who can serve as a consortium leader and restricting Pilot support to the eligible school and library consortium members).

[123] *See* 47 U.S.C. §§ 254(c)(3); 254(h)(1)-(2).

[124] *See infra* section III.K.

[125] *See* Appendix B.

[126] *Cybersecurity NPRM,* 2023 WL 8605080 at *16, para. 40.

[127] Eligible equipment and services must meet a number of additional criteria to be reimbursable expenses (e.g., cost effectiveness). *See, e.g.*, *infra* section III.F.

threats, namely, (i) advanced/next-generation firewalls; (ii) endpoint protection; (iii) identity protection and authentication; and (iv) monitoring, detection, and response. Moreover, for each of these categories, we provide a non-exhaustive list of examples of eligible services and equipment in the P-ESL. Through the list of examples, we confirm that the wide range of services and equipment we had proposed for inclusion in the *Cybersecurity NPRM*, or that commenters had otherwise requested, are eligible.[128] We designate the eligible services and equipment for the duration of the Pilot through the P-ESL. We also delegate authority to the Bureau, as needed, to clarify and make technical changes to the P-ESL consistent with the standards we establish today, to promote efficient program administration and account for technological evolution.

38. We agree with commenters who opine that Pilot participants should have flexibility to determine which solutions best serve their needs by basing eligibility on broader considerations, rather than a specific and potentially rigid set of pre-authorized components.[129] Our approach is consistent with Rubrik's view that we "provide general guidance for applicants, but not lock them into specific technology products."[130] Our approach also includes as eligible the advanced or next-generation firewalls, endpoint security and protection, and other advanced security services and equipment identified by E-Rate stakeholders, including FFL and CoSN.[131] At the same time, by enumerating four non-limiting categories of eligible technology, we find that our approach also meets the recommendations of commenters that we "establish general categories of eligible offerings"[132] without "specify[ing] the precise technologies or solutions that must be relied upon"[133] and allow "[p]ilot participants to select any product and/or services that fall into any of the eligible categories."[134] Our approach also ensures that most, if not all, of the cybersecurity services and equipment needed to implement recommendations from the CISA K-12 Cybersecurity Report, the Education Department K-12 Digital Infrastructure Briefs, and other federal resources and guides are eligible while still allowing Pilot participants significant flexibility to determine to the extent which any of these specific measures would be most cost-effective for them to implement. While we decline to make these or other federal recommendations the sole basis for determining eligibility for the purposes of today's Pilot,[135] we strongly encourage all participants to consider these federal recommendations, particularly those that can be implemented at little or no cost, as part of their assessment of which services and equipment to request to be funded through the Pilot. We direct the Bureau to identify these federal recommendations, and we direct the Bureau and USAC to facilitate access to these recommendations by including information related to them on relevant program websites and in training materials that each entity makes available to Pilot participants. We further direct

[128] We clarify, for example, that this includes cybersecurity services provided by CISA and NIST provided they qualify as eligible services and equipment subject to the exclusions discussed in section III.D.2 below. *See, e.g.*, Tim Roemer/Global Market Innovators Comments at 1 (GMI).

[129] ActZero Comments at 7; Cybersecurity Coalition/ITI Comments at 3-4; NCTA Comments at 4; Rubrik Comments at 3; Electronic Privacy Information Center Reply at 2 (EPIC); MISEN Comments at 3.

[130] Rubrik Comments at 3.

[131] *See* CoSN et al 2021 E-Rate Cybersecurity Cost Estimate at 9-10 (advocating for the eligibility of Intrusion Prevention / Intrusion Detection (IPS/IDS), Virtual Private Network (VPN), Distributed Denial-of-Service protection (DDoS), Network Access Control (NAC), anti-virus, anti-malware, anti-spam, Domain Name System (DNS) security, blocking and filtering, cloud application protection and multi-factor authentication (MFA)). Each of these tools/services are eligible as specified in the P-ESL. *See* Appendix B.

[132] NCTA Comments at 4; MISEN Comments at 8.

[133] NCTA Comments at 4.

[134] MISEN Comments at 8.

[135] *See Cybersecurity NPRM,* 2023 WL 8605080 at *17, para. 41 (seeking comment on whether we should "determine eligible measures based on the recommendations from the CISA K-12 Cybersecurity Report, the [ED] K-12 Digital Infrastructure Briefs, and/or other federal partner resources and guides").

the Bureau and USAC to periodically update the information provided on the websites and in the training materials to reflect relevant updates to the recommendations that may issue during the duration of the Pilot.

39. We find that specifying eligibility based on broader considerations is appropriate in the context of a Pilot that aims to study the effectiveness of a wide variety of technological solutions. We further find that our approach, in which we decline to attempt to exhaustively list every possible technological category or eligible service or piece of equipment within a category, is reasonable and reflects the rapidly changing nature of the technical solutions available to address cyber threats and attacks. Our approach also ensures that services or equipment are not deemed ineligible merely because the service provider or equipment maker uses a label or term to describe it that is not specifically enumerated in the P-ESL. To provide participants with further flexibility, and in view of a lack of consensus around the terminology used to describe similar cyber solutions,[136] we make eligible both the specific services and equipment identified in the P-ESL, as well as ones that have "substantially similar features or their equivalents."[137] We also make eligible security updates and patches,[138] which will help to ensure that participants are protected even as threat vectors evolve over the course of the Pilot. We find that this will help to ensure that the services and equipment funded through the Pilot do not reach their end of useful life prematurely, thus avoiding waste in the Pilot Program.

40. We further find our approach strikes a reasonable balance between specifying basic limits on the scope of eligible services and equipment, which reflects the limited funding available for the Pilot and the need to safeguard Pilot funds from being used on components unrelated to Pilot objectives, while providing participants with clarity and significant flexibility to address their unique cybersecurity threat profiles, which they are ultimately in the best position to assess.[139] Moreover, our enumeration of four key categories of technology, and specific services and equipment within each area, ensures that USAC will be positioned to expediently conduct program integrity and service reviews and quickly issue funding decisions for the eligible Pilot Program services and equipment.

41. We clarify that our inclusion of a given technological category, equipment or service in the P-ESL and/or any subsequent determination by USAC that a specific piece of equipment or service is eligible in the Pilot Program,[140] is not an endorsement by the Commission or USAC that the equipment or service is sufficiently cost- or technologically-effective for its intended purpose (e.g., in preventing a breach, a loss of data or other harm). Rather, we expect participants to select equipment and services from among those that are eligible based on their own assessment of cost-effectiveness in addressing their specific needs. Accordingly, a participant may not rely on eligibility determinations made by the Commission or USAC in the Pilot as a defense or safe harbor should it experience a cyber incident, including a breach, a data loss other or other harm. Moreover, we clarify that the services and equipment listed in today's P-ESL are eligible only when they are used on or as a part of a participant's school or library broadband network that directly furthers its educational mission. We find this clarification

[136] *See*, *e.g.*, CoSN et al 2021 E-Rate Cybersecurity Cost Estimate at 8 (noting that the functionality included within various types of cybersecurity solutions, namely, next-generation firewalls, endpoint protection and advanced+ security, "can be difficult to identify because of overlapping functionality between security services, particularly when different security platforms from different vendors are involved.").

[137] *See* Appendix B at 1. We direct USAC, as administrator of the Pilot program, in consultation with the Bureau, to make determinations, as necessary, on whether specific services or equipment have "substantially similar features or [are] their equivalents". In doing so, we expect that USAC will use all of the customary tools at its disposal (i.e., that it uses in E-Rate to verify eligibility), including follow-up information requests to participants for additional technical information, when making eligibility determinations for the Pilot program.

[138] *Id*. at 1-2; Cisco Comments at 13.

[139] *See*, *e.g.*, MISEN Comments at 8-9.

[140] *See supra* note 137.

appropriate to ensure that we can satisfy the statutory purpose of the E-Rate program, as well as our goal of measuring the costs associated with cybersecurity services and equipment, as discussed later in this Order.[141] We also decline to limit eligible services and equipment for the Pilot to those that are used on E-Rate-funded broadband networks only. We find this step reasonable given that Pilot participants are not limited solely to current applicants in the E-Rate program.

a. Advanced and Next-Generation Firewalls

42. In the *Cybersecurity NPRM*, we sought comment on whether to make advanced and next-generation firewalls eligible for the Pilot and, if so, how to define the scope of these terms.[142] We adopt this proposal to enable Pilot participants to protect their networks from outside cyber attackers by blocking malicious or unnecessary network traffic.[143] For purposes of the Pilot, we define an "advanced" or "next-generation" firewall as "equipment, services, or a combination of equipment and services that limits access between networks, excluding basic firewall services and components that are currently funded through the E-Rate program."[144] This definition is reflected in the P-ESL.[145]

43. We agree with the vast majority of commenters that advanced or next-generation firewalls are a logical starting point and an important tool to include in the Pilot as we study the potential use of universal service funding to protect eligible schools and libraries from cyber threats and attacks.[146] We also agree that making these tools eligible in the Pilot will provide the Commission with a stronger understanding of the technical benefits and cost implications of potentially funding these tools in the broader E-Rate program.[147] While no commenter directly opposed the view that advanced and next-generation firewalls could meaningfully improve security postures, a few commenters opined that the associated funding could be used more effectively in other ways, including to fund training of "staff and end-users."[148] We disagree with these commenters and find that funding advanced and next-generation firewalls is justified in light of the Commission's previous findings establishing the value of these

[141] *See infra* at para. 99 (discussing the three main goals).

[142] *Cybersecurity NPRM,* 2023 WL 8605080 at *17, para. 42.

[143] *See*, *e.g.*, CISA, *Understanding Firewalls for Home and Small Office Use* (Feb. 23, 2023), https://www.cisa.gov/news-events/news/understanding-firewalls-home-and-small-office-use.

[144] *See* Appendix B at 1; *see also*, *e.g.*, CoSN, ALA, SHLB Coalition, SETDA, Council GCS et al. Comments at 9-10 (CoSN et al. January 29 Comments). Excluded from our definition of "advanced" or "next-generation" firewall, and thus from eligibility in today's Pilot, are basic firewalls provided as part of the vendor's Internet service, which are funded in E-Rate as a category one service, and separately priced basic firewalls, which are funded in E-Rate as a category two service. *See, e.g.*, *Modernizing the E-Rate Program for Schools and Libraries*, WC Docket No. 13-184, Order, DA 21-1602, 2021 WL 6063032, at *7, 9 (WCB Dec. 17, 2021) (*FY 2022 ESL Order*). "Advanced" and "next-generation" firewalls, as used throughout this Report and Order, refer to equipment and services that are not currently eligible for E-Rate support and thus are distinct from the "basic firewall" equipment and services that are currently eligible for support in the E-Rate program. *See supra* para. 9; *see also Universal Service First Report and Order*, 12 FCC Rcd at 9008-15, paras. 436-49; 47 U.S.C. § 254(h)(2)(A).

[145] *See* Appendix B at 1.

[146] *See*, *e.g.*, ActZero Comments at 2-3; Cisco Comments at 7-9, 15; Clark County School District (CCSD) Comments at 1; CoSN et al. February 1 *Ex Parte* Letter at 1-2; Fortinet Reply at 2; FFL Comments at 11-12; Cybersecurity Coalition/ITI Comments at 5; Juniper Networks Comments at 2 (JN); Learning Technology Center of Illinois Reply at 1-2 (LTC); Local Education Agencies *Ex Parte* Letter at 1; MISEN Comments at 8-10; Palo Alto Networks Comments at 4; Vector Resources Inc. dba Vector USA Reply at 3 (Vector).

[147] *Id.*

[148] *See*, *e.g.*, Clear Creek Amana Express Comments (advocating for a "reduc[tion]" in the "funding of advanced or next [generation] firewalls and [a] diver[sion] [of] that funding to user awareness and staff training" instead); Apptegy, Inc. Comments at 3 (Apptegy) (opining that it would be more "impactful" to use Pilot funds for, among other things, "establish[ing] a cybersecure culture").

technologies,[149] and we find it reasonable to extend Pilot funding to these tools rather than to fund, e.g., training more broadly than described further below or the less-vetted alternatives raised by commenters. We further find that the funding of specific advanced firewall technologies will provide more quantifiable and tractable benefits compared with funding broad cybersecurity training programs, based on undetermined materials and methods.

44. However, we do agree that funding some level of training will help to ensure that the Pilot-funded equipment and services are used effectively and for maximal benefit. Accordingly, we make training eligible on terms similar to those in E-Rate, namely, when the training included "as a part of installation services but only if it is basic instruction on the use of eligible equipment, directly associated with equipment installation, and is part of the contract or agreement for the equipment" and if it "occur[s] coincidently or within a reasonable time after installation."[150] We find that this approach balances the need to ensure that applicants have access to training that will enable them to effectively oversee, interpret, and supervise the Pilot-funded equipment and services and prevent the limited Pilot funds from being disproportionately used for cybersecurity awareness training for staff and end-users,[151] thereby, limiting the number of technical solutions that can be implemented and evaluated during the course of the Pilot. However, in contrast to the E-Rate program, we do not require that the training be provided "[o]n-site" to be eligible.[152] We find it appropriate to fund off-site training as much of the equipment and services identified in the P-ESL are likely to be supplied or otherwise provided to a participant remotely. As explained above, we note that there are numerous free cybersecurity training resources already available through our federal government partners.[153] We also expect, based on our years of experience directing USAC's administration of the E-Rate program, that vendors are likely to include basic training at no additional cost as part of their sale of the eligible equipment and services.

45. We also clarify that for the purposes of today's eligibility rules, "advanced" and "next-generation" firewalls exclude services and/or equipment that are eligible in the E-Rate program. Participants are therefore required to cost allocate components or features that are eligible in E-Rate (e.g., basic firewall components and features) when seeking reimbursement for their eligible equipment and services in the Pilot. Our approach reflects a definition of the term "firewall" endorsed by the National Institute of Standards and Technology (NIST)[154] with a carve out for services and equipment that are already funded through the E-Rate program. We find it is appropriate to adopt a broad definition as this is consistent with our objective to determine the technological benefits and monetary costs associated with a wide and diverse range of tools for addressing cyber threats and attacks. At the same time, we find it reasonable to exclude from our definition basic firewall services and equipment that are currently funded

[149] The Commission has previously declined to fund advanced firewalls, even while finding that these technologies would address "legitimate concern[s]," on the basis that E-Rate program funding is constrained. *See*, *e.g.*, *Schools and Libraries Sixth Report and Order*, 25 FCC Rcd at 18762, 18808-09, para. 105; *see also Modernizing the E-Rate Program for Schools and Libraries*, WC Docket No. 13-184, Report and Order, 34 FCC Rcd 11219, 11237, para. 46 (2019).

[150] *Modernizing the E-Rate Program for Schools and Libraries*, WC Docket No. 13-184, Order, DA 23-1171, 2023 WL 8803733, at *13 (WCB Dec. 15, 2023) (*FY 2024 ESL Order*).

[151] We also note that managed cybersecurity services are eligible. *See, e.g.,* Appendix B at 3 (making eligible "Managed detection & response (MDR)" and "Managed Service Providers").

[152] *Id.*

[153] We note, for example, that CISA offers training on a variety of topics on its website. *See* CISA, *Training*, https://www.cisa.gov/resources-tools/training (last visited Apr. 1, 2024). NIST also has free training materials available at https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content (last visited Apr. 26, 2024). *See also supra* note 103.

[154] NIST, *Glossary*, https://csrc.nist.gov/glossary/term/firewall (last visited Apr. 1, 2024); *see* definition 1 (defining a firewall as "[a] gateway that limits access between networks in accordance with local security policy.")

through the E-Rate program. We find that this approach ensures that Pilot funds are spent efficiently, i.e., only on services and equipment not already funded through other USF programs, and that this approach will thus maximize the amount of data and information collected on cybersecurity tools during the Pilot. We further find that our approach provides sufficient clarity to Pilot participants, and flexibility to request funding for advanced firewalls as they may continue to evolve over the course of the Pilot, while avoiding difficulties associated with attempting to exhaustively enumerate all relevant technological features.[155] To further address commenter views, and as reflected in the P-ESL, we confirm that most, if not all, of the relevant features that commenters endorse as "advanced" and "next-generation" firewall features, including intrusion detection and prevention, application-level inspection, anti-malware and anti-virus protection, VPN, Domain Name System (DNS) security, distributed denial-of-service (DDoS) protections, and content filtering technologies, are eligible for the Pilot.[156]

46. We decline to adopt the proposal of some commenters, made in this proceeding and in response to the Bureau's recent Public Notices related to the scope of the Funding Year 2024 E-Rate ESL,[157] that we immediately make advanced and/or next-generation firewalls eligible in the E-Rate program, even as we continue to study the benefits and costs other services and equipment through the proposed Pilot.[158] Making advanced and/or next-generation firewalls immediately eligible in the E-Rate program would run directly counter to our proposed purpose of the Pilot to, among other things, "measur[e] the costs associated with . . . advanced firewall services, and the amount of funding needed to adequately meet the demand for these services if extended to all E-Rate participants."[159] As similarly noted by the National Education Organizations (EdGroup), an aim of the Pilot is to further "demonstrate the need for and costs of cybersecurity measures such as advanced firewalls, and to gauge how districts would respond to available federal funding."[160] We find it reasonable, and consistent with our obligation to be a careful steward of limited USF funds, to first study the costs and benefits of advanced and/or next-generation firewalls in the Pilot, before making any determination on whether and how to potentially make these services and equipment eligible through the E-Rate program.

b. Endpoint Protection

47. Next, we make endpoint protection, including anti-virus, anti-malware, and anti-ransomware, services and equipment eligible in the Pilot so that participants can protect their networks from potential vulnerabilities introduced by desktops, laptops, mobile devices and other end-user devices connected to their networks.[161] For the purposes of the Pilot, we define endpoint protection as

[155] *See*, *e.g.*, IOB Comments at 10.

[156] Cybersecurity Coalition/ITI Comments at 5.

[157] *See Wireline Competition Bureau Seeks Comment on Proposed Eligible Services List for the E-Rate Program*, WC Docket No. 13-184, Public Notice, DA 23-819 (WCB 2023); *see also Wireline Competition Bureau Seeks Additional Comment on Adding Wi-Fi on School Buses to Proposed Eligible Services List for the E-Rate Program*, WC Docket No. 13-184, Public Notice, DA 23-1011 (WCB 2023).

[158] *See*, *e.g.*, Council GCS Comments at 2; SHLB Coalition, ALA, CoSN, et al. *Ex Parte* Letter, WC Docket No. 13-184, at 3 (rec. July 3, 2023) (SHLB et al. July 3 *Ex Parte* Letter); ALA Reply at 3; FFL Reply at 2; LTC Reply at 1-2; Local Education Agencies *Ex Parte* Letter at 1; MISEN Comments at 7; WI DPI Reply at 2; ITI and The Cybersecurity Coalition Comments, WC Docket No. 13-184, at 5-7 (rec. Oct. 25, 2023); Tyler Moore Comments, WC Docket No. 13-184, at 1 (rec. Oct. 26, 2023); *see also FY 2024 ESL Order*, 2023 WL 8803733 at *5 (declining to address commenter requests that the Bureau add advanced and/or next-generation firewalls to the FY2024 ESL and identifying the instant proceeding as addressing related subject matter).

[159] *Cybersecurity NPRM,* 2023 WL 8605080 at *8, para. 19.

[160] EdGroup Reply at 3.

[161] *See*, *e.g.*, NIST, *Glossary*, https://csrc.nist.gov/glossary/term/endpoint_protection_platform (last visited Apr. 1, 2024) (NIST Endpoint Protection Platform).

"equipment, services, or a combination of equipment and services that implements safeguards to protect school- and library-owned end-user devices, including desktops, laptops, and mobile devices, against cyber threats and attacks."[162] This definition is reflected in the P-ESL.[163]

48. We agree with the many commenters who argue for the inclusion of specific endpoint technologies that we make eligible today.[164] We also agree with commenters that providing funding for endpoint protection should be a priority in investigating ways to improve a school's or library's network security.[165] We find that our approach is justified as school and library networks continue to evolve to include an ever increasing number of endpoint devices, including desktops, laptops, and mobile devices, that serve as points of vulnerability.[166] Moreover, we find that this approach provides funding to address the Center for Internet Security's (CIS) observations that a large percentage of cyberattacks involve ransomware, malware, web application hacking, insider and privilege misuse, and target intrusions.[167] No commenter objects to the Pilot funding endpoint protection. We further find that our definition of endpoint protection is reasonable as it largely reflects a definition endorsed by NIST, but allows for tools to be software- or non-software-based and emphasizes that, to be eligible, tools must defend against cyberattacks.[168]

c. Identity Protection and Authentication

49. We also make identity protection and authentication tools eligible in the Pilot so that participants can prevent malicious actors from accessing and compromising their networks under the guise of being legitimate users.[169] Such tools may include DNS/DNS-layer security, content blocking and filtering/URL filtering, multi-factor authentication (MFA)/phishing-resistant MFA, single sign-on (SSO) and event logging. For the purposes of the Pilot, we define identity protection and authentication as "equipment, services, or a combination of equipment and services that implements safeguards to protect a user's network identity from theft or misuse and/or provide assurance about the network identity of an entity interacting with a system."[170] This definition is reflected in the P-ESL.[171]

50. We agree with the large number of commenters who argue for the inclusion of specific

[162] *See* Appendix B at 1-2.

[163] *Id.*

[164] *See*, *e.g.*, Alliance for Digital Innovation Comments at 2 (ADI); CIS Comments at 3-4 (insider and privilege misuse, target intrusions, web application hacking), Cisco Comments at 8-9 (ani-virus, SSL inspections); CrowdStrike Comments at 1-3 (XDR); Crown Castle Comments at 3-4 (anti-ransomware); Cybersecurity Coalition/ITI Comments at 5 (anti-spam); Microsoft Corporation *Ex Parte* Letter, WC Docket No. 13-184, at 11 (rec. Aug. 2, 2023) (Microsoft August 2 *Ex Parte* Letter) (privileged Access Management); MISEN Comments at 8-10 (anti-malware).

[165] ADI Comments at 2; CIS Comments at 10; Cisco Comments at 9; Cybersecurity Coalition/ITI Comments at 4; SHLB et al. July 3 *Ex Parte* Letter at 2, 4.

[166] *See*, *e.g.*, ADI Comments at 2.

[167] CIS Comments at 3.

[168] *See* NIST Endpoint Protection Platform (defining an "endpoint protection platform" as "[s]afeguards implemented through software to protect end-user machines such as workstations and laptops against attack (e.g., antivirus, antispyware, antiadware, personal firewalls, host-based intrusion detection and prevention systems, etc.)").

[169] *See* CISA and National Security Agency (NSA), *Identity and Access Management Recommended Best Practices Guide for Administrators*, at 2-3 (Mar. 21, 2023), https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF.

[170] *See* Appendix B at 2-3.

[171] *Id.*

identity protection and authentication technologies that we make eligible today.[172] We also agree with commenters that deploying these tools will better ensure that unauthorized users will be unable to gain network access, unable to cause network damage if they do gain access, and/or provide an early warning to schools and libraries of unusual or anomalous behavior that could signal the presence of near and future cyber threats or attacks while they can still be effectively remediated.[173] No commenter objects to the Pilot funding identity protection and authentication technologies. Moreover, we find that our definition of identity protection and authentication is reasonable as it largely reflects a definition of "identity authentication" endorsed by NIST, and also clarifies that protection involves protection from theft or misuse.[174]

d. Monitoring, Detection, and Response

51. We further make network monitoring, detection and response, including the use of security operations centers (SoCs) for managed cybersecurity services, eligible in the Pilot so that participants can promptly and reliably detect and neutralize malicious activities that would otherwise compromise their networks.[175] For purposes of the Pilot, we define monitoring, detection and response as "equipment, services, or a combination of equipment and services that monitor and/or detect threats to a network and that take responsive action to remediate or otherwise address those threats."[176] This definition is reflected in the P-ESL.[177]

52. We agree with the large number of commenters who argue for the inclusion of specific monitoring, detection and response technologies that we make eligible today.[178] We also agree with

[172] *See*, *e.g.*, MISEN Comments at 8-10 (active countermeasure tools, intrusion detection systems (IDS), web content controls); Cisco Comments at 7-8, 10-11 (cloud application protection); ADI Comments at 3 (credential stuffing); Council GCS Comments at 3 (content blocking and filtering/URL filtering); Friday Institute Comments at 7 (content caching systems and service); NCTA Comments at 3-4 (customer portal services); ADI Comments at 3 (digital identity tools); Cisco Comments at 8-10 (distributed-denial-of-service (DDOS) protection and DNS/DNS-layer security, email and web security); ADI Comments at 3 (identity governance & technologies, logging practices); Crown Castle Comments at 4 (network access control); MISEN Comments at 8-10 (offsite/immutable back-ups); Cisco Comments at 9 (MFA/phishing-resistant MFA); Microsoft August 2 *Ex Parte* Letter at 11 (MFA); Friday Institute Comments at 6-7 (patching); ADI Comments at 3 (password spraying, privileged identity management); JN Comments at 4 (products with TPM chips); JN Comments at 2 (Secure Access Service Edge (SASE)); K12 SIX Comments at 2 (secure-by-design equipment and services); MISEN Comments at 8-10 (security information and event management (SIEM)); Cisco Comments at 8-9 (security updates); Friday Institute Comments at 6 (single sign-on (SSO)); JN Comments at 4 (trusted platform module (TPM)); Robert Frisby Express Comments (wireless access controllers); Zscaler Reply at 2 (zero trust architecture).

[173] ADI Comments at 3; CrowdStrike Comments at 3; Cybersecurity Coalition/ITI Comments at 4; MISEN Comments at 8-10.

[174] NIST, *Glossary*, https://csrc.nist.gov/glossary/term/identity_authentication (last visited Apr. 26, 2024) (defining "identity authentication" as "[t]he process of providing assurance about the identity of an entity interacting with a system").

[175] *See generally* CISA, *CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks* (Feb. 28, 2023), https://www.cisa.gov/sites/default/files/2023-03/aa23-059a-cisa_red_team_shares_key_findings_to_improve_monitoring_and_hardening_of_networks_1.pdf.

[176] *See* Appendix B at 3.

[177] *Id.*

[178] *See*, *e.g.*, ADI Comments at 2 (bug bounty solutions & services); ActZero Comments at 3 (compliance assessment, dark web scanning); MISEN Comments at 8-10 (data loss prevention, internal/external vulnerability scanning, network/device monitoring & response, network traffic analysis, Network Detection Response (NDR), penetration testing); MISEN Comments at 12 (managed detection & response (MDR)); Vector Reply at 1 (Managed Service Providers); ActZero Comments at 3 (maturity models); CIS Comments at 10 (Security Operations Centers (SoCs)); Microsoft August 2 *Ex Parte* Letter at 10 (SoCs); ActZero Comments at 3 (SoCs); Crown Castle

(continued….)

commenters who advocate for the inclusion of these services and equipment as an important approach to remediating cyber threats and attacks, particularly given the limited resources of schools/libraries to hire or retain staff or other personnel to conduct these activities themselves.[179] No commenter objects to the funding of network monitoring, detection and response solutions.

2. Ineligible Equipment and Services

53. We impose a number of limitations on eligibility to ensure the efficient and appropriate use of limited Pilot funds, and to avoid duplicative funding, protect against waste, fraud, and abuse, and stretch the limited support available through the Pilot. First, as noted above, we make ineligible for the Pilot funding any services, equipment, or associated cost that is already eligible through the E-Rate program.[180] We similarly make ineligible for Pilot funding any service, equipment, or associated cost for which an applicant has already received full reimbursement, or plans to apply for full reimbursement, through any other USF or federal, state, Tribal, or local government program through which reimbursement is sought.[181] Participants may, however, use Pilot funding to support Pilot-eligible services and equipment that participants were previously paying for themselves, subject to our competitive bidding rules, as this will allow the Commission to evaluate the efficacy of using universal service funding to support cybersecurity services and equipment, while potentially freeing up funding for participants to use for other needs. We find that limiting eligibility in this manner ensures that the Commission maximizes the use of the limited Pilot funding by eliminating the provision of redundant or duplicative support for the same cybersecurity services and equipment funded through other sources. It will also maximize the data and information the Commission is able to collect on new services and equipment not already funded through E-Rate or other programs, thus efficiently using Pilot resources to best inform any potential Commission action based on the Pilot data. As is customary in E-Rate, we require Pilot participants to perform a cost allocation to remove from their funding requests costs associated with ineligible components or functions of an otherwise eligible equipment or service.[182]

54. In the *Cybersecurity NPRM*, we proposed to limit eligibility to "equipment that is network-based (i.e., that excludes end-user devices, including, for example, tablets, smartphones, and laptops) and services that are network-based and/or locally installed on end-user devices, where the devices are owned or leased by the school or library," and to equipment and services that are "designed to identify and/or remediate threats that could otherwise directly impair or disrupt a school's or library's network, including to threats from users accessing the network remotely."[183] We adopt this proposal in the P-ESL with a clarification that "network-based" services include those that are cloud-based and

(Continued from previous page)
Comments at 4 (threat hunting/updates and threat intelligence); Cybersecurity Coalition/ITI Comments at 4-5 (vulnerability management); Microsoft August 2 *Ex Parte* Letter at 11 (vulnerability management).

[179] Cisco Comments at 9-11; Cybersecurity Coalition/ITI Comments at 4; Friday Institute Comments at 9; GMI Comments at 1;Vector Reply at 1.

[180] *See generally FY 2024 ESL Order* (identifying services, equipment, and associated costs that are eligible in the E-Rate program).

[181] These restrictions on duplicative funding share similarities to those in the Connected Care Pilot Program. *See*, *e.g.*, *Connected Care Pilot Order*, 35 FCC Rcd at 3399, para. 60 (declining to provide recipients with funding for data connections for which they already receiving funding, or are eligible to receive funding, through other federal programs).

[182] *See*, *e.g.*, USAC, Cost Allocations for Services, https://www.usac.org/e-rate/applicant-process/before-you-begin/eligible-services-overview/cost-allocations-for-services/ (last visited Apr. 25, 2024) (summarizing cost allocation processes in the context of E-Rate).

[183] *Cybersecurity NPRM,* 2023 WL 8605080 at *18, para. 43.

server-based. In doing so, we address concerns raised by some commenters[184] by confirming that the term "network-based" solutions includes both cloud and server-based solutions. We find this clarification appropriate since both servers and cloud architectures are used in conjunction with a network.

55. In taking this action, we disagree with the view expressed by Clark County School District (CCSD) that limiting eligibility in the way we had proposed would "not go far enough in protecting end-users."[185] Contrary to CCSD's views, our considerations for eligibility specifically encompass "end-user devices, where the devices are owned or leased by the school or library."[186] We also disagree with CTIA's view that eligibility should extend to end-user devices not owned or leased by the school or library since "leaving even one device exposed compromises an entire network."[187] While we are sympathetic to this view on a technical level, we find it administratively and financially impractical to expand eligibility to an even larger (and unknowable) number of additional devices that school and library patrons may seek to connect to their networks over the duration of the Pilot Program. For purposes of the Pilot, we therefore prioritize protection for (i.e., limit eligibility to) devices that are the most essential to a school's or library's educational mission and likely to be used to convey traffic on the networks of these participants. Our overall approach further addresses CTIA's concerns by making a wide range of network-based protections available to monitor, detect, and remediate potential threats introduced by an end-user device that does not qualify for funding under today's rules.[188] Practically speaking, schools and libraries cannot as easily limit access to their networks by their leased and owned devices while still fulfilling their core educational mission. We thus find that our approach strikes a reasonable balance between affording protections to the devices most essential and likely to be used on a school's or library's network, reducing threats that may be posed by non-funded devices (e.g., through our decision to make eligible network-level protection technologies) and effectively deploying the limited amount of Pilot funding to provide benefits to a diverse range of schools and libraries. Accordingly, for these reasons and those previously provided in the *Cybersecurity NPRM*,[189] we adopt our proposal as clarified above.

56. To further protect the Pilot's limited funds, we restrict eligibility in a number of ways. We deem ineligible (i) staff salaries and labor costs for a participant's personnel and (ii) beneficiary and consulting services that are not related to the installation and configuration of the eligible equipment and services. This mirrors restrictions in the E-Rate program that have proven to be effective in conserving limiting USF funds.[190] We expect that this action will provide similar benefits in the context of the Pilot. We similarly deem ineligible insurance costs and any costs associated with responding to specific ransom demands. We find that these restrictions are necessary to ensure that the limited Pilot funding is used for the evaluation of specific technologies, i.e., eligible cybersecurity services and equipment, so that we can

[184] Lumen Reply at 5 (requesting that we clarify that network-based services include cloud-based solutions); CCSD Comments at 2 (requesting that we make eligible cloud-based and server-based solutions); NCTA Comments at 4 (requesting that we make eligible cloud-based solutions).

[185] CCSD Comments at 1.

[186] *Cybersecurity NPRM,* 2023 WL 8605080 at *18, para. 43.

[187] CTIA Reply at 8-9 (citing CCSD Comments at 2); *see also* Northwestern Consolidated School District of Shelby County Express Comment at 1.

[188] *See generally* Appendix B.

[189] *Cybersecurity NPRM,* 2023 WL 8605080 at *18, para. 43 (reasoning that our proposed approach would be justified as it would permit Pilot participants to "cost-effectively procure remotely-located equipment and services," be "consistent with the way that many modern security services are increasingly offered," strike a "reasonable balance between protecting [Pilot participants'] networks with the need to limit the scope of protections given the limited Pilot funding available, and "reflect[] the reality that schools and libraries often already restrict the permissions available to third-party-owned devices that connect to their networks").

[190] *FY 2024 ESL Order*, 2023 WL 8803733 at *8-9.

gain maximal insight into the technical effectiveness of those offerings. We find it reasonable to exclude these enumerated uses from the Pilot, which has even more limited funding available as compared to the E-Rate program.

57. In the *Cybersecurity NPRM*, we sought comment on "whether we should place restrictions on the manner or timing of a Pilot participant's purchase of security measures," including whether "funding [should] be limited to a participant's one-time purchase of security measures or [if it] should . . . cover the on-going, recurring costs that a Pilot participant may incur, for example, in the form of continual service contracts or recurring updates to the procured security measures."[191] We received only a few comments in response with commenters suggesting that any such restrictions should be minimally burdensome and avoid unnecessarily interfering with participants' attempts to obtain funding support.[192] Accordingly, we confirm that Pilot participants may request reimbursement for one-time purchases, as well as the recurring costs of eligible security measures. As discussed above,[193] Pilot participants will be permitted to request reimbursement as expenses are incurred, whether for one-time or recurring expenses, subject to the limitations regarding participants' budgets[194] as well as funding commitments.[195]

58. *Supply Chain Restrictions.* In the *Cybersecurity NPRM*, we proposed to apply the Secure and Trusted Communications Networks Act of 2019 to Pilot participants by prohibiting these participants from using any funding obtained through the program to purchase, rent, lease, or otherwise obtain any of the services or equipment on the Commission's Covered List or to maintain any of the services or equipment on the Covered List that was previously purchased, rented, leased, or otherwise obtained.[196] We also sought comment on whether "there are any other restrictions or requirements that we should place on recipients of Pilot funds based on the Secure [and Trusted Communications] Networks Act and/or other . . . concerns related to supply chain security."[197] We adopt our proposal to bar Pilot participants from using Pilot funding in ways prohibited by the Secure and Trusted Communications Networks Act and/or the Commission's rules, including Commission rules 54.9 and 54.10, that implement the Secure and Trusted Communications Networks Act.[198] Accordingly, Pilot participants are prohibited by section 54.9 of the Commission's rules from using funding made available through the Pilot to "purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by any company posing a national security threat to the integrity of communications networks or the communications supply chain,"[199] including Huawei Technologies

---

[191] *Cybersecurity NPRM,* 2023 WL 8605080 at *16, para. 40. *See also* discussion *supra* at para. 31.

[192] Cisco Comments at 13; Dallas ISD Comments at 4.

[193] *See supra* para. 31.

[194] *See supra* paras. 25-29.

[195] *See infra* para. 85.

[196] *Cybersecurity NPRM* at *23, para. 60 (citing the Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609) (Secure and Trusted Communications Networks Act)). The Covered List is published and available here: https://www.fcc.gov/supplychain/coveredlist (last accessed Mar. 25, 2024).

[197] *Cybersecurity NPRM,* 2023 WL 8605080 at *23, para. 60.

[198] The Commission has previously found that "the prohibitions in sections 54.9 and 54.10 of the Commission's rules are consistent with, and fully implement, section 3(a) of the Secure Networks Act." *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs,* WC Docket No. 18-89, Second Report and Order, 36 FCC Rcd 14284, 14326-27, para. 96 (2020).

[199] *See* 47 CFR § 54.9.

Company and ZTE Corporation, and their parents, affiliates, and subsidiaries.[200] Pilot participants are also prohibited by section 54.10 of the Commission's rules from using Pilot funding to "[p]urchase, rent, lease, or otherwise obtain any . . . communications equipment or service" or "[m]aintain any . . . communications equipment or service previously purchased, rented, leased, or otherwise obtained" that is included on the Commission's Covered List.[201] We note that the entities, services and equipment designated under these rules may evolve over time as the Commission's Public Safety and Homeland Security Bureau (PSHSB) revises its designations of covered companies and/or issues updates to the Covered List.[202] It is the responsibility of Pilot participants to ensure they remain in compliance with the Secure and Trusted Communications Networks Act, and the Commission's related rules, if such revisions are made. We find that these actions will effectively ensure that potential risks and vulnerabilities in Pilot participants' communications networks are addressed in the manner intended and directed by Congress in the Secure and Trusted Communications Networks Act. Cisco generally supports this approach,[203] and no commenter opposes it.

E. FCC Form 484 Application and Pilot Participation Selection Processes

59. *Application Process for Pilot Program.* In this section of the Order, we adopt application and selection processes for the Pilot Program patterned after the Connected Care Pilot Program, adopt several of the application, selection, and administrative proposals from the *Cybersecurity NPRM*, and designate USAC to be the administrator for the Pilot Program. In the *Cybersecurity NPRM*, we proposed to structure the Pilot Program in a manner similar to the Connected Care Pilot Program.[204] In particular, we proposed that schools, libraries, and consortia would apply to be Pilot participants and that those entities selected to participate in the Pilot would be eligible to apply for funding for eligible cybersecurity services and equipment.[205] We also proposed that Pilot participants would receive a funding commitment and, after receipt of the commitment, would be eligible to receive cybersecurity services and equipment and submit requests for reimbursement for Pilot funding.[206] We further proposed that USAC be appointed the administrator of the Pilot Program.[207] Two commenters specifically expressed support for our proposal to structure the Pilot in a manner similar to the Connected Care Pilot Program.[208] Only one commenter, the American Library Association (ALA), addressed our proposal that USAC be appointed the administrator of the Pilot Program, explicitly agreeing that the application process and other aspects of

[200] On June 30, 2020, the Commission's Public Safety and Homeland Security Bureau (PSHSB) issued final designations of Huawei and ZTE as covered companies within the meaning of Commission rule 54.9. *See generally Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation*, PS Docket No. 19-351, Order, 35 FCC Rcd 6604 (PSHSB 2020) (*Huawei Designation Order*); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – ZTE Designation*, PS Docket No. 19-352, Order, 35 FCC Rcd 6633 (PSHSB 2020) (*ZTE Designation Order*).

[201] *See* 47 CFR § 54.10.

[202] *See*, *e.g.*, 47 CFR § 54.9 (specifying that the PSHSB may make determinations that another company or companies pose a national security threat and may reverse its prior designations in certain circumstances); 47 CFR § 1.50002 (specifying that the PSHSB "shall . . . update the Covered List" based on prescribed criteria).

[203] Cisco Comments at 17.

[204] *Cybersecurity NPRM,* 2023 WL 8605080 at *10, paras. 25-26; *see generally Connected Care Pilot Order*.

[205] *Cybersecurity NPRM,* 2023 WL 8605080 at *10, para. 26.

[206] *Id*.

[207] *Id*.

[208] IOB Comments at 6 ("IOB generally supports the Commission's proposal to structure the Pilot program similarly to the recent rural healthcare Connected Care Pilot Program . . . ."); CoSN et al. January 29 Comments at 13 ("We support the Commission's plan to model the cybersecurity pilot after the successful Connected Care Pilot.").

the Pilot Program should be administered by USAC.[209]

60. We also proposed in the *Cybersecurity NPRM* that entities interested in participating in the Pilot be required to submit a Schools and Libraries Cybersecurity Pilot Program Application (FCC Form 484) describing their proposed use of Pilot funds, including, but not limited to, the following information: (i) identification and contact information; (ii) cybersecurity posture and risk management practices; (iii) information on unauthorized access and cybersecurity incidents; (iv) the specific types of cybersecurity services and equipment to be purchased with Pilot funds; and (iv) how the entities plan to collect data and track their cybersecurity progress if selected as a Pilot participant.[210] While there was minimal opposition to the collection of general information,[211] the majority of commenters recommended against the collection of applicant-specific cybersecurity information. For example, some commenters recommended that the Commission refrain from seeking information about previous cyber threats, attacks, or incidents as part of the FCC Form 484 application.[212] Still others recommended that applicants not be required to provide details regarding their cybersecurity postures, network environments, or current protection measures (or lack thereof).[213] Several commenters recommended that the FCC Form 484 application process be minimally burdensome,[214] and a few commenters recommended that it align with E-Rate tools and concepts that are familiar to E-Rate applicants wherever possible.[215]

[209] ALA Comments at 4 ("[W]e . . . also agree that this process and other aspects of the Pilot Program should be administered by USAC.").

[210] *Cybersecurity NPRM,* 2023 WL 8605080 at *11, *20, paras. 27, 49.

[211] *See, e.g.*, Crown Castle Comments at 3 (supporting the Commission's proposed data collection and reporting requirements); Dallas ISD Comments at 4 (agreeing that applicants should be required to articulate their proposed pilot plan). *But see* State E-Rate Coordinators' Alliance Reply at 2, 4-7 (SECA) (expressing concern that applicants may not be able to describe how they plan to use Pilot program funds and recommending that "information regarding financial aspects of the proposed project" be omitted from the application).

[212] *See, e.g.*, ActZero Comments at 5 ("Program design and eligibility criteria should not be overly proscriptive or based on historical events."); ADI Comments at 3-4 (recommending that the Commission refrain from seeking information about previous cybersecurity threats or incidents as part of the application); ALA Comments at 4 (urging the Commission not to seek detailed cybersecurity information and noting that "some applicants may be reluctant to publicly disclose their security breaches"); LTC Reply at 2-3 (warning that publicly sharing information about prior offenses could open the door to future cybersecurity threats); Palo Alto Networks Comments at 2-3 (opining that disclosing details of existing vulnerabilities and incidents of unauthorized access could pose confidentiality and security concerns for applicants).

[213] *See, e.g.*, Cybersecurity Coalition/ITI Comments at 2-3 (recommending that the collection of detailed cybersecurity information be voluntary); Dallas ISD Comments at 4 (asserting that the provision of detailed cybersecurity information should not be required without an assurance of confidentiality from potential malicious actors); Palo Alto Networks Comments at 2-3 (urging that the Commission not disclose specific information about cybersecurity incidents); Zscaler Reply at 2 (recommending that any reporting requirements be "actionable, secure, and not onerous").

[214] Access, ALA, CoSN, SHLB Coalition et al. December 13 *Ex Parte* Letter at 1-2 (stating that the application should not be overly burdensome) (CoSN et al. December 13 *Ex Parte* Letter); ATARC Reply at 2 (advocating for a simplified application process); City of NY OTI Reply at 2 (concurring that that streamlining the application process is crucial); LTC Reply at 3 (noting that asking for excessive amounts of data from K-12 schools and libraries could be burdensome and a barrier to participation in the Pilot); Palo Alto Networks Comments at 3 (recommending that the Commission make the application process "as manageable as possible"); Rubrik Comments at 1 (asserting that the Commission should make the application process as easy as possible for K-12 schools and libraries); SECA Reply at 2 (describing the amount of information requested for submission on the proposed FCC Form 484 as "arduous").

[215] *See e.g.*, Lumen Reply at 6 (agreeing that the Pilot should generally mirror existing E-Rate Program rules, forms, and processes); NCTA Comments at 5 (agreeing that the Pilot program should, for the most part, mirror the existing (continued….)

61. Finally, we proposed in the *Cybersecurity NPRM* that applicants and participants submit their FCC Form 484 applications via an online platform designed and operated by USAC and inquired as to confidentiality or security concerns.[216] We also asked how the Commission could best leverage its prior experience in other USF and Congressionally-appropriated programs and sought comment on lessons learned.[217] For administrative efficiency, we further proposed that the Bureau select Pilot participants in consultation with the Office of Economics and Analytics (OEA), PSHSB, and the Office of the Managing Director (OMD), as needed.[218] We also proposed to delegate to the Bureau the authority to implement the proposed Pilot and direct USAC's administration of the program consistent with the Commission's rules and oversight.[219] No commenter addressed the submission of the FCC Form 484 applications using an online platform designed and operated by USAC, though some expressed concerns about the confidentiality and security of cybersecurity data provided as part of the application process.[220] Comments related to past experience and lessons learned focused on the requests for reimbursement and invoicing processes, [221] are discussed later in this Report and Order. Many commenters supported the Commission's legal authority to conduct the Pilot Program,[222] but did not address Bureau review of Pilot Program applications in consultation with OEA, PSHSB, and OMD, or the delegation of authority to the Bureau to implement the Pilot or direct USAC's administration of the Pilot.

62. Based on the record, we adopt several of the proposals from the *Cybersecurity NPRM*. Specifically, we adopt the application, selection, and administrative proposals discussed in detail below, and we designate USAC to be the administrator of the Pilot. In doing so, we are mindful of the concerns expressed by commenters about the scope of information to be included in the FCC Form 484 application and agree that the initial application process would benefit from a decrease in the amount of cybersecurity-sensitive school and library data requested.[223] To that end, and as discussed in greater detail below, the FCC Form 484 application will be split into two parts. The first part will collect a more general level of cybersecurity information about the applicant and its proposed Pilot project, and will use pre-populated data where possible, as well as a number of "yes/no" questions and questions with a predetermined set of responses (i.e., multiselect questions with predefined answers). The second part will collect more detailed cybersecurity data and Pilot project information, but only from those who are

(Continued from previous page)
E-Rate rules); *see also* CoSN et al. August 7 *Ex Parte* Letter (recommending that the application process align whenever possible with tools and concepts familiar to E-rate applicants).

[216] *Cybersecurity NPRM,* 2023 WL 8605080 at *11, para. 27.

[217] *Id*.

[218] *Id*.

[219] *Id*.

[220] *See e.g.*, CIS Comments at 5; City of NY OTI Reply at 2; Dallas ISD Comments at 4; Palo Alto Networks Comments at 2-3; Friday Institute Comments at 8; WI DPI Reply at 2-3.

[221] *See e.g.,* Dallas ISD Comments at 4 ("As with the application evaluation process and lessons learned from ECF, requests for reimbursement or invoices submitted appropriately to the Administrator should likewise be processed in a timely, predictable, and reliable manner.").

[222] *See infra* para. 114.

[223] We recognize that FCC Form 484 applications could contain sensitive information. As such, the USAC cybersecurity platform that applicants, and participants once selected for the Pilot, will use to submit their FCC Form 484 applications will be a closed system that can only be accessed by the applicant or participant, USAC, and the FCC. Applicants and participants will not be able to view each other's FCC Form 484 applications and the FCC Form 484 data will not be made available to the public. However, the other Pilot form data, FCC Forms 470, 471, and 472/474 data, may be publicly available as federal funding is being provided to the Pilot participants, and the public data may include the name of the Pilot participant, services and equipment requested, names of service providers, and the amount of Pilot funding committed and disbursed.

selected as Pilot participants.[224] As discussed further below, we will treat all cybersecurity-related information requested and provided in the FCC Form 484 as presumptively confidential, and will not make it routinely available for public inspection.[225]

63. To be considered for the Pilot, an applicant must complete and submit part one of the FCC Form 484 application describing its proposed Pilot project and providing information to facilitate the evaluation and eventual selection of high-quality projects for inclusion in the Pilot.[226] Specifically, the applicant must explain how its proposed project meets the considerations outlined below. In addition, the applicant must present a clear strategy for addressing the cybersecurity needs of its K-12 school(s) and/or library(ies) pursuant to its proposed Pilot project, and clearly articulate how the project will accomplish the applicant's cybersecurity objectives. We anticipate that successful applicants will be able to demonstrate that they have a viable strategic plan for providing eligible cybersecurity services and equipment directly to the school(s) and/or library(ies) included in their proposed Pilot projects. Further, we expect applications to be tailored to the unique circumstances of each applicant. USAC and/or the Bureau may disqualify from consideration for the Pilot those applications that provide a bare minimum of information or are generic or template in nature.

64. *Part One Application Information.* For the first part of the FCC Form 484 application, we direct the Bureau and USAC to collect a general level of cybersecurity information from schools, libraries, and consortia that apply to participate in the Pilot Program. At a minimum, applications to participate in the Pilot Program must contain the following required information:

- Names, entity numbers, FCC registration numbers, employer identification numbers, addresses, and telephone numbers for all schools, libraries, and consortium members that will participate in the proposed Pilot project, including the identity of the consortium leader for any proposals involving consortia.
- Contact information for the individual(s) who will be responsible for the management and operation of the proposed Pilot project (name, title or position, telephone number, mailing address, and email address).
- Applicant number(s) and type(s) (e.g., school; school district; library; library system; consortia; Tribal school or library (and Tribal affiliation)), if applicable, and current E-Rate participation status and discount percentage, if applicable.[227]

[224] To clarify, the FCC Form 484 itself will not change from the proposed form circulated as part of the Commission's initial information collection submission to the Office of Management and Budget, nor will it increase the burden time for applicants or participants. Rather, this approach will streamline the initial application process, allowing for the submission of an increased number of applications from a more diverse array of applicants and will restrict the collection of particularly sensitive cybersecurity data to only those who are selected as Pilot participants.

[225] *See* 47 CFR § 0.457(d)(2); *see also infra* para. 76. Note that material submitted is still subject to the Commission's rules governing requests for inspection of records not routinely available for public inspection. *See* 47 CFR § 0.461.

[226] *See Cybersecurity NPRM,* 2023 WL 8605080 at *20, para. 49. In order to facilitate the application review process, and pursuant to the Paperwork Reduction Act of 1995 (PRA), the Commission sought OMB approval for a Schools and Libraries Cybersecurity Pilot Program Application Form concurrent with the release of the *Cybersecurity NPRM* for applicants to use when submitting their proposed Pilot projects to the Commission. Although the original comment periods for the application form have passed, as part of the information collection process, parties will have another opportunity to comment on the form. *Notice of Office of Management and Budget Action*, OMB Control No. 3060-1323, Comment on Proposed Rule (requesting resubmission of information collection when proposed rule is finalized which will result in an additional 30-day comment period).

[227] Note that there is no need for an applicant to indicate its urban or rural status, as that information will be auto-populated by USAC based on U.S. Census Bureau data that is also used in the E-Rate program for this determination.

- A broad description of the proposed Pilot project, including, but not limited to, a description of the applicant's goals and objectives for the proposed Pilot project, a description of how Pilot funding will be used for the proposed project, and the cybersecurity risks the proposed Pilot project will prevent or address.

- The cybersecurity equipment and services the applicant plans to request as part of its proposed project, the ability of the project to be self-sustaining once established, and whether the applicant has a cybersecurity officer or other senior-level staff member designated to be the cybersecurity officer for its Pilot project.

- Whether the applicant has previous experience implementing cybersecurity protections or measures (answered on a yes/no basis), how many years of prior experience the applicant has (answered by choosing from a preset menu of time ranges (e.g., 1 to 3 years)), and whether the applicant has experienced a cybersecurity incident within a year of the date of its application (answered on a "yes/no" basis), information about the applicant's participation or planned participation in cybersecurity collaboration and/or information-sharing groups.

- Whether the applicant has implemented, or begun implementing, any Education Department or CISA recommendations (answered on a "yes/no" basis), a description of any Education Department or CISA free or low-cost cybersecurity resources that an applicant currently utilizes or plans to utilize, or an explanation of what is preventing an applicant from utilizing these available resources.

- An estimate of the total costs for the proposed Pilot project, information about how the applicant will cover the non-discount share of costs for the Pilot-eligible services, and information about other cybersecurity funding the applicant receives, or expects to receive, from other federal, state, local, or Tribal programs or sources.

- Whether any of the ineligible services and equipment the applicant will purchase with its own resources to support the eligible cybersecurity equipment and services it plans to purchase with Pilot funding will have any ancillary capabilities that will allow it to capture data on cybersecurity threats and attacks, any free or low-cost cybersecurity resources that the applicant will require service providers to include in their bids, and whether the applicant will require its selected service provider(s) to capture and measure cost-effectiveness and cyber awareness/readiness data.

- A description of the applicant's proposed metrics for the Pilot project, how they align with the applicant's cybersecurity goals, how those metrics will be collected, and whether the applicant is prepared to share and report its cybersecurity metrics as part of the Pilot Program.

To facilitate the inclusion of a diverse set of Pilot projects and to target Pilot funds to the populations most in need of cybersecurity support, we anticipate selecting projects from, and providing funding to, a combination of large and small and urban and rural schools, libraries, and consortia, with an emphasis on funding proposed Pilot projects that include low-income[228] and Tribal applicants.[229] Similarly, and

[228] *See* 47 CFR § 54.2007. For purposes of the Pilot program, an applicant is considered "low-income" based on its discount percentage which, in turn, is determined by indicators of poverty and urban/rural designation. *Id.* The discounts available to applicants selected to participate Pilot range from 20 percent to 90 percent of the pre-discount price for all eligible services and equipment provided by eligible providers, with 90 percent discounts representing the neediest applicants. *Id*., § 54.2007(b).

addressing concerns expressed by ActZero, we encourage participation in the Pilot by a broad range of service providers and note that the rules and requirements we adopt here do not discourage new companies from participating.[230] Nor do we require service providers to have preexisting service provider identification numbers (SPIN) before submitting cybersecurity bids or previous E-Rate experience before participating in the Pilot. [231]

65. When an applicant submits part one of its FCC Form 484 application, it will be required to certify, among other things, that it is authorized to submit the application and is responsible for the data being submitted; the data being submitted is true, accurate, and complete; if selected for the Pilot, it will comply with all rules and orders governing the program, including the competitive bidding rules and the requirement to pay the non-discount share of costs for Pilot-eligible services and equipment from eligible sources; all requested Pilot-funded eligible services and equipment will be used for their intended purposes; the schools, libraries, and consortia listed in the FCC Form 484 application are not already receiving, and do not expect to receive, other funding for the same cybersecurity services and equipment for which Pilot funding is being sought; it may be audited pursuant to its Pilot Program application and will retain any and all records related to its application for ten years; and, if audited, it will produce those records at the request of the appropriate officials.[232] The applicant must also certify that it understands that failure to comply with the Pilot Program rules and order(s) may result in the denial of funding, cancellation of funding commitments, and/or the recoupment of past funding disbursements.[233] We emphasize that we are committed to protecting the integrity of the Pilot and ensuring that USF funds disbursed through the Pilot are used for eligible and appropriate purposes. In the event of a violation of Pilot Program rules or requirements, the Commission reserves the right to take appropriate actions, including, but not limited to, seeking recovery of funds or further enforcement action. Applicants who participate in the Pilot Program must also comply with all applicable federal and state laws, including sections 502 and 503(b) of the Act, Title 18 of the United States Code, and the federal False Claims Act.[234]

66. While we understand the desire by some commenters to keep the initial application as streamlined as possible,[235] in order to evaluate the proposed Pilot projects and select well-defined and

(Continued from previous page)

[229] *See id.*, § 54.2000 (explaining that an entity is "Tribal" if it is a school operated by or receiving funding from the Bureau of Indian Education (BIE), or if it is a school or library operated by any Tribe, Band, Nation, or other organized group or community, including any Alaska native village, regional corporation, or village corporation (as defined in, or established pursuant to, the Alaska Native Claims Settlement Act (43 U.S.C. § 1601 *et seq*.) that is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians).

[230] ActZero Comments at 7.

[231] *Id*. We will require new service providers participating in the Pilot to submit a Service Provider and Billed Entity Identification Number and General Contract Information Form (FCC Form 498) to obtain a service provider identification number (SPIN) in order to provide the requested services/equipment and receive reimbursement.

[232] *See* 47 CFR § 54.2004(c)(2).

[233] *Id*.

[234] *See* 47 CFR § 54.2004(c)(2)(i)(A) (requiring an applicant to certify acknowledgement that any false statement on its application or on other documents it submits as part of the Pilot program can be punished by fine or forfeiture under the Act (47 U.S.C. §§ 502, 503(b)), or fine or imprisonment under Title 18 of the United States Code (18 U.S.C. § 1001), or can lead to liability under the federal False Claims Act (31 U.S.C. §§ 3729–3733)) and 47 CFR § 54.2004(c)(2)(i)(C) (requiring an applicant to certify awareness that any false, fictitious, or fraudulent information, or the omission of any material fact, may subject it to criminal, civil or administrative penalties for fraud, false statements, false claims, or otherwise pursuant to U.S. Code Title 18, §§ 1001, 286–287 and 1341, and Title 31, §§ 3729–3730 and 3801–3812).

[235] *See supra* para. 60, note 214.

sustainable projects, it is incumbent on us to require certain information at the application stage. Thus, we disagree with commenters who say that applicants will need to possess a prohibitive amount of knowledge during the application stage and will not be able to describe how they propose to use Pilot Program funds until *after* they have been selected as Pilot participants.[236] Although an applicant may not know the precise cybersecurity services and equipment it would seek to fund with Pilot funding, it is unlikely that an applicant would apply to participate in the program without having some general cybersecurity goals or plans for using the funding, if selected as a participant. Additionally, this Report and Order contains a list of Pilot-eligible services and equipment that will aid applicants as they begin formulating their proposed Pilot projects in advance of the opening of the FCC Form 484 application window.[237] Applicants, therefore, should do their best to provide the requested information in the application, including information on estimated costs related to their proposed cybersecurity project.

67. *Selection Process for Pilot Program*. To select Pilot participants, we direct the Bureau and USAC to use limited prerequisites and a broad and objective set of evaluation factors with an emphasis on funding low-income and Tribal entities, consistent with the E-Rate and Connected Care Pilot programs.[238] In the *Cybersecurity NPRM*, we sought comment on how to evaluate and prioritize Pilot applications. In particular, we sought comment on what prerequisites, if any, the Commission should adopt to select participants.[239] For example, we asked whether the adoption of free and low-cost cybersecurity tools and resources should be required for an applicant to be selected as a Pilot participant; Pilot participants should be required to correct known security flaws and conduct routine back-ups; Pilot participants should be required to join cybersecurity information-sharing groups, such as MS-ISAC or K12 SIX; Pilot participants should be required to implement, or demonstrate their plans to implement, recommended best practices from organizations like the Education Department, CISA, and NIST; and Pilot participants should be required to take steps to improve their cybersecurity posture by designating an officer or senior staff member to be responsible for cybersecurity implementation, updates, and oversight.[240] The Commission received mixed reactions to its proposed use of prerequisites to select Pilot participants. At least one commenter thought the Commission should not utilize prerequisites to determine Pilot participation.[241] Commenters were split on the proposal to require the adoption of free and low-cost cybersecurity tools and resources for an applicant to be selected as a Pilot participant.[242] No

[236] *See, e.g.,* SECA Reply at 2, 4-7.

[237] *See supra* para. 37 and *infra* Appendix B (discussing and adopting a Pilot program ESL).

[238] *See* 47 CFR § 54.505(c) (setting discount rates based on the entity's level of poverty and location in an urban or rural area); *Connected Care Pilot Order*, 35 FCC Rcd at 3405-3408, para. 68 (seeking information on "whether the health care provider is located in a rural area, on Tribal lands, or is associated with a Tribe" and "whether the health care provider will primarily serve veterans or low-income patients" to facilitate selection of a diverse set of pilot projects).

[239] *Cybersecurity NPRM,* 2023 WL 8605080 at *15, para. 37.

[240] *Id*.

[241] Palo Alto Networks Comments at 2 (asserting that "a lack of cybersecurity education, training, and risk management practices should not immediately disqualify K-12 organizations from participating" in the Pilot).

[242] *Compare* CCSD Comments at 1 ("Requiring applicants to show they are leveraging free and low-cost tools is burdensome and such tools do not sufficiently protect an applicant's network."); CIS Comments at 4, 8 (stating that "[t]he FCC should not require implementation of specific free and low-cost tools for participant eligibility for Pilot funding"); Council GCS Comments at 4 (explaining that many urban districts are already implementing several low-cost and high-leverage cybersecurity strategies and requiring implementation or use of specific free and low-cost tools could eliminate under-resourced districts from the pool of applicants) *with* CTIA Reply at 9 (supporting mandating that K-12 schools and libraries that participate in the Pilot fully leverage the free and low-cost K-12 cybersecurity resources provided by CISA and the Education Department); SECA Reply at 5 (recommending that the Commission specify that using the free vulnerability assessment offered by CISA is sufficient for meeting the application prerequisite requirement).

commenter spoke directly to whether Pilot participants should be required to correct known security flaws or conduct routine back-ups as part of the Pilot Program, though a small number of commenters discussed whether Pilot funding should be targeted to allow schools and libraries to implement some or all of the items contained in the CISA list of highest priority steps.[243] Some commenters thought requiring Pilot participants to join cybersecurity information-sharing groups was too onerous,[244] while others found such a requirement beneficial.[245] Some commenters supported the requirement for Pilot participants to implement, or demonstrate plans to implement, recommended best practices from organizations like the Education Department, CISA, and NIST or recommended using the best practices to evaluate Pilot Program success,[246] though at least one commenter expressed reservations about the Commission doing so.[247] The State E-Rate Coordinators Alliance (SECA) proposed that the Commission "specify that completion or submission of an application for the free vulnerability assessment offered by CISA . . . [be] sufficient for meeting the assessment prerequisite as part of the Form 484 application process."[248] Clear Creek Amana, however, cautioned against relying on federal resources outside of a limited incident response plan following the NIST frameworks.[249] A few commenters supported the proposal that a school, library, or consortium should have implemented or begun implementing a cybersecurity framework or program to participate in the Pilot.[250] However, others called for selection based on a holistic view of an applicant's cybersecurity expertise and risk.[251] CIS stated that designating an officer or senior staff member to be responsible for cybersecurity implementation, updates, and oversight was an important step towards cyber maturity that should be achievable by Pilot participants.[252] ADI similarly recommended that the Commission make leadership commitment a requirement to participate in the Pilot Program, noting that "[s]enior leadership commitment plays a pivotal role in prioritizing cybersecurity

[243] *See, e.g.*, CIS Comments at 3; IOB Comments at 5.

[244] *See e.g.*, Cybersecurity Coalition/ITI Comments at 3 (expressing reservations about requiring applicants to join existing information sharing and collaboration groups but finding it appropriate for the Commission to encourage applicants to voluntarily participate in such groups and establish a relationship with CISA and FBI field personnel); EdGroup Reply at 4 (asserting that schools and libraries should not be required to make use of federal government tools and resources, as suggested by the *Cybersecurity NPRM*, because many schools and libraries have already implemented their own cybersecurity strategies).

[245] *See, e.g.*, CIS Comments at 8 (requiring Pilot participants to seek no-cost MS-ISAC membership is appropriate because it can expose them to a community of their peers and experts in the cybersecurity that can assist them); K12 SIX Comments at 3 (stating that the Pilot should incentivize the sharing of threat intelligence, including by requiring membership in information sharing and collaboration groups).

[246] *See e.g.*, CIS Comments at 8; CoSN et al. January 29 Comments at 15.

[247] IOB Comments at 5 (expressing concern regarding the "[p]proposal to devote scarce Pilot program funds to advance the cybersecurity priorities of other government agencies such as CISA, [the Education Department], and NIST").

[248] SECA Reply at 5 (referencing the free vulnerability assessment offered by CISA at https://www.cisa.gov/cyber-hygiene-services but specifying that the requirement should not extend to the implementation of specific free and low-cost tools).

[249] Clear Creek Amana Express Comments.

[250] *See e.g.*, Apptegy Comments at 2 (urging the Commission to align the Pilot as much as possible with CISA's CPGs and recommendations); CIS Comments at 4-5 (recommending the Commission require Pilot participants to assess themselves before the Pilot and annually against a recognized cybersecurity framework).

[251] *See e.g.*, ADI Comments at 3-4; Coalition/ITI Comments at 3; Zscaler Reply at 2.

[252] CIS Comments at 8; *accord* Zscaler Reply at 3 (underscoring the importance of leadership commitment to cybersecurity because it is "essential for prioritizing cybersecurity initiatives, allocating resources, and fostering a culture of security within educational institutions").

within organizations."[253]

68. We also asked questions about reliance on objective versus subjective factors and how such factors should be used to select Pilot participants. In terms of objective factors, we asked whether the selection of Pilot participants should be based on E-Rate category two discount rate levels, location (e.g., urban vs. rural), and/or participant size (i.e., small vs. large).[254] We also sought comment on whether certain of those factors are more or less important than others from a Pilot selection standpoint and requested the underlying rationale for such determinations.[255] Commenters generally agreed that the Pilot should prioritize the neediest applicants or those applicants that qualify for the highest discount percentages in the E-Rate program.[256] Commenters overwhelmingly supported the Commission's proposal to incorporate a diverse array of applicants in the Pilot, including both urban and rural and large and small participants.[257] Many commenters advocated for the preferential selection of consortia and statewide, regional, and local government applications, noting that such applications allow schools and libraries to stretch their cybersecurity dollars and extend cybersecurity protections to a larger pool of recipients.[258] Similarly, other commenters encouraged the Commission to enable school districts to work across district and community boundaries to participate in the Pilot Program.[259]

69. For subjective Pilot selection factors, we inquired as to whether the Pilot Program would benefit from including schools and libraries with advanced cybersecurity expertise only or whether cybersecurity expertise should not factor into Pilot participant selection at all.[260] Relatedly, we also

[253] ADI Comments at 4-5.

[254] *Cybersecurity NPRM,* 2023 WL 8605080 at *13, para. 34.

[255] *Id*.

[256] *See, e.g*., CoSN, ALA, Council GCS, SECA, SETDA, SHLB Coalition et al. January 10 *Ex Parte* Letter at 2 (CoSN et al. January 10 *Ex Parte* Letter); Council GCS Comments at 3-4; Crown Castle Comments at 4; Dallas ISD Comments at 3; EdGroup Reply at 5.

[257] *See e.g.*, ALA Comments at 5; ALA Reply at 2-3; ASCA-CSBA Federal Partnership Reply at 3-4; CoSN et al. January 29 Comments at 14; EPIC Reply at 4; EdGroup Reply at 5-6; NTCA Comments at 1; Palo Alto Networks Comments at 2; WI DPI Reply at 3.

[258] *See, e.g.*, ALA Reply at 1-2 (suggesting that the Commission "consider offering some type of priority status for consortium applications that include smaller libraries and schools"); Allendale Reply at 2 (highlighting the buying power of regional and state-wide collaboratives); CCSD Comments at 1 (suggesting rewarding collaborative efforts that benefit the greatest number of applicants and end users); Cybersecurity Coalition/ITI Comments at 6 (suggesting that to maximize the Pilot budget, the Commission consider a preference for applications that aggregate the needs of multiple schools and libraries); E-Rate Central Comments at 2 (urging the Commission and USAC to encourage larger and more resourceful Pilot applicants to incorporate smaller less technically savvy entities in their consortium applications); K12 SIX Comments at 5-6 (asserting that the Pilot should "incentivize and encourage consortia applications that can provide valuable services at scale across regions and states"); MISEN Comments at 3 ("Consortia entities should be specifically identified as eligible Pilot program applicants.") and 11 (explaining that allowing consortia to participate in the Pilot will stretch the limited funding and increase the impact for more students and schools); Microsoft Comments at 3 ("One way to incentivize approaches that optimize cyber-hygiene while minimizing waste and inefficiency would be to prioritize funding for state-wide deployment efforts."); Wayne RESA Reply at 2 (supporting eligibility for consortia applicants because they can help drive down costs and provide support for layers of needed protections); WI DPI Reply at 3 (agreeing that the Commission and USAC should encourage larger and more resourceful pilot applicants to incorporate smaller and less technically savvy entities into consortium applications).

[259] *See, e.g.*, ACSA-CSBA Federal Partnership Reply at 4; City of NY OTI Reply at 2; MISEN Comments at 3 ("Shared resources should be incentivized in Pilot program participants. Applicants should be encouraged to be creative in launching partnerships with other agencies and groups for the benefit of the greater good."); Microsoft Comments at 3; Questar Comments at 1.

[260] *Cybersecurity NPRM,* 2023 WL 8605080 at *13, para. 34.

sought comment on how the Commission could ensure that schools and libraries that lack funding, expertise, or are otherwise under-resourced could meaningfully participate in the Pilot.[261] We asked commenters to address whether Pilot participants should be required to demonstrate that they have started to take actions to improve their cybersecurity posture.[262] Conversely, we also asked commenters whether a school or library should be required to provide a certification or other confirmation that, absent participation in the Pilot, it does not have the resources to start implementing CISA's K-12 cybersecurity recommendations.[263] Commenters generally agreed that the Pilot would most benefit from including participants with a mix of cybersecurity expertise and varying cybersecurity postures.[264] With respect to how to ensure that under-resourced schools and libraries are able to meaningfully participate in the Pilot, commenters suggested that the FCC and USAC conduct early and detailed Pilot Program outreach,[265] including providing technical and other assistance to those applicants who are likely to need it most.[266] No commenters addressed the proposal that a school or library be required to provide a certification or other confirmation that it does not have the resources to start implementing the CISA K-12 cybersecurity recommendations absent selection for the Pilot. CTIA recommended that applicants be required to disclose funding from non-Pilot sources and explain how Pilot Program funding would complement, but not duplicate, the applicant's existing cybersecurity tools and support.[267]

70. Along these same lines, we also asked whether participation in the Pilot should be limited to those schools and libraries that have faced or are facing particular types of cybersecurity threats or attacks.[268] In particular, we sought comment on the types of cybersecurity threats and attacks encountered by schools and libraries and how they should be evaluated, if at all, when selecting Pilot participants[269] and similarly, whether an applicant's previous history of cybersecurity threats or attacks should be taken into consideration as part of the Pilot Program selection process.[270] We also asked what role, if any, cybersecurity risk, geographic or socioeconomic factors, staffing constraints or financial

[261] *Id*.

[262] *Id*.

[263] *Id*.

[264] *See, e.g.*, CIS Comments at 6 (stating that the Pilot should not be limited to institutions that have suffered cyberattacks); Palo Alto Networks Comments at 2 (stating that current cybersecurity posture should not be an initial decision factor in the application process); SECA Reply at 3 (stating that Schools and libraries may not be sophisticated enough to have a current cybersecurity plan); WI DPI Reply at 3 (limiting the Pilot to only applicants with advanced cybersecurity will narrow the pool and will not be representative of all E-rate applicants).

[265] *See, e.g.*, ALA Comments at 5-6 ("A critical issue in this regard is that assistance from USAC must start early in the application process, well before the actual application filing deadline. Some may argue that such outreach compromises a desire to maintain a more 'hands-off' objective process to select participants. But we say that for under-resourced applicants it is more important to get the right applicants and to do what is needed to ensure this, vs. a more independent selection process.").

[266] *See, e.g.*, ACSA-CSBA Federal Partnership Reply at 4-5 (urging the Commission to direct USAC to provide technical assistance in advance of the application period); ALA Comments at 5 (stating that without considerable support from USAC, the Commission will likely get a smaller number of applications from small libraries or will get applications of lower quality when compared to larger libraries); City of NY OTI Reply at 2 (recommending the provision of "readily accessible support resources to assist with the application process"); WI DPI Reply at 3 (agreeing with ALA that the Commission should require USAC to provide direct, hands-on support for smaller applicants).

[267] CTIA Reply at 10.

[268] *Cybersecurity NPRM,* 2023 WL 8605080 at *14, para. 35.

[269] *Id*.

[270] *Id.*, para. 36.

need, or technical challenges should play in Pilot participant selection.[271] Commenters urged the Commission to forgo reliance on whether an applicant has faced or is facing a particular type of cybersecurity threat or attack, an applicant's previous history with cybersecurity threats or attacks, or the frequency with which an applicant has experienced a cybersecurity incident as drivers of Pilot participant selection.[272] Commenters were generally supportive of selecting and prioritizing applicants who face geographic, socioeconomic, financial, and other challenges, or who serve low-income and under-resourced populations.[273]

71. We agree with commenters who support using a broad and objective set of evaluation factors to select Pilot Program participants. After reviewing the record, we conclude that the Pilot Program goals will best be served by directing funding to: (1) the neediest eligible schools, libraries, and consortia who will benefit most from cybersecurity funding (i.e., those at the highest discount rate percentages); (2) as many eligible schools, libraries, and consortia as possible; (3) those schools, libraries, and consortia that include Tribal entities; and (4) a mix of large and small and urban and rural, schools, libraries, and consortia. Selecting Pilot participants in this manner is consistent with our standard practice in E-Rate of prioritizing funding for the most resource-constrained schools, libraries, and consortia and is logical to apply here. It also achieves our goal of ensuring that the Pilot contains a diverse cross-section of applicants with differing cybersecurity postures and experiences. We direct the Bureau to weigh these considerations during the Pilot application review and participant selection processes.

72. We have considered commenters' suggestions regarding the potential application factors and have determined that the considerations outlined above will provide us with meaningful information with which we can select Pilot projects and participants. We acknowledge that commenters suggested we weigh other considerations, but we believe that the considerations listed above best enable us to select high-quality projects that will meet Pilot goals and target Pilot funding to the schools and libraries with the greatest need. Further, each of these considerations play an important part in helping us better understand the relationship of certain cybersecurity services and equipment to the overall cybersecurity health and posture of entities in varying contexts and with varying levels of cybersecurity expertise.

73. We direct the Bureau and USAC to review the applications and select Pilot projects and participants based on applicants' responses, weighing the considerations listed above,[274] in combination

[271] *Id*.

[272] *See, e.g.*, ActZero Comments at 5; ADI Comments at 4; CIS Comments at 6-7; CrowdStrike Comments at 5; Cybersecurity Coalition/ITI Comments at 3; Dallas ISD Comments at 4; LTC Reply at 3; Palo Alto Networks Comments at 2; Rubrik Comments at 3; WI DPI Reply at 3; Zscaler Reply at 2.

[273] ACSA-CSBA Federal Partnership Reply at 4-5 (encouraging the Commission to provide technical assistance to help under-resourced school districts participate Pilot and expressing concern that Pilot funding may disproportionately be awarded to applicants with greater resources); ALA Comments at 5 (encouraging the Commission to assist schools in smaller, rural communities); CoSN et al. December 13 *Ex Parte* Letter at 2 (encouraging the Commission to prioritize high-need schools and libraries consistent with E-Rate but also ensure that applicants of all sizes are eligible to participate Pilot); CoSN et al. January 29 Comments at 14 (encouraging the Commission to prioritize the inclusion of the highest need schools and libraries consistent with E-Rate and select a higher amount of the most impoverished applicants that request to participate in the Pilot); EdGroup Reply at 5 (encouraging the Commission to prioritize the highest need schools and libraries consistent with E-Rate by oversampling high financial need schools and libraries within each of the Pilot's target demographics); Rochester Institute of Technology (RIT) *Ex Parte* Letter at 3 (explaining that "many districts with budget constraints often are forced to hire teachers who are also required to take on part-time IT administrator roles" and "[w]ith only 24 hours in a day, it is challenging for them to do both roles well"); Quilt Reply at 2 (explaining that "while K-12 has the experience and expertise available to implement cybersecurity protections, the human, technological, and financial resources needed to do so are currently spread too thin).

[274] *See supra* para. 64.

with the applicants' category one discount rates.[275] In selecting Pilot projects and participants, limited initial screening prerequisites should be employed, but the Bureau and USAC may exclude applications that are incomplete or do not meet Pilot Program eligibility standards.[276] The Bureau and USAC should also work to ensure that, to the extent feasible and based on qualified applications, Pilot Program funding is not heavily concentrated in any particular state or region, and instead is distributed widely throughout the United States, including the District of Columbia and the U.S. territories, with an emphasis on funding proposed Pilot projects that include low-income and Tribal applicants.[277] We decline to require Pilot applicants or participants to join information-sharing organizations like MS-ISAC, though we highly encourage all applicants or participants to do so.[278] In choosing participants for the Pilot, the Bureau and USAC should also consider the cost of the proposed Pilot project compared to the total Pilot Program cap. This does not mean that proposed Pilot projects should be evaluated based on their total project budgets, but, rather, the Bureau and USAC should seek to select an array of Pilot projects with varying costs that can all be funded within the Pilot Program's cap. In addition, the Bureau and USAC should seek to select an array of Pilot participants with differing levels of exposure to cybersecurity threats and attacks.[279] Although applicants' responses will be considered consistent with the considerations listed above when evaluating proposed Pilot projects, the considerations are not determinative of whether a Pilot project will be selected because we recognize that each proposed Pilot project will have its own unique strengths and potential challenges. Our goal is to ensure the selection of proposed Pilot projects that present a well-defined plan for meeting the cybersecurity needs of specific schools, libraries, or consortia, with a particular emphasis on resource-challenged and Tribal applicants and the three Pilot Program goals discussed in greater detail later in this Order.

74. *Prioritization*. In the event that the number of FCC Form 484 applications received exceeds the number of projects that can be funded through the Pilot, we direct the Bureau and USAC to prioritize the selection of Pilot participants by considering their funding needs in combination with the funding needs of the same type(s) of applicants.[280] As previously discussed, under the rules for the Pilot, eligible schools and libraries may receive discounts ranging from 20 percent to 90 percent of the pre-discount price of eligible services and equipment, based on indicators of need.[281] Schools and libraries in areas with higher percentages of students eligible for free or reduced-price lunch through the National School Lunch Program (or a federally approved alternative mechanism) qualify for higher discounts for

[275] *See supra* para. 30.

[276] *See generally Cybersecurity NPRM,* 2023 WL 8605080 at *1, 8-10, 13, 15, 19, 22 paras. 2, 19-24, 34, 37-38, 47, 56; *see also* 47 CFR § 54.2002 (Eligible Recipients). Other prerequisites that the Commission may employ during initial screening are whether an applicant indicates a willingness to follow Pilot program rules and procedures (including Pilot reporting requirements) or will be unable to pay for Pilot-ineligible items or its share of the cost of Pilot-eligible items.

[277] *See, e.g.*, CoSN et al. January 29 Comments at 14 ("Additionally, the Commission should seek to ensure the group of pilot participants reflect diverse characteristics, such as being located throughout the country, in rural and urban areas, and range in size from small to large organizations.").

[278] *See, e.g.*, CIS Comments at 8 ("The FCC should require Pilot participants to seek no-cost MS-ISAC membership as it can expose schools and libraries to a burgeoning community of their peers and experts in the cybersecurity industry that would assist in improving their cybersecurity maturity and expose them to no and low-cost solutions that are available to them.").

[279] We will not eliminate proposed Pilot projects based on an applicant's cybersecurity maturity or posture, but, rather, we will consider an applicant's cybersecurity maturity and posture, including whether the applicant has successfully developed or otherwise implemented a cybersecurity and/or incident response plan, to select a variety of Pilot projects.

[280] *See supra* para. 24.

[281] *See* 47 CFR § 54.2007.

eligible services than those with lower levels of eligibility for such programs.[282] Our priority rules for the Pilot provide that funds shall be allocated first to requests for support at the 90 percent discount rate.[283] To the extent funds remain after discounts are awarded to entities eligible for a 90 percent discount, the rules Pilot rules provide that the Administrator shall continue to allocate funds for discounts to participants at each descending single discount percentage.[284] The Pilot rules also provide that if sufficient funds do not exist to grant all requests within a single discount percentage, the Administrator shall allocate the remaining support on a pro rata basis over that single discount percentage level.[285] Funding for libraries will be prioritized based on the percentage of free and reduced lunch eligible students in the school district that is used to calculate the library's discount rate.[286] Funding for individual schools that are not affiliated financially or operationally with a school district, such as private or charter schools that apply individually, will be prioritized based on each school's individual free and reduced student lunch eligible population.[287] For those schools and libraries selected as Pilot participants that do not participate in the E-Rate program, their discount rate will be calculated based on indicators of need as outlined above and their funding prioritized consistent with the prioritization rules for the Pilot described in this paragraph.[288] This prioritization gives applicants serving the highest poverty populations first access to funds while allowing us to fund within a discount band even where funding is not sufficient to reach all participants in the band. This system of prioritization is also consistent with Fortinet's recommendation that "the Commission . . . consider a tiered prioritization scheme for Pilot support requests"[289] and the recommendations of commenters that those schools, libraries, and consortia with a higher discount rate receive funding ahead of those who are entitled to a lower discount rate.[290]

75. *Part Two Application Information.* For the second part of the FCC Form 484 application, we direct the Bureau and USAC to collect more detailed cybersecurity information from applicants who are selected to participate in the Pilot Program. As previously noted, we have bifurcated the application into two parts, seeking a general level of cybersecurity information from applicants and leaving the more detailed cybersecurity reporting for the selected Pilot participants. This has the benefit of limiting the amount of sensitive cybersecurity information that will be provided by applicants at the application stage and will reduce the initial application burden. We require Pilot participants to provide such information to help establish a baseline that will enable us to effectuate the Performance Goals and Data Reporting discussed in section III.I. Applicants should be aware, that, if selected to participate in the Pilot Program, they will be required to provide the following additional (or substantially similar) cybersecurity information, as applicable, and may be removed from the Pilot Program if they refuse or fail to do so:

- Information about correcting known security flaws and conducting routine backups,[291] developing and exercising a cyber incident response plan,[292] and any cybersecurity changes or advancements the participant plans to make outside of the Pilot-funded services and

[282] *See* 47 CFR § 54.2007(b)(1)-(2), (c); *see also* 47 CFR § 54.505(b)(1)-(2), (c).

[283] *See* 47 CFR § 54.2001(d).

[284] *Id.*

[285] *Id.*

[286] *See* 47 CFR § 54.2007(b)(2); *see also* 47 CFR § 54.505(b)(2).

[287] *See* 47 CFR § 54.2007(b)(1); 47 CFR § 54.505(b)(1).

[288] 47 CFR § 54.2001(d).

[289] Fortinet Reply at 5.

[290] *See supra* para. 68.

[291] *Cybersecurity NPRM,* 2023 WL 8605080 at *15, para. 37.

[292] *Id*. at *9, para. 22.

equipment.[293]

- A description of the Pilot participant's current cybersecurity posture, including how the school or library is currently managing and addressing its current cybersecurity risks through prevention and mitigation tactics.[294]
- Information about a participant's planned use(s) for other federal, state, or local cybersecurity funding (i.e., funding obtained outside of the Pilot).[295]
- Information about a participant's history of cyber threats and attacks within a year of the date of its application; the date range of the incident; a description of the unauthorized access; a description of the impact to the K-12 school or library; a description of the vulnerabilities exploited and the techniques used to access the system; and identifying information for each actor responsible for the incident, if known.[296]
- A description of the specific Education Department or CISA cybersecurity recommendations that the participant has implemented or begun to implement.[297]
- Information about a participant's current cybersecurity training policies and procedures, such as the frequency with which a participant trains its school and library staff and, separately, information about student cyber training sessions, and participation rates.[298]
- Information about any non-monetary or other challenges a participant may be facing in developing a more robust cybersecurity posture.[299]

76. *Instructions for Filing Applications*. As previously discussed, in order to facilitate the application process, we plan to provide an application titled "Schools and Libraries Cybersecurity Pilot Program Application" (FCC Form 484) that applicants must use when submitting their project proposals to the Commission. Applicants will be required to complete each section of the first part of the application and make the required certifications. The applications for the Pilot Program must be submitted through the Pilot portal on USAC's website during the announced FCC Form 484 application filing window discussed below. We direct the Bureau to issue a Public Notice subsequent to the release of this Report and Order that specifies the effective date of the Pilot Program rules and the filing window dates for submitting Pilot applications. The Public Notice must also include details on how to submit an application using the Pilot portal on USAC's website. In response to concerns about the security and confidentiality of cybersecurity information provided as part of the Pilot, as stated previously we are only requiring more general information at the application stage of the Pilot. The more detailed, cybersecurity-related information will only be provided by the Pilot participants.[300] As noted above, some commenters have expressed concerns that this type of information is sensitive and could be used by malicious cybersecurity actors for nefarious purposes. We agree and find that the cybersecurity-related information that is being requested and provided in the FCC Form 484 constitutes sensitive business information and includes trade secrets. Accordingly, we will treat it as presumptively confidential under our rules and will

[293] *Id*. at *10, para. 24.

[294] *Id*. at *11, para. 27.

[295] *Id*. at *15, para. 38.

[296] *Id*. at *9, *11, *14, paras. 21, 27, 36.

[297] *Id*. at *13, *15, paras. 34, 37-38.

[298] *Id*. at *9, para. 21.

[299] *Id*. at *14-15, paras. 36, 38.

[300] A participant's failure to submit the more detailed, cybersecurity-related information required by the second part of the FCC Form 484 application will lead to removal from the Pilot.

withhold it from public inspection.[301] We further note that FCC Form 484 data will be protected by security protections built into USAC's Pilot portal.[302]

77. *Instructions for Establishing Application Schedule and Reviewing Applications*. We delegate to the Bureau the authority to establish an application schedule consistent with the direction provided in this Report and Order; review Pilot FCC Form 484 applications; and select Pilot projects and participants, doing so in an efficient and expedited manner. We further direct the Bureau to consult with OEA, PSHSB, OMD, and the Office of General Counsel (OGC), as needed, regarding the review of Pilot applications and selection of participants.[303] After selecting the Pilot participants, we direct the Bureau to announce its selections through a Public Notice that will provide further detail about the Pilot Program requirements, including providing additional information and instruction regarding Pilot requirements for competitive bidding, submitting requests for funding, and invoicing, as well as the Pilot-specific data and metrics reporting requirements discussed herein and the format for those reporting and metrics requirements.[304]

78. *Establishing an Application Filing Window*. To facilitate an efficient and equitable application review process, we direct the Bureau to establish an application filing window, after which it will review applications from all eligible applicants by weighing the considerations discussed above.[305] Establishing a single filing window was well received by those commenters who addressed the proposal[306] and opening a single window will allow the Bureau to review all applications before making selections. We expect that adopting a single FCC Form 484 application filing window and proceeding in this manner will assist with our goal of selecting a diverse cross-section of Pilot participants with a particular focus on the under-resourced applicants who are most in need of cybersecurity funding.

F. Competitive Bidding, Requests for Services, and Invoicing and Reimbursement Processes

79. We next adopt competitive bidding processes and rules for the Pilot Program that mirror the E-Rate program to ensure that the limited Pilot funds are used for the most cost-effective eligible services and equipment; the integrity of the Pilot Program is protected; and potential waste, fraud, and abuse is prevented. We direct the Bureau and USAC to model the Pilot Program requests for services, invoicing, and reimbursement processes and forms on existing E-Rate and ECF program processes and forms to the extent possible for the Pilot Program, consistent with record support.[307] In particular, we expect the Bureau and USAC to leverage the following FCC forms for the Pilot that will mirror existing

[301] *See* 47 CFR § 0.457(d).

[302] *See supra* para. 62, note 223.

[303] *See, e.g.*, Dallas ISD Comments at 4 (recommending that the Commission "design the application and select evaluators with a strong competency in cybersecurity").

[304] Generally speaking, the rules for this Pilot program will become effective 30 days from publication in the Federal Register. However, certain rules contain information collection requirements that will not be effective until approved by the Office of Management and Budget (OMB). We direct the Bureau to announce the effective date of those rules upon approval by OMB. We also direct the Bureau to provide an explanation of the selection process when announcing participant selections, to explain why certain applicants were selected, and others were not.

[305] *See supra* para. 64.

[306] *See, e.g.*, CoSN et al. August 7 *Ex Parte* Letter at 1; Fortinet Reply at 3.

[307] *See e.g.*, IOB Comments at 5-6 (advocating for a certification approach in the application process that is similar to how E-Rate certifications are currently handled); Lumen Reply at 6 (agreeing that "the Cybersecurity Pilot should generally mirror the existing E-Rate Program rules, forms, and processes"); NCTA Comments at 5 (agreeing with the Commission's proposal that the Pilot program should, for the most part, mirror the existing E-Rate rules); *see also* CoSN et al. August 7 *Ex Parte* Letter at 2 ("The application process must . . . align whenever possible with tools and concepts that are familiar to E-rate applicants.").

E-Rate and ECF forms: (1) FCC Form 470 (Description of Services Requested and Certification Form); (2) FCC Form 471 (Description of Services Ordered and Certification Form); (3) FCC Form 472 (Billed Entity Applicant Reimbursement (BEAR) Form); and (4) FCC Form 474 (Service Provider Invoice (SPI) Form).[308] We require Pilot participants and service providers to make certain certifications on Pilot Program forms to protect the integrity of the Pilot.[309] We also require them to submit invoices with their reimbursement requests that support the amounts requested and approved in their Pilot FCC Form 471 applications. By modeling the Pilot processes and forms on existing E-Rate and ECF processes and forms, we expect to save Pilot participants time needed to familiarize themselves with the new forms and reduce administrative cost and burden.

1. Competitive Bidding Requirements

80. As in the E-Rate program, we adopt competitive bidding processes and rules for the Pilot Program to ensure that the limited Pilot funds are used for the most cost-effective eligible services and equipment, to protect the integrity of the Pilot. Competitive bidding is a cornerstone of several USF programs, including the E-Rate and Connected Care Pilot programs, and is critical to ensuring that applicants obtain the most cost-effective offering available.[310] Currently, under the E-Rate program rules, to obtain support an applicant must first conduct a competitive bidding process and comply with the Commission's competitive bidding rules.[311] Applicants begin the competitive bidding process by filing a completed E-Rate FCC Form 470 with USAC.[312] USAC, in turn, posts the form on its website for potential competing service providers to review and submit bids on.[313] An applicant must wait at least 28 days from the date on which its E-Rate FCC Form 470 is posted on USAC's website before entering into a signed contract or other legally binding agreement with a service provider and submitting an E-Rate FCC Form 471 to seek funding for selected services and equipment.[314] The E-Rate FCC Form 470 must specify and provide a description of the eligible services and equipment requested with sufficient detail to enable potential service providers to submit responsive bids.[315]

81. In the *Cybersecurity NPRM*, we proposed a competitive bidding process and rules for

[308] Although the Pilot program will leverage the FCC forms from the E-Rate and ECF programs, the Pilot forms will have their own distinct prefixes or identifiers to distinguish them from the E-Rate and ECF forms.

[309] *See, e.g.*, 47 CFR §§ 54.2005(c)(2)(i)-(xiii), 54.2006(a0(2)(i)-(xvi), 54.2008(a)(1)(i)-(xiii), 54.2008(a)(2)(i)-(xiii).

[310] *See Universal Service First Report and Order*, 12 FCC Rcd at 9029, para. 480; *see also Request for Review of the Decision of the Universal Service Administrator by Ysleta Independent School District*, CC Docket No. 02-6, Order, 18 FCC Rcd 26407, 26417, para. 22 (2003) (explaining that competitive bidding for services eligible for discount is a cornerstone of the E-rate program); *Connected Care Pilot Order*, 35 FCC Rcd at 3411, para. 75 (adopting competitive bidding requirements for the Connected Care Pilot Program); *see also Promoting Telehealth in Rural America*, WC Docket No. 17-310, Report and Order, 34 FCC Rcd 7335, 7410, para. 161 (2019) (*2019 RHC Report and Order*) (codifying the requirement for "fair and open" competitive bidding processes in the Rural Health Care Program).

[311] 47 CFR § 54.503.

[312] *Id*.

[313] *Id*. § 54.503(c).

[314] *Id*. §§ 54.503(c)(4), 54.504(a). The rule states that USAC must send confirmation of the posting to the entity requesting service, which includes the date after which the requestor may sign a contract with its chosen provider(s), and that the entity must wait at least four weeks from the date on which its description of services is posted before making commitments with the selected providers of services. *Id.*§ 54.503(c)(4). USAC's website calls this the "28-Day Waiting Period" and reminds applicants that state or local procurement regulations may require a longer waiting period or impose additional requirements. *See* USAC, *28-Day Waiting Period*, https://www.usac.org/e-rate/applicant-process/competitive-bidding/28-day-waiting-period/ (last visited Mar. 25, 2024).

[315] 47 CFR § 54.503(c)(1)(i)-(ii).

Pilot participants that mirror the existing E-Rate competitive bidding process and rules.[316] Because of the structural similarities between the E-Rate program and the Pilot, the proven effectiveness of the E-Rate processes and rules, and the reduced compliance burden for Pilot participants who are already familiar with existing E-Rate requirements, we conclude that our proposal is reasonable and we adopt it here. To begin, we adopt a Pilot FCC Form 470, modeled after the E-Rate form, that Pilot participants will use to describe their desired Pilot-eligible services and equipment and initiate the competitive bidding process. Likewise, we adopt competitive bidding requirements modeled on section 54.503 of the Commission's rules, with which Pilot participants must comply to ensure they conduct an open and fair competitive bidding process.[317] This includes, among other things, the requirement that a Pilot participant must wait at least 28 days from the date the Pilot FCC Form 470 is posted on USAC's website before entering into a legally binding agreement or contract with a service provider and must submit a Pilot FCC Form 471 to seek funding for Pilot-eligible services and equipment.[318] It also includes the requirement that before entering into an agreement or contract with a service provider(s), a Pilot participant carefully consider all bids submitted and select the most cost-effective service offering with price as the primary (i.e., most heavily-weighted) factor in the vendor selection process.[319] Finally, it includes a restriction on the receipt of gifts[320] and a requirement that the competitive bidding process be conducted in a fair and open manner (i.e., all potential service providers have access to the same information and are treated in the same manner throughout the entire process).[321]

82. Because the competitive bidding process is essential to ensuring that Pilot participants obtain the most cost-effective eligible services and equipment, protecting program integrity, and preventing potential waste, fraud, and abuse in the Pilot, we decline CCSD's recommendation that applicants with existing contracts for cybersecurity solutions be allowed to request Pilot Program funding to cover the cost of those contracts and be exempt from any competitive bidding requirements.[322] Similarly, because an open and fair competitive bidding process hinges on all bidders being on equal footing, we also decline E-Rate Central's proposal that applicants be allowed to conduct their competitive bidding processes before submitting their FCC Form 484 applications and be permitted to work alongside their selected service providers to develop their proposed Pilot projects.[323]

2. Requests for Services and Equipment Process

83. As proposed in the *Cybersecurity NPRM*, we adopt the Pilot FCC Form 471, modeled after the E-Rate FCC Form 471, for Pilot participants and their service provider(s).[324] In the E-Rate program, applicants file an FCC Form 471 to request discounts on eligible services and equipment for the upcoming funding year.[325] The E-Rate FCC Form 471 requires detailed descriptions of the services and

[316] *Cybersecurity NPRM,* 2023 WL 8605080 at *19, para. 47 and n.123.

[317] *See* 47 CFR § 54.2005.

[318] *Compare* 47 CFR § 54.2005(c)(4) *with* 47 CFR § 54.503(c)(4).

[319] *Compare* 47 CFR § 54.2005(c)(2)(viii) *with* 47 CFR § 54.503(c)(2)(ii)(B). As explained by E-Rate program rule 54.511, "[i]n determining which service offering is the most cost-effective, entities may consider relevant factors other than the pre-discount prices submitted by providers, but price should be the primary factor considered." 47 CFR § 54.511(a).

[320] *Compare* 47 CFR § 54.2005(d) *with* 47 CFR § 54.503(d).

[321] *Compare* 47 CFR § 54.2005(a) *with* 47 CFR § 54.503(a).

[322] CCSD Comments at 1.

[323] E-Rate Central Comments at 2-3.

[324] *Cybersecurity NPRM,* 2023 WL 8605080 at *20, para. 49.

[325] *See generally* 47 CFR § 54.504. Applicants also file an FCC Form 471 for the ECF program. *See generally* 47 CFR § 54.1710.

equipment requested, including the costs of and service dates for the services and equipment; the selected service provider(s); and certifications regarding compliance with program rules.[326] Applicants must wait until the Allowable Contract Date (ACD), which is 28 days after the E-Rate FCC Form 470 is certified and submitted to USAC, to certify and submit its E-Rate FCC Form 471.[327] Once an applicant certifies and submits its E-Rate FCC Form 471, USAC issues a Receipt Acknowledgment Letter (RAL) to both the applicant and its selected service provider(s).[328] Following the issuance of the RAL, and after USAC conducts its program integrity assurance (PIA) review process, USAC issues a Funding Commitment Decision Letter (FCDL) to both the applicant and the selected service provider(s), at which point they may begin to invoice after the receipt or delivery of the requested eligible services and/or equipment.[329]

84. Similar to the E-Rate program, Pilot participants must file a Pilot FCC Form 471 to request discounts on eligible services and equipment.[330] As with the E-Rate form, the Pilot FCC Form 471 will include information on the recipients of services and equipment and the selected service provider(s); detailed descriptions of the services and equipment requested, including the costs of and service dates; and certifications regarding compliance with Pilot rules.[331] Pilot participants will be required to wait until the ACD to certify and submit the Pilot FCC Form 471.[332] Once a Pilot participant certifies and submits the Pilot FCC Form 471, USAC will provide the Pilot participant an opportunity to correct any errors on the form, through a RAL or similar process, after which USAC will issue an FCDL. Pilot participants will submit Pilot FCC Form(s) 471 to cover the full Pilot project, and will be allowed to submit service and equipment substitution change requests, if needed, during the three-year Pilot.

85. We direct the Bureau and USAC to announce and open a Pilot FCC Form 471 application filing window to speed the availability of funds to the selected Pilot participants.[333] During this application filing window, selected Pilot participants may submit their Pilot FCC Form 471 to request eligible equipment and services that are needed to implement their Pilot project through the online system implemented by USAC.[334] As we are adopting forms, processes, and procedures that are used in the E-Rate and ECF programs, we expect that this application filing window process will be familiar to most of the selected Pilot participants. Pilot participants will have a three-year period from the date of their FCDL to receive and implement the services and equipment funded through the Pilot.[335] Pilot participants will be required to report on the progress of their Pilot projects and how the Pilot funding is

[326] 47 CFR § 54.504; *see also* E-Rate FCC Form 471, Description of Services Ordered and Certification Form.

[327] 47 CFR § 54.503(c)(4); .*See also* USAC Website, *FCC Form 471 Filing*, https://www.usac.org/e-rate/applicant-process/applying-for-discounts/fcc-form-471-filing/ (last visited Mar. 26, 2024) (explaining that an applicant may not certify the FCC Form 471 before the ACD, which is 28 days after its FCC Form 470 is submitted and certified).

[328] *See* USAC Website, *FCC Form 471 Filing*, https://www.usac.org/e-rate/applicant-process/applying-for-discounts/fcc-form-471-filing/ (last visited Mar. 26, 2024) (explaining that after the FCC Form 471 has been certified, USAC issues a RAL to both the applicant and the selected service provider(s)).

[329] *See* USAC Website, *FCC Form 471 Filing*, https://www.usac.org/e-rate/applicant-process/applying-for-discounts/fcc-form-471-filing/ (last visited Mar. 26, 2024) (explaining that after USAC has reviewed the funding request(s) included in the FCC Form 471 and issued the RAL, it issues an FCDL to both the applicant and the selected service provider(s)).

[330] *See generally* 47 CFR § 54.2006.

[331] *Id.*

[332] *Id*., §§ 54.2005(c)(4); 54.2006(a)(2)(viii).

[333] USAC announces a specific filing window each year for E-rate Forms 471. *See* USAC Website, *FCC Form 471 Filing*, https://www.usac.org/e-rate/applicant-process/applying-for-discounts/fcc-form-471-filing/ (last visited Apr. 16, 2024).

[334] *Id*., § 54.2006(d).

[335] *Id*., § 54.2001(c).

being used to improve their cybersecurity postures throughout the three year term, consistent with the annual reporting requirements discussed later in this Order.[336] We further expect that using a Pilot FCC Form 471 application filing window will allow USAC to quickly size demand, review applications, and issue funding decisions, thereby allowing the flow of funding more quickly to Pilot participants. In the event that demand does not exceed available funds, we delegate authority to the Bureau to direct USAC to open additional Pilot FCC Form 471 application filing windows and to commit additional funding up to each Pilot participant's allotted budget. No Pilot participant will be allowed to request or receive more funding than what is calculated based on the per-Pilot participant budget rule.[337]

3. Invoicing and Reimbursement Process

86. *Invoicing.* Consistent with the E-Rate program, and pursuant to the *Second Report and Order*,[338] we permit both Pilot participants and service providers to submit requests for reimbursement using the Pilot FCC Forms 472 and 474, respectively.[339] We agree with those commenters who explain that allowing both participant and service provider invoicing options is the most efficient and direct way to provide funding to eligible schools and libraries.[340] We conclude that, on balance, allowing both invoicing options for the submission of Pilot reimbursement requests is an efficient and effective way to ensure that participants are actually able to purchase Pilot-eligible services and equipment, and aligns most closely with the E-Rate program, which commenters support.[341] Consistent with E-Rate program rules, Pilot participants must be permitted to select the method of invoicing.[342] For administrative simplicity, Pilot participants must also specify on their Pilot FCC Form 471 whether the participant or the service provider will be conducting the invoicing for each funding request.[343] As part of the reimbursement process, Pilot participants and service providers must provide the required certifications, along with any necessary documentation to support their requests.[344] Requests for reimbursement must be submitted to USAC within ninety (90) days after the last date to receive service, and Pilot participants or service providers may request a one-time extension of the invoicing filing deadline, if the request is timely filed.[345]

---

[336] *See* 47 CFR § 54.2004(e); *see also infra* paras. 107-111 (discussing the Pilot data reporting requirements).

[337] *Id*., § 54.2001(b).

[338] *Schools and Libraries Universal Service Support Mechanism*, CC Docket No. 02-6, Second Report and Order and Further Notice of Proposed Rulemaking, 18 FCC Rcd 9202, 9217-18, paras. 44-47 (2003) (*Second Report and Order*) (finding that providing applicants with the right to choose the payment method is consistent with section 254 of the Act and could prevent cash flow problems associated with requiring schools and libraries to pay in full).

[339] *See* 47 CFR § 54.514(c) (specifying that the applicant must be permitted to choose the invoicing method); *see also id.*, § 54.1711 (discussing the BEAR and SPI invoicing requirements in the ECF program).

[340] *See e.g.*, ActZero Comments at 7-8 (stating that the invoicing method should be determined between Pilot participants and their service providers); Lumen Reply at 6-7 (advocating the flexibility for schools and libraries to select the BEAR process instead of requiring service providers to submit invoices).

[341] *See e.g.*, Lumen Reply at 6 (agreeing that the Pilot should generally mirror existing E-Rate Program rules, forms, and processes); NCTA Comments at 5 (agreeing that the Pilot program should, for the most part, mirror the existing E-Rate rules).

[342] *See. e.g.*, 47 CFR § 54.514(c); *see also Second Report and Order*, 18 FCC Rcd at 9217-18.

[343] Unlike in the ECF program, the Pilot participant will not need to first obtain the consent of the service provider to use the service provider invoicing (SPI) method. *See Establishing Emergency Connectivity Fund to Close the Homework Gap*, WC Docket No. 21-93, Report and Order, 36 FCC Rcd 8696, 8742, para. 95 (2021) (*Emergency Connectivity Fund Report and Order*).

[344] 47 CFR § 54.2008.

[345] *Id.*, § 54.2008(d), (e). We chose a ninety (90) day deadline for requests for reimbursement, as opposed to the 120 day deadline in the E-Rate program, because of the limited nature of the Pilot program and because Pilot participants (continued….)

87. *Invoicing Documentation.* As in the ECF program, to protect the integrity of the Pilot and protect against potential waste, fraud, and abuse, we require Pilot participants and service providers to submit, along with their reimbursement requests, invoices detailing the items purchased.[346] Invoices must support the amounts requested and approved in the Pilot FCC Form 471 application. We disagree with Lumen and NCTA that the submission of invoices with reimbursement requests would limit flexibility for Pilot participants and serves no purposes in this context.[347] Rather, the submission of invoices with the Pilot FCC Forms 472/474 will help expedite the review of those requests and the corresponding disbursement of funds. Moreover, although the Pilot Program is not an emergency program, it is being conducted on an expedited basis, thus necessitating swift and efficient final invoicing decisions. While we will not require Pilot participants and service providers to submit other supporting documentation at the time they submit their Pilot request(s) for reimbursement, pursuant to our certifications and document retention requirements, all participants must certify receipt/delivery of eligible services and equipment and that only eligible services and equipment were invoiced,[348] as well as retain and provide upon request by USAC, the Commission (including Commission staff) and its Office of the Inspector General (OIG), or any other authorized federal, state, or local agency with jurisdiction over the entity, all records related to their Pilot FCC Forms 470, 471, and 472/474 (including, for example, competitive bidding documentation and contracts) for at least ten years from the last date of service or delivery of equipment.[349]

G. USAC's Role as the Administrator of the Pilot Program

88. Consistent with the terms of the Memorandum of Understanding (MOU) between the Commission and USAC,[350] and pursuant to the rules adopted today,[351] we designate USAC as the Administrator of the Pilot Program. We will use USAC's services to review, process, and approve the Pilot FCC Forms 470, 471, 472, 474, and 484, as well as recommend funding commitments, issue funding commitment decision letters, review requests for reimbursement and invoices, and payment of funds, as well as other administration-related duties.[352] The one commenter that directly addressed the issue supported using USAC and its processes for the efficient and effective administration of the Pilot Program,[353] and we agree that USAC's experience administering the E-Rate and Connected Care Pilot programs, along with the other federal universal service programs makes it uniquely situated to be the administrator of the Pilot Program. In designating USAC as the Administrator of the Pilot Program we note that USAC may not make policy, interpret unclear statutes or rules relied upon to implement and

(Continued from previous page)
may submit their requests at any point during the Pilot. A ninety (90) day deadline will result in quicker reimbursement and more administrative certainty for participants who submit their reimbursement requests near or at the end of the three-year Pilot period, especially given the automatic one-time extension of the invoicing filing deadline provided to all Pilot participants, provided such extensions are timely filed. *Compare id. with* 47 CFR 54.514(a).

[346] *Id*. § 54.2008(b). *See id.* § 54.1711(b) (requiring detailed invoices in the ECF program).

[347] Lumen Reply at 7; NCTA Comments at 5-6.

[348] 47 CFR § 54.2008.

[349] *Id*. § 54.2009. *See id.* § 54.516(a).

[350] *See generally* Memorandum of Understanding Between the Federal Communications Commission and the Universal Service Administrative Company (Dec. 19, 2018) (FCC/USAC MOU), https://www.fcc.gov/sites/default/files/usac-mou.pdf.

[351] *See generally* 47 CFR § 54.2011.

[352] *Id.*

[353] *See* ALA Comments at 4 ("[W]e . . . also agree that this process and other aspects of the Pilot Program should be administered by USAC.").

administer the Pilot Program, or interpret the intent of Congress.[354] In its administration of the Pilot Program, we also direct USAC to comply with, on an ongoing basis, all applicable laws and federal government guidance on privacy and information security standards and requirements such as the Privacy Act,[355] relevant provisions of the Federal Information Security Modernization Act of 2014,[356] NIST publications, and Office of Management and Budget guidance.

89. We notify Pilot participants, including their selected service providers that, similar to the E-Rate program and other USF programs, they shall be subject to audits and other investigations to evaluate their compliance with the statutory and regulatory requirements for the Pilot. USF Program audits have been successful in helping program applicants and participants improve compliance with the Commission's rules and in protecting the funds from waste, fraud, and abuse. We direct USAC to perform such audits pursuant to the Commission's and USAC's respective roles and responsibilities as set forth in the MOU and section 54.2011 of the Commission's rules.[357] We are also mindful of the privacy concerns raised regarding providing personally identifiable information (PII) to Commission or USAC staff about individual students, school staff, or library patrons that may be collected as part of the cybersecurity measures implemented through the Pilot.[358] While we do not anticipate that Pilot participants will need to share the PII of students, school staff, or library patrons in connection with their Pilot FCC forms, audits (or related compliance tools), or reporting, we note that the Commission, USAC, and any contractors or vendors will abide by all applicable federal and state privacy laws. We also direct the Commission, USAC, and contractor/vendor staff to take into account the importance of protecting the privacy of students, school staff, and library patrons, to design requests for information from schools and libraries that minimize the need to produce information that might reveal PII, and to work with auditors to accept anonymized or deidentified information in response to requests for information wherever possible. If anonymized or deidentified information regarding the students, school staff, and library patrons is not sufficient for auditors' or investigative purposes, the auditors or investigators may request that the school or library obtain the consent of the parents or guardians, for students, and the consent of the school staff member or library patron to have access to PII or explore other legal options for obtaining PII. We additionally delegate to the Bureau and OMD, in consultation with OGC (and specifically the Senior Agency Official for Privacy) the authority to establish requirements for the Bureau's, USAC's, or any contractor's/vendor's collection, use, processing, maintenance, storage, protection, disclosure, and disposal of PII in connection with any Pilot FCC forms, audit (or other compliance tool), or reporting.

H. Pilot Program Integrity Protections

90. We take seriously our obligation to be a careful steward of the USF and to protect the integrity of the Pilot Program. We are committed to ensuring the integrity of the Pilot and will pursue instances of waste, fraud, or abuse under our own procedures and in cooperation with law enforcement agencies. The specific procedures we adopt regarding document retention requirements, the prohibition on gifts, certifications, audits, suspension and debarment, and the treatment of eligible services and equipment are modeled after our E-Rate processes and are tools at our disposal to protect the Pilot and

[354] 47 CFR § 54.2011(c).

[355] 5 U.S.C. § 552a.

[356] The Federal Information Security Management Act of 2002 (FISMA), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002), was subsequently modified by the Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283, Dec. 18, 2014). As modified, FISMA is codified at 44 U.S.C. §§ 3551 *et seq.*

[357] *See generally* FCC/USAC MOU; *see also* 47 CFR § 54.2011(h).

[358] *See, e.g.,* CoSN et al. January 29 Comments at 15-16 (urging the Commission to adopt an open data model for the Pilot that enables a variety of parties to independently analyze and use aggregated or anonymized data to support informed decision-making but recommending a layered data management strategy that could include, among other things, removing all PII from applicant's or participant's data).

ensure the limited program funding is used for its intended purposes to support Pilot Program goals and enable the purchase of Pilot-eligible services and equipment.

1. Document Retention and Production Requirements

91. In the *Cybersecurity NPRM*, we sought comment on whether "document retention requirements" for the Pilot, including those based on modifying rules from the Commission's E-Rate program, would help "protect the program integrity of the Pilot."[359] We adopt this proposal. Specifically we include a new section 54.2010(a) of the Commission's rules, modeled after a corresponding E-Rate rule, that requires Pilot participants to "retain all documents related to their participation in the [Pilot] program sufficient to demonstrate compliance with all program rules for at least 10 years from the last date of service or delivery of equipment" and "maintain asset and inventory records of services and equipment purchased sufficient to verify the actual location of such services and equipment for a period of 10 years after purchase."[360] We also include a new section 54.2010(b) of the Commission's rules, also modeled after a corresponding E-Rate rule, that requires Pilot participants and service providers to "produce such records upon request of any representative (including any auditor) appointed by a state education department, the Administrator, the Commission, its Office of the Inspector General, or any local, state, or federal agency with jurisdiction over the entity."[361]

92. While commenters generally did not opine on these issues, we find that this new rule, section 54.2010(a), will ensure that participants have sufficient records on hand related to all aspects of their participation in the Pilot to permit entities with jurisdiction over the participant, including USAC and the Commission, to make efficient and reliable determinations of compliance, e.g., as part of any post-audit review or investigation that bears on potential waste, fraud and abuse in the Pilot Program. We find that this new rule, section 54.2010(b), will effectively establish (or confirm) that a Pilot participant must provide documents to external parties with valid jurisdiction when a request is made for the retained documents. We find today's actions are warranted as the Commission, as a careful steward of the USF's limited funds, has a strong interest in ensuring that sufficient documentation is available and can be accessed to permit external parties with jurisdiction to make reliable and efficient determinations of potential waste, fraud and abuse in the Pilot. We also find that today's new rules will meaningfully inform potential Commission short-term action, e.g., through enforcement or other remediation steps if the integrity of the Pilot Program is threatened, and long-term action, that could potentially result in future revision of Commission or USAC processes to better protect the USF and the USF programs. Moreover, we find these rules, including the associated "10 year" retention and production requirements, are likely to be effective in protecting the integrity of the Pilot because they are modeled after existing section 54.516 of the Commission's rules with only clarifying amendments reflective of the structure of the Pilot. We have found the E-Rate rules to be effective over the course of our many years of experience overseeing USAC's administration of the E-Rate program. As the Commission has previously noted, these rules, including the 10 year retention and production requirement, appropriately balance the need to have pertinent document available for potential litigation with corresponding administrative burdens and storage costs borne by E-Rate applicants and service providers.[362] We expect similar benefits to accrue in relation to the Pilot.

[359] *Cybersecurity NPRM,* 2023 WL 8605080 at *21, para. 51.

[360] 47 CFR § 54.2010(a); *see also* 47 CFR § 54.516(a).

[361] 47 CFR § 54.2010(b); *see also* 47 CFR § 54.516(b).

[362] *See First 2014 E-Rate Order*, 29 FCC Rcd at 8974-75 (extending the E-Rate document retention period from five to 10 years).

2. Gift Rule

93. In balancing the longstanding goal of fair and open procurement with the disbursement of USF support for eligible equipment and services, we adopt gift restrictions for the Pilot.[363] Consistent with the E-Rate program, we prohibit eligible schools and libraries receiving Pilot Program support, including their employees, officers, representatives, agents, independent contractors, consultants, and individuals who are on the governing boards, from soliciting or accepting any gift or other thing of value from a service provider participating in or seeking to participate in the Pilot.[364] Similar to the E-Rate program, participating service providers, including their employees, officers, representatives, agents, independent contractors, consultants, and individuals who are on governing boards, are likewise prohibited from offering or providing any gift or other thing of value to eligible entities, including their employees, officers, representatives, agents, independent contractors, consultants, and individuals who are on the governing boards.[365]

3. Certifications

94. As an additional measure to protect the integrity of the Pilot, we also require participants to provide several certifications as part of the FCC Form 484 application, competitive bidding, requests for services, and invoicing processes.[366] Similarly, we require their selected service providers to provide certifications related to Pilot invoicing processes. We find, and no commenter disagrees, that the use of certifications are a key compliance mechanism to protect the limited funds. All certifications must be made subject to the provisions against false statements contained in the Act[367] and Title 18 of the United States Code.[368]

95. *Duplicate Funding Certification*. For the reasons discussed in section D.2, we confirm that we will not provide support for eligible services and equipment, or the portion of eligible services and equipment, that have already been reimbursed with other federal, state, Tribal, or local funding, or are eligible for discounts from E-Rate or another universal service program.[369] No commenters opposed adopting this limitation to stretch the Pilot's limited funds. To implement this prohibition on requesting or receiving duplicative funding, we will require Pilot participants and service providers to certify on the FCC Forms 472 or 474 that they are not seeking support or reimbursement for Pilot-eligible services and equipment that have been purchased and reimbursed with other federal, state, Tribal, or local funding, or are eligible for discounts from E-Rate or another universal service program.[370] We take this action to ensure that the limited Pilot support will be used for its intended purposes and clarify that if the Pilot-eligible services and equipment were fully reimbursed through other sources, participants and service providers should not be seeking funding through the Pilot Program.

96. *Additional Certification Requirements*. We also require Pilot participants, when submitting their FCC Form 470 competitive bidding forms and FCC Forms 472 and 474 requests for reimbursement (i.e., invoicing forms), to provide several additional certifications.[371] For example, Pilot

[363] 47 CFR § 54.2005(d); *accord* NCTA Comments at 5.

[364] *See* 47 CFR § 54.2005(d); *see also id.* § 54.503(d).

[365] *Id.*

[366] *See Cybersecurity NPRM,* 2023 WL 8605080 at *32-35, *37-39, *42-45.

[367] *See* 47 U.S.C. §§ 502, 503(b).

[368] *See* 18 U.S.C. § 1001.

[369] 47 CFR § 54.2006(a)(2)(x); *see also supra* para. 53.

[370] 47 CFR § 54.2006(a)(2)(x).

[371] *See id*., §§ 54.2005(c)(2) (requiring participants submitting FCC Forms 470 to certify, among other things, their eligibility to participate in the Pilot; the truthfulness, accuracy, and completeness of the information on their application; that any false statements may be punished by fine, forfeiture, or imprisonment and that failure to

(continued….)

participants and service providers must certify that they are seeking funding for only Pilot-eligible services and equipment. Pilot participants and service providers should be aware that the certification descriptions referenced in this section are not exhaustive and it is incumbent on them to familiarize themselves with the certifications required by each of the Pilot forms and rules that are applicable to them.[372]

4. Audits

97. Any support provided for cybersecurity services and equipment funded through the Pilot may be subject to audits and reviews currently used for the USF programs (e.g., Beneficiary and Contributor Audit Program (BCAP) audits, and Payment Integrity Assurance (PIA) reviews), and could be subject to recovery measures should the Commission and/or USAC find a violation of our rules and deem it appropriate. Specifically, applicants and service providers may be subject to audits and other investigations by USAC and/or Bureaus and Offices of the Commission to evaluate compliance with the rules we adopt today. We consider audits and other review mechanisms in the E-Rate program to be important tools in ensuring compliance with our rules and identifying instances of waste, fraud, and abuse.[373] Considering the action we take today to create the Pilot Program using universal service funding, we expect that these tools will continue to be paramount to our ability to ensure that these finite

(Continued from previous page)
comply with Pilot program rules may result in denial, cancellation, or recoupment of support; that the Pilot-funded services and equipment will be used for educational purposes and the participant will not sell, resell, or transfer the services and equipment except as permitted by Pilot rules; that they will consider all bids submitted with price as the primary factor and will select the most cost-effective service offering(s); that they have the resources necessary to effectively use Pilot-funded services and equipment; that they are in compliance with all applicable competitive bidding and procurement requirements; and that they may be audited and will retain all required documentation for a period of at least 10 years); 54.2006(a)(2) (requiring participants and/or service providers submitting FCC Forms 471 to certify, among other things, their eligibility to participate in the Pilot; the truthfulness, accuracy, and completeness of the information they provide; that any false statements may be punished by fine, forfeiture, or imprisonment and that failure to comply with Pilot program rules may result in denial, cancellation, or recoupment of support; that Pilot program support will be used consistent with Pilot program requirements; that the non-discount portion of the costs of Pilot-eligible services and equipment will be paid; that a fair and open competitive bidding process has been conducted that complies with all applicable competitive bidding and procurement requirements; that the Pilot FCC Form 470 was available for at least 28 days before bids were considered and service providers selected; that Pilot program support is only being sought for eligible services and equipment; that the Pilot-funded services and equipment will not be sold, resold, or transferred except as permitted by Pilot rules; that a service and equipment inventory will be maintained; that they may be audited and will retain all required documentation for a period of at least 10 years; and that they will notify the Administrator if any entity on the FCC Form 471 is criminally convicted or held civilly liable for acts that may subject them to suspension and/or debarment from the universal service support mechanisms).

[372] *See* 47 CFR §§ 54.2004 (Application for Pilot Program Selection and Reporting of Information); 54.2005 (Competitive Bidding Requirements); 54.2006 (Requests for Funding); 54.2008 (Requests for Reimbursement).

[373] *First 2014 E-Rate Order*, 29 FCC Rcd at 8974-76, paras. 261-64 (revising the E-Rate program document retention requirements to ten years after the latter of the last day of the applicable funding year or the service delivery deadline for the funding request and clarifying that applicants and service providers must permit auditors, investigators, USAC, the Commission, or any local, state, or federal agency with jurisdiction over the entity to enter their premises to conduct E-rate compliance audits and inspections); *Schools and Libraries Universal Service Support Mechanism*, CC Docket No. 02-6, Fifth Report and Order, 19 FCC Rcd. 15808, 15813, 15817-18, 15823-27, paras. 13, 29, 45-50 (2004) (explaining that audits are a tool for the Commission and USAC to ensure E-Rate program integrity and detect and deter waste, fraud, and abuse, and concluding that failure to comply with an authorized audit or other investigation is, in and of itself, a rule violation that may warrant the recovery of universal service support). *See also Cybersecurity NPRM,* 2023 WL 8605080 at *21, para. 51 (seeking comment on program integrity protections that mirror E-Rate program integrity protections, including audits and other methods of review); *accord supra* note 215 (referencing commenter support for aligning Pilot program rules and processes with E-Rate program rules and processes).

funds are used appropriately and consistent with our rules.

5. Suspension and Debarment

98. Consistent with our proposal in the *Cybersecurity NPRM*, we will apply our existing USF suspension and debarment rules to the Pilot.[374] In addition, to the extent that the Commission adopts updated and final suspension and debarment rules in a separate and pending proceeding, we will apply the updated rules to the Pilot Program."[375]

99. While commenters did not opine on these issues, we find it beneficial to apply our USF suspension and debarment rules, which are applicable to existing USF programs and codified at section 54.8 of our rules, to the Pilot as well.[376] Our decision to make these rules binding on persons, including individuals and entities, involved in the Pilot provides these groups with notice as to the types of behavior that could result in their suspension and debarment (and the suspension and debarment of others), the processes by which suspension and debarment would be determined, and some of the consequences of such action.[377] We also find that this action will permit Pilot participants to make better-informed decisions as to the consultants and other persons that they choose to employ or otherwise retain (e.g., based on factors that are identified in our suspension and debarment rules) for work on the Pilot Program, which will protect participants, and the USF, from waste, fraud and abuse. As the Pilot incorporates administrative processes, forms, and rules from E-Rate and other USF programs, we find it reasonable to apply our existing USF suspension and debarment rules to the Pilot as well. We find that doing so ensures that participants are able to engage a variety of persons with expertise and skills relevant to the USF generally, and Pilot specifically, while also preventing potential bad actors from undermining the Pilot's goals. Ultimately, we find that our action will support our mission to maintain the Pilot's integrity and protect it from waste, fraud, and abuse.

100. Similarly, we find it appropriate to apply any new Commission USF suspension and debarment rules that may be finalized during the course of the Pilot to the Pilot as well.[378] As discussed above, today's Pilot incorporates administrative processes, forms, and rules from E-Rate and other USF programs. We therefore find it reasonable to apply any new suspension and debarment rules developed for those programs to the Pilot as well.

I. Performance Goals and Data Reporting

101. We adopt three performance goals, discussed in greater detail below, to enable us to evaluate the Pilot Program. We expect that, to the extent that the Pilot Program meets these goals, the results of the Pilot will help us assess the costs and benefits of utilizing universal service funds to support schools' and libraries' cybersecurity needs, as well as how other federal resources could best be leveraged to ensure that these needs are addressed in the most efficient and effective manner.[379] We also adopt a periodic reporting requirement designed to allow the Commission evaluate the goals and success of the Pilot Program while, to the extent possible, taking steps to minimize the burden on Pilot participants.

---

[374] *Cybersecurity NPRM,* 2023 WL 8605080 at *21, para. 51 (citing 47 CFR § 54.8).

[375] *Id*. (citing *Modernizing Suspension and Debarment Rules*, GN Docket No. 19-309, Notice of Proposed Rulemaking, 34 FCC Rcd 11348 (2019)).

[376] *See* 47 CFR § 54.8 (setting forth the Commission's rules regarding suspension and debarment).

[377] 47 CFR § 54.8.

[378] *Cybersecurity NPRM,* 2023 WL 8605080 at para 51 (citing *Modernizing Suspension and Debarment Rules*, GN Docket No. 19-309, Notice of Proposed Rulemaking, 34 FCC Rcd 11348 (2019)).

[379] *See, e.g., Connected Care Pilot Order*, 35 FCC Rcd at 3415, para. 83 (finding that the Connected Care Pilot Program goals will "help advance the Commission's statutory obligation to promote universal service by providing the Commission with information that will help inform it about how best to allocate limited universal service funding").

102. In the *Cybersecurity NPRM*, we proposed three performance goals for the Pilot Program. Specifically, we proposed the goals of: (i) improving the security and protection of E-Rate-funded broadband networks and the data on those networks; (ii) measuring the costs associated with cybersecurity services and equipment, and the amount of funding needed to adequately meet the demand for these services if extended to the E-Rate program; and (iii) evaluating how to leverage other federal K-12 cybersecurity tools and resources to help schools and libraries effectively address their cybersecurity needs.[380] Additionally, we proposed and sought comment on how we can best measure progress towards these goals, to ensure that the limited Pilot funds are used most impactfully and effectively.[381] We also sought comment on how to evaluate the Pilot, including whether participants should submit periodic reports and other assessments and evaluations.[382]

103. Based on the record, we adopt our three proposed performance goals for the Pilot. We note that commenters broadly supported the three proposed goals, considering them appropriate to allow the Commission to assess the effectiveness and cost of the cybersecurity services and equipment used in the Pilot.[383]

104. *First Performance Goal: Improving the Security and Protection of E-Rate-Funded Broadband Networks and Data.* First, we adopt a goal for the Pilot Program of improving the security and protection of E-Rate-funded broadband networks and data. Funding made available by the Pilot will help participants acquire cybersecurity services and equipment to improve the security of their broadband networks and data. Commenters generally supported this goal.[384] Cisco, for example, deemed the goal consistent with the Commission's "statutory responsibilities to adapt the universal service rules to account for advances in telecommunications and information technology."[385] Making funding available for cybersecurity services and equipment will help Pilot participants protect and secure their E-Rate-funded broadband networks and data to mitigate increasing cybersecurity threats. In adopting this goal, we emphasize that we are not only seeking to improve the security and protection of E-Rate-funded Pilot participants, but also to gather information to aid the exploration of improving the security and protection of E-Rate-funded networks going forward. To that end, and as discussed herein, we are not limiting Pilot participation to existing E-Rate participants but will allow all eligible schools, libraries, and consortia to apply for the Pilot. By taking a holistic approach that incorporates all types of eligible schools and libraries, we seek to gather data that will help us evaluate how best to safeguard E-Rate-funded networks now and in the future.

---

[380] *Cybersecurity NPRM,* 2023 WL 8605080 at *8, para. 19.

[381] *Cybersecurity NPRM,* 2023 WL 8605080 at *10, para. 23.

[382] *Cybersecurity NPRM,* 2023 WL 8605080 at *10, para. 24.

[383] *See* Cisco Comments at 3; Dallas Independent School District Comments at 3 (Dallas ISD); CTIA Reply at 5. We recognize that the Commission is but one of many federal agencies that play a role in protecting school and library networks and data, which is why our proposed goals focus on evaluating how the Commission can contribute in this area and collaborate with our other federal partners. We therefore disagree with comments by K12 SIX that our proposed goals are "based on common misconceptions about the state of U.S. K-12 cybersecurity" or that the proposed Pilot is "out of step with the documented cybersecurity threats facing the K-12 sector." K12 SIX Comments at 6-9. We agree with K12 SIX's comments that the proposed Pilot alone will not fully address all the cybersecurity-related challenges faced by K-12 schools and libraries, including implementing appropriate governance practices and addressing new technologies, such as artificial intelligence. *Id*. However, we find that our proposed Pilot program and performance goals are tailored appropriately to determine whether and what cybersecurity services, including advanced firewall services, could effectively be funded through the E-Rate program, which is one of the primary purposes of this limited Pilot program.

[384] *See e.g.* Cisco Comments at 6; IOB Comments at 3; Palo Alto Networks, Inc. Comments at 1 (Palo Alto Networks).

[385] Cisco Comments at 6.

105. *Second Performance Goal: Measuring the costs associated with cybersecurity services and equipment, and the amount of funding needed to adequately meet the demand for these services if extended to all E-Rate participants*. Next, we adopt a goal of measuring the costs and effectiveness of cybersecurity services and equipment. By making a wide range of cybersecurity services and equipment eligible for USF support, the Pilot will enable the Commission to gather data on the associated cost and effectiveness of various cybersecurity solutions. As ALA, in particular, has observed, there are concerns about the cost to the USF of adding any new E-Rate eligible services and equipment, including cybersecurity services and equipment.[386] By measuring these costs as part of the Pilot, the Commission will be well-positioned to evaluate the potential challenges to funding these types of services and equipment over the long term. In addition, to measure effectiveness, CIS recommended that we require participants "to assess themselves before the Pilot and annually against a recognized cybersecurity framework and provide their scores as a measurement of success against their individual baseline."[387] With such recommendations in mind, we adopt a goal of measuring the costs and effectiveness of cybersecurity services and equipment, gathering data for the Commission to determine whether it is economically feasible to support advanced firewall and other cybersecurity services and equipment with universal service funding. In adopting this goal, we disagree with commenters who suggest that, in collecting data to evaluate the Pilot, our goal should be focused on determining "how to best modernize the E-rate Category 2 to include cybersecurity permanently"[388] or adopting concurrent changes to our category two rules to permit funding for advanced firewalls and MFA.[389] Although we hope to learn more about whether and how to best fund cybersecurity services and equipment at the conclusion of the Pilot, we do not prejudge the appropriate mechanism or services and equipment to fund and, instead, look holistically at how universal service funds could be used to meet the K-12 schools' and libraries' demand for cybersecurity services and equipment.[390]

106. *Third Performance Goal: Evaluating how to leverage other federal K-12 cybersecurity tools and resources to help schools and libraries effectively address their cybersecurity needs*. Third, we adopt a goal of evaluating how to best leverage other available and low cost and free federal resources to better equip schools and libraries with proactively addressing K-12 schools' and libraries' cybersecurity risks, though we do not go so far as to require the use of specific federal government tools and resources as initially suggested in the *Cybersecurity NPRM*.[391] Commenters generally agreed with this goal.[392] The

[386] ALA Comments at 3 ("We share concerns about the cost to the Universal Service Fund (USF) of adding any E-rate eligible services.").

[387] CIS Comments at 2. We note, in response to concerns raised by CrowdStrike, that the requirement that Pilot participants provide initial data, as well as file annual reports, will allow the Commission to measure performance improvements. *See* CrowdStrike Comments at 5 (stating that it is "unlikely that many K-12 schools and libraries were measuring this information before the beginning of the pilot program" and "the FCC may encounter difficulties measuring performance improvements within pilot participants").

[388] CoSN et al. August 7 *Ex Parte* Letter at 2; *see also* IOB Comments at 3.

[389] *See e.g.,* MISEN Comments at 7 ("MISEN believes the Pilot program's funding will fall short of making any real impact and that the Commission could make current-generation firewalls, related components, and licensing and Multi-Factor Authentication immediately eligible for E-Rate, thereby stretching the pilot funding. The FCC can make eligible advanced firewalls and MFA under current Category 2 budgets, and let applicants make their purchasing decisions. This will bring no additional burden to the Fund.").

[390] *See* discussion *supra* at para. 46 regarding our decision not to make additional services eligible before the conclusion of the Pilot.

[391] *See Cybersecurity NPRM,* 2023 WL 8605080 at *13, para. 34; *see also, e.g.*, EdGroup Reply at 4 (explaining that the Commission should not require the use of government tools and resources "because many schools and libraries have implemented their own cybersecurity strategies already"); Rubrik Comments at 2 (clarifying that not all of CISA's programs are offered for free and "it may be overly burdensome to require schools and libraries to implement these tools before applying" to the Pilot). Requiring the use of specific federal tools and resources could pose a barrier to participation for under-resourced districts. *See* Council GCS Comments at 4 ("In response to the (continued….)

Friday Institute for Education Innovation (Friday Institute), for example, stated that our federal partners "provide a wealth of best practices and knowledge," and "[r]elying on their expertise is a prudent approach to shaping the E-rate program's cybersecurity component."[393] CTIA emphasized the importance of collaborating with other agencies to pursue and implement shared cybersecurity objectives.[394] Commenters emphasize that collaboration with other federal partners is "vital,"[395] with the Cybersecurity Coalition and Information Technology Industry Council (Cybersecurity Coalition/ITI) noting that they are "pleased" that the Pilot is focused on "how to balance [the] 'complementary work of federal agency partners.'"[396] We agree with commenters on the importance of leveraging the expertise of our federal, state, and local partners, and adopting this goal for the Pilot Program signals our intent to continue to work collaboratively on shared objectives to streamline our efforts to address schools' and libraries' cybersecurity challenges. To this end, we agree with commenters that, where possible, we should align our Pilot with the cybersecurity goals of our federal partners.[397]

107. *Data reporting*. To measure the Pilot's success in meeting the aforementioned goals, we adopt initial, annual, and final reporting requirements for participants. In the *Cybersecurity NPRM*, we proposed that Pilot participants submit certain information to apply for the Pilot, a progress report for each year of the Pilot, and a final report at the conclusion of the Pilot.[398] We also proposed that these

(Continued from previous page)
Commission's question on whether eligibility for the pilot should require that applicants implement recommendations from federal agencies or take advantage of free federal resources, the Council does not recommend conditioning participation on these grounds. As mentioned above, many urban districts are already implementing several low-cost and high-leverage cybersecurity strategies. Requiring evidence of wholesale implementation or use of these resources could potentially eliminate under-resourced districts from the pool of applicants.").

[392] *See e.g.*, CTIA Reply at 9 ("CTIA supports the idea of mandating that 'participating K-12 schools and libraries fully leverage the free and low-cost K-12 cybersecurity resources provided by our federal partners, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and the U.S. Department of Education"); Cisco Comments at 8 ("CISA is the federal government's expert agency for cybersecurity. It is therefore appropriate for the Commission to leverage the CISA K-12 cybersecurity recommendations in determining eligible services for the Pilot Program."); CIS Comments at 3 ("Funding should be allowed for any cybersecurity protection that improves or enhances the cybersecurity of an organization, such as those contained in the CIS Critical Controls, the [Education Department] or CISA K-12 cybersecurity recommendations, or the CISA Cybersecurity Performance Goals (CPGs).").

[393] Friday Institute Comments at 9.

[394] CTIA Reply at 4 ("As the Commission implements this program, it should continue to coordinate closely with other federal agencies, including the Cybersecurity and Infrastructure Security Agency ("CISA") and the Department of Education.").

[395] K12 Tech Talk Podcast Comments at 2 (K12 Tech Talk); K12 TechPro Comments at 2.

[396] Cybersecurity Coalition/Information Technology Industry Council Comments at 2. *See also* Palo Alto Network Comments at 6; MISEN Comments at 12.

[397] Apptegy Comments at 2 ("Apptegy believes that Commission's Schools and Libraries Cybersecurity Program should be as aligned as possible with the Cybersecurity Infrastructure and Security Agency (CISA) cross-sector cybersecurity performance goals (CPGs) and recommendations."); CIS Comments at 3 ("Funding should be allowed for any cybersecurity protection that improves or enhances the cybersecurity of an organization, such as those contained in the CIS Critical Controls, the DOE or CISA K-12 cybersecurity recommendations, or the CISA Cybersecurity Performance Goals (CPGs)."); Cybersecurity Coalition/ITI Comments at 5 ("The Coalition and ITI are also supportive of the Commission allowing participants to use Pilot funds to meet any of the Department of Education or CISA K-12 Cybersecurity recommendations or CISA CPGs to otherwise improve their cybersecurity posture."); Rubrik Comments at 3 ("Requiring that applications fall within CISA's K-12 Cybersecurity Report guidance or CISA's Cybersecurity Performance Goals (CPGs) gives applicants some needed flexibility while also ensuring applications will meet the goals of the pilot.").

[398] *Cybersecurity NPRM,* 2023 WL 8605080 at *10, paras. 23-24.

reports contain information on how Pilot funding was used, any changes or advancements that were made to the school's or library's cybersecurity efforts outside of the Pilot-funded services and equipment, the number of cyber incidents that occurred each year of the Pilot Program, and the impact of each cyber incident on the school's or library's broadband network and data.[399] We sought comment on these proposals, as well as the best ways for the Commission to evaluate the Pilot and measure progress towards the proposed performance goals.[400]

108. Commenters generally agreed with our proposal to establish data reporting requirements.[401] Crown Castle Fiber LLC (Crown Castle) noted the value of data reporting requirements, stating that they provide "valuable insight into the types of new services and equipment that applicants purchase to address their network and data security concerns and the impact of implementing various cybersecurity solutions."[402] FFL emphasized that the effectiveness of the Pilot Program should be measured by progress made toward the implementation of solutions and tactics known to increase resiliency to attacks, not by the presence or characteristics of cyberattacks or applicant responses during an applicant's participation in the Pilot.[403] CTIA suggested that the reporting requirements use standardized metrics to obtain a common baseline of data across participants to aid in program evaluation.[404]

109. Some commenters provided detailed recommendations about the reporting metrics the Commission should use to gather and report Pilot data. CrowdStrike, for example, stated that one promising evaluation metric is mean time to detection and response, and suggested that the Commission designate a "control group" of similar organizations to assess Pilot success.[405] Rubrik proposed a variety of metrics to measure Pilot effectiveness, such as the ability to quickly recover from a cyber event; identify sensitive data on the network where it resides and determine who has access to it; and test cyber recovery functionality to properly plan for a cyber event.[406] The City of New York Office of Technology and Innovation (City of NY OTI) suggested specific metrics that could include "Mean Time to Detect"; "Mean Time to Response"; "False Positive Rate"; "True Positive Rate"; and "Investigation Rate to Incident Containment Rate."[407]

110. Based on the record, we adopt the requirement for initial, annual, and final reporting so that Pilot participants evaluate and report on their cybersecurity readiness before they begin participation in, during, and after the Pilot Program.[408] Specifically, after providing an initial baseline assessment using information that includes the reporting requirements for the second part of the application process

[399] *Id*.

[400] *Id*.

[401] *See e.g.* CTIA Reply at 2 ("CTIA supports the broad consensus that the Pilot Program should be carefully structured, with clear goals and metrics and associated reporting requirements, to obtain actionable data on whether and how to effectively support cybersecurity going forward."); Crown Castle Comments at 3 ("To this end, Crown Castle supports the Commission's proposed data collection and reporting requirements for Pilot Program applicants, including submission of a proposed advanced cybersecurity action plan and ongoing reporting on cybersecurity incidents during the funding period.").

[402] Crown Castle Comments at 3.

[403] FFL Reply at 4.

[404] CTIA Reply at 6.

[405] CrowdStrike Comments at 5.

[406] Rubrik Comments at 2-3.

[407] City of NY OTI Reply at 1.

[408] *See also* 47 CFR § 54.2004(e) (codifying the Pilot data reporting requirements and adopting measures regarding non-compliance with the rule).

explained in more detail in Section E above,[409] Pilot participants will be required to submit annual reports, followed by a final report at the completion of the program. In establishing these periodic reporting requirements, the Commission seeks to balance its need for gathering the data necessary to evaluate the goals and success of the Pilot with commenters' recommendations that it minimize the burden on Pilot participants to the extent possible.[410] We find that tracking participants' cybersecurity progress over the course of the Pilot will be essential in helping us determine whether and how to fund schools' and libraries' cybersecurity needs through the E-Rate program or another universal service program on an ongoing basis. As stated below, information contained in initial, annual, and final reports will be presumptively confidential; however, we do plan to use school or library data as a tool to evaluate the Pilot and determine next steps. Additionally, at our discretion, we may create for public release a version of this information that is aggregated, anonymized, or otherwise not subject to protection from disclosure under the Freedom of Information Act. To accomplish the goal of periodic reporting by Pilot participants, we delegate to the Bureau the authority to use school and library data to evaluate the Pilot, as well as the authority to create and release a public version of this information, as described above. We also direct the Bureau to release a Public Notice (or multiple Public Notices, as needed) detailing the specific information to be provided by Pilot participants, the timing for the submission of these reports, and to consider developing a standardized reporting form and publicizing its availability. In developing the required reporting metrics, we direct the Bureau to consult with OEA and relevant federal partners to identify those metrics that will best serve the needs of the Pilot and allow the Commission to evaluate whether and to what extent the Pilot succeeded in meeting the three performance goals discussed above.[411]

111. Finally, in making these data reporting recommendations, a few commenters expressed concerns about protecting both the sensitive nature of the data and insulating Pilot applicants and participants from malicious cybersecurity actors who would use the data for nefarious purposes.[412] We are sensitive to and agree with these concerns and have measures in place to protect the school- and library-specific cybersecurity data it requests as part of the Pilot Program.[413] Specifically, we find that the information provided by Pilot participants in the initial, annual, and final reports required by the Pilot constitutes sensitive business information and the reports may also contain trade secrets. We therefore will treat this information as presumptively confidential under our rules and withhold it from public inspection.[414] In addition, and as addressed in more detail above, we have elected to bifurcate the application process, seeking a more general level of cybersecurity information from applicants and leaving the more detailed cybersecurity reporting for Pilot participants.[415] Taken together, we expect that

[409] *See supra* para. 75.

[410] We disagree with commenters that recommend the Commission avoid collecting detailed information because such an approach unnecessarily hamper our ability to effectively evaluate the Pilot. *See* Friday Institute Comments at 8 ("[W]e advise against the data collection methodology proposed in the NPRM. Requesting schools to disclose potentially sensitive security data, or to quantify attacks and mitigations, may not yield statistically valid or meaningful results. Such data could be misleading and possibly jeopardize school security.").

[411] We do not expect that such metrics should require—or even invite—participants to include the personally identifiable information of students, staff, or library patrons, except to the extent that a point of contact or certifying official is required for such reports. If the Bureau determines there may be a need for such information, we direct it to consult with the OGC—and specifically the Senior Agency Official for Privacy—to ensure appropriate protections are in place for such information.

[412] *See* CIS Comments at 5 (stressing the importance of safeguarding sensitive information provided as part of the Pilot and protecting the anonymity of the filing entity); Friday Institute Comments at 8; WI DPI Reply at 3.

[413] *See supra* paras. 62 & note 223, 76 & note 301.

[414] *See* 47 CFR § 0.457(d); *see also supra* paras. 62, 76 (discussing confidentiality of information contained in the FCC Form 484).

[415] *See supra* paras. 64, 75.

these measures will alleviate commenters' concerns about protecting Pilot participants' sensitive information regarding cybersecurity threats and readiness.

J. Appeals of USAC Decisions and Waiver Requests

112. We provide a path for recourse to parties aggrieved by decisions issued by USAC as a result of or during the Pilot. Specifically, we adopt appeal and waiver request rules consistent with those that govern USAC's administration of the USF programs, including the E-Rate program.[416] We find these existing processes sufficient to provide a meaningful review of decisions issued by USAC and the Commission regarding the Pilot. However, we make one modification for the Pilot Program appeal and waiver rules and provide a 30-day timeframe to request the review of an action by USAC,[417] or to request the review of a decision by USAC or a waiver of the Commission's rules.[418] Despite assertions from some commenters that modifying the rules in this manner would limit Pilot participant flexibility and is unnecessary in this context,[419] we think this change will benefit Pilot participants (and the program generally) by providing faster timeframes for appeal and waiver decisions and final Pilot funding decisions. Additionally, we find that a 30-day timeframe is appropriate given the limited three-year duration of the Pilot Program.

K. Legal Authority

113. We conclude that the Commission has legal authority to establish a Pilot Program that provides USF support for cybersecurity services and equipment to eligible schools and libraries. As a preliminary matter, in the *Cybersecurity NPRM*, we tentatively concluded that the Commission has sufficient legal authority for funding cybersecurity services and equipment for schools and libraries pursuant to sections 254(c)(1), (c)(3), (h)(1)(B), and (h)(2) of the Act.[420] We noted that the Pilot is consistent with Congress's view that the USF represents an evolving level of service, informing potential future actions that the Commission would take to further its obligation to "establish periodically" universal service rules that "tak[e] into account advances in telecommunications and information technologies and services."[421] Additionally, we noted that the existing record supported the view that the Pilot is "technically feasible and economically reasonable" as required by section 254(h)(2)(A) of the Act.[422] We also noted that the proposed Pilot appeared consistent with section 254(c)(3) of the Act, which grants the Commission authority to "designate additional services for [USF] support . . . for schools [and] libraries", as the Pilot would allow for the designation of additional services that may be used by participating schools and libraries based on USF funding.[423] In the *Cybersecurity NPRM*, we sought additional comment on such views and on the other sources of legal authority, such as the extent to which the Pilot fulfills the Commission's mandate to make "[q]uality services" available at just, reasonable, and affordable rates,[424] and the limits and restrictions that we should place on recipients of Pilot funds to remain within the statutory authority.[425]

---

[416] *See* 47 CFR § 54.2012; s*ee also* 47 CFR §§ 54.719-54.725.

[417] 47 CFR § 54.2012(b).

[418] *Id*. Section 54.720 of the rules allows 60 days to request review or a waiver.

[419] Lumen Reply at 7; NCTA Comments at 5-6.

[420] *Cybersecurity NPRM,* 2023 WL 8605080 at * 21, para. 52.

[421] *Id.;* 47 U.S.C. § 254(c)(1).

[422] *Cybersecurity NPRM,* 2023 WL 8605080 at *22, para. 54; *see* 47 U.S.C. § 254(h)(2)(A).

[423] *Cybersecurity NPRM,* 2023 WL 8605080 at *23, para. 57; *see* 47 U.S.C. § 254(c)(3).

[424] *Cybersecurity NPRM,* 2023 WL 8605080 at *23, para. 58; *see* 47 U.S.C. § 254(b)(1).

[425] *Cybersecurity NPRM,* 2023 WL 8605080 at *23, para. 60.

114. Commenters generally supported our conclusion that sufficient legal authority exists for the creation of this Pilot Program.[426] In particular, commenters agreed that universal service is an "evolving level of telecommunications services,"[427] and noted that the Pilot-supported services and equipment "reflect ongoing advances in schools and libraries broadband networks and services."[428] Furthermore, Cisco stated that enhanced cybersecurity services and equipment strengthens and ensures access to and usability of broadband networks, supporting the Act's mandate that the Commission enhance access to advanced telecommunications and information services for schools and libraries.[429] Cisco also noted that the scale and number of cyber threats and attacks increased during the pandemic, as schools shifted to heavier reliance on technology services, and "such changed circumstances support consideration of a change in the Commission's policy with respect to the funding of cybersecurity measures for schools and libraries," in furtherance of Congress's mandate "to take into account evolving technologies and to designate additional services to support enhanced connectivity for schools and libraries."[430]

115. We agree with these assessments, and affirm our conclusion in the *Cybersecurity NPRM* that the Commission has sufficient legal authority to use universal service funds to support cybersecurity services and equipment for eligible schools and libraries, for several reasons. First, we agree that providing support for cybersecurity services and equipment fulfills our mandate under section 254(c)(1) of the Act to periodically refine universal service to take into account advances in technology and services.[431] As CoSN points out, the Pilot Program will provide support for new services and equipment that reflect advances in school networking technology.[432] By studying how best universal service funds can be used to support E-Rate funded networks and data, the Pilot enables us to refine universal service in today's modern educational environment, pursuant to section 254(c)(1) of the Act.

116. Second, we find that Pilot funds will be used for "educational purposes," pursuant to section 254(h)(1)(B) of the Act.[433] E-Rate rules require schools and libraries to use eligible services "primarily for educational purposes," defined for schools as "activities that are integral, immediate, and proximate to the education of students," and for libraries as "activities that are integral, immediate, and proximate to the provision of library services to library patrons."[434] Pilot funds will help ensure that school and library connections are reliable and not disrupted by cyberattacks, and will further protect the sensitive data often stored on those networks. As such, use of Pilot funds serves an educational purpose,

[426] ACSA-CSBA Federal Partnership Reply at 5 ("The ACSA-CSBA Partnership believes the Commission has clear legal authority through Section 254 of the Telecommunications Act of 1996 to conduct the proposed cybersecurity pilot program."); Cisco Comments at 6 ("[T]he Commission has the requisite legal authority to use universal service funding to support the provision of cybersecurity and advanced firewall services to participating schools and libraries."); CoSN et al. January 29 Comments at 8-9 ("We agree with the Commission's analysis and finding that it has the legal authority for the proposed pilot."); EdGroup Reply at 3 ("We agree with the Commission's analysis that it has the legal authority to move forward with this pilot.").

[427] 47 U.S.C. § 254(c)(1).

[428] CoSN et al. January 29 Comments at 8-9.

[429] Cisco Comments at 13.

[430] *Id*. at 14-15.

[431] 47 U.S.C. § 254(c)(1).

[432] CoSN et al. January 29 Comments at 8-9.

[433] 47 U.S.C. § 254(h)(1)(B) (providing that E-Rate discounts be applied to services provided to eligible schools and libraries for "educational purposes").

[434] 47 CFR §§ 54.500; 54.504(a)(v); *Schools and Libraries Universal Service Support Mechanism*, CC Docket No. 02-6, Second Report and Order and Further Notice of Proposed Rulemaking, 18 FCC Rcd 9202, 9208, para. 17 (2003).

by promoting the education of students, or the provision of library services to library patrons, free from disruption, cyberattack, or theft of sensitive data, pursuant to our mandate under section 254(h)(1)(B) of the Act.

117. Furthermore, we conclude that the use of universal service support for advanced firewalls and other cybersecurity services and equipment for educational purposes fits within the Commission's authority and direction under section 254(h)(1)(B) of the Act to designate "services that are within the definition of universal service under subsection (c)(3)," which authorizes the Commission to designate non-telecommunications services for support.[435] In the *First Universal Service Order*, we found that section 254(h)(1)(B) through section 254(c)(3) of the Communications Act authorizes universal service support for telecommunications services *and* additional services such as information services.[436] We therefore find that, to the extent any of the advanced firewall or cybersecurity services are not telecommunications services, those services nevertheless can be purchased with universal service support pursuant to section 254(h)(1)(B) of the Act. In addition, section 254(h)(1)(B) through section 254(c)(3) of the Act provides authority to support the advanced firewall and cybersecurity equipment that the Pilot will fund to protect E-Rate funded networks and data. In the *First Universal Service Order*, the Commission concluded that "we can include 'the information services,' e.g., protocol conversion and information storage, that are needed to access the Internet, as well as internal connections, as 'additional services' that section 254(h)(1)(B), through section 254(c)(3), authorizes us to support."[437] The Commission further distinguished between ineligible types of peripheral equipment (e.g., laptops) and eligible equipment that is necessary to make the services functional.[438] Therefore, we also find that because advanced firewall and cybersecurity equipment are critical to support the services that will protect E-Rate funded networks and data, they fall into the latter category and we therefore conclude that the Commission has authority under section 254(h)(1)(B) through section 254(c)(3) of the Act to support the purchase of advanced firewall and cybersecurity equipment for educational purposes.

118. Additionally, the Commission has concluded that, pursuant to sections 4(i) and 254(c)(1), (c)(3), (h)(1)(B), and (h)(2) of the Act, E-Rate supported services can be provided by both telecommunications carriers and non-telecommunications carriers.[439] In reaching this conclusion, the

---

[435] *Federal State Joint Board on Universal Service*, CC Docket No. 96-45, Report and Order, 12 FCC Rcd 8776, 9009-11, paras. 437-39 (1997) (*First Universal Service Order*) (concluding that section 254(h)(1)(B) through section 254(c)(3) of the Communications Act authorizes universal service support for telecommunications services *and* additional services such as information services). Note that this was upheld in *Texas Office of Public Utility Counsel v. FCC*, 183 F.3d 393 (5th Cir. 1999). In particular, the Fifth Circuit found that sections 254(c) and (h) of the Communications Act provided authority for various aspects of the E-Rate and Rural Health Care programs, including the conclusion that the Communications Act authorizes universal service support for telecommunications services and additional services such as information services. *Id.*, 183 F.3d at 440-46. The Commission continues to find the Court's reasoning persuasive on this issue.

[436] *See First Universal Service Order*, 12 FCC Rcd at 9010-11, para. 439 (stating that "[T]he term used in section 254(h)(1)(B), 'any of its *services* that are within the definition of universal service under subsection (c)(3),' cannot be read as a generic reference to the heading of that section. Rather, the varying use of the terms 'telecommunications services' and 'services' in sections 254(h)(1)(A) and 254(h)(1)(B) suggests that the terms were used consciously to signify different *meanings*. In addition, the mandate in section 254(h)(2)(A) to enhance access to "advanced telecommunications and information services," particularly when read in conjunction with the legislative history as discussed below, suggests that Congress did not intend to limit the support provided under section 254(h) to telecommunications services.'").

[437] *See First Universal Service Order*, 12 FCC Rcd at 9010-11, para. 439.

[438] *See also First Universal Service Order*, 12 FCC Rcd at 9021, para. 459 (holding that equipment such as a router is eligible for support if "necessary to transport information all the way to individual classrooms").

[439] *See Universal Service First Report and Order*, 12 FCC Rcd at 9008-15, paras. 436-49, and 9084-90, paras. 589-600; *Sixth Report and Order*, 25 FCC Rcd at 18767-68, para. 10.

Commission determined that section 254(h)(1)(B)'s requirement that discounts for services be provided to "telecommunications carriers" does not "stand as a bar to our authority to allow non-telecommunications providers to provide such services and participate in the E-rate program" under sections 254(h)(2)(A) and 4(i) because limiting the eligibility of such services to only those provided by telecommunications carriers would "unduly limit the flexibility of schools and libraries to select the most cost-effective broadband solutions to meet their needs, which would be inconsistent with our schools and libraries policies."[440] Moreover, permitting the provision of such services by both telecommunications and non-telecommunications carriers "enhances access to advanced telecommunications and information services for public and non-profit elementary and secondary school classrooms and libraries."[441] Consistent with this authority, we likewise allow Pilot participants to purchase eligible services and equipment from both telecommunications and non-telecommunications providers because it will provide Pilot participants with greater access and flexibility to select the best option at lower costs.

119. Third, and separately, we affirm our authority under section 254(h)(2)(A) of the Act, as the Pilot will enhance access to advanced telecommunications and information services for elementary and secondary school classrooms and libraries.[442] The use of Pilot-supported services to protect school and library broadband networks further enhances school classroom and library access to other advanced telecommunications and information services.[443] Specifically, we agree with CoSN that "cyberattacks throttle or completely thwart the ability of schools and libraries to use the 'advanced telecommunications and information services' promised by the Act."[444] Supporting cybersecurity services through the Pilot will enable and encourage participants to make full use of their connectivity services, with the reassurance that their broadband networks and services, and the information contained in them is protected.

120. Lastly, we find that the Pilot Program is economically reasonable, and a prudent use of limited universal service funds. The Commission has previously found that expanding the types of cybersecurity services and equipment beyond basic firewall services to be cost-prohibitive to the E-Rate program.[445] Since then, however, the COVID-19 pandemic changed how K-12 schools and libraries use their broadband networks for educational purposes, and K-12 schools and libraries increasingly find themselves prime targets for cyber threats and attacks by malicious actors who seek to exploit the schools' and libraries' network data.[446] In light of such developments, as well as an increased cap for E-Rate funding, exploring expanding funding for cybersecurity services and equipment beyond basic firewalls is now prudent to determine whether there is more the Commission can do to protect schools' and libraries' E-Rate-funded broadband networks. Furthermore, by conducting a limited Pilot, the Commission can best determine whether it can support these essential services without jeopardizing the ability of the E-Rate program to continue to support the connectivity of school and library broadband

[440] *See Sixth Report and Order*, 25 FCC Rcd at 18768, para. 11.

[441] *See* 47 U.S.C. § 254(h)(2)(A); *Sixth Report and Order*, 25 FCC Rcd at 18767-68, paras. 10-11.

[442] *See* 47 U.S.C. § 254(h)(2)(A).

[443] 47 U.S.C. § 254(h)(2)(A); *see also* CoSN Comment at 8 (stating that without the proposed supported cybersecurity services, schools and libraries will be unable to fully utilize their e-rate supported networks. As of now, cyber and ransomware attacks have already caused numerous schools and libraries to routinely shut down their networks entirely or face costly disruptions that prohibit user access.); *see also Cybersecurity NPRM,* 2023 WL 8605080 at *22, para. 54.

[444] CoSN et al. January 29 Comments at 9.

[445] *See, e.g.*, *Schools and Libraries Sixth Report and Order*, 25 FCC Rcd at 18808-18809, para. 105 (declining to extend basic firewall services because the limited funds available to support E-Rate); *2019 Category Two Budget Order*, 34 FCC Rcd at 11236-37, para. 46 & n.123 (declining to make additional services eligible to focus funding on internal connections needed to deliver high-speed broadband to students and library patrons via LANs and WLANs).

[446] *See supra* para. 5.

networks. Generally, commenters were in favor of increasing funding to support cybersecurity services beyond basic firewalls. For example, CIS recommended that the Commission "allow funding for any cybersecurity protection that improves or enhances the cybersecurity of an organization."[447] Cisco stated that "enhanced cybersecurity and advanced firewalls are needed for the delivery of reliable and useable broadband connectivity to students and educators" and funding such services is "consistent with the public interest, convenience, and necessity."[448] As a result, we find funding cybersecurity services and equipment through the Pilot to be a prudent use of the limited USF support and conclude that the Pilot is economically reasonable pursuant to section 254(h)(2)(A) of the Act.

L. The Children's Internet Protection Act

121. We conclude that the requirements of the Children's Internet Protection Act (CIPA) are triggered by the purchase of eligible services or equipment through the Pilot Program. As we have explained in the E-Rate and ECF programs, CIPA applies to the use of school- or library-owned computers, including laptop and tablet computers, if the school or library accepts support for services and equipment that are used for Internet access, Internet services, or internal connections.[449] As discussed in the *Cybersecurity NPRM*, Congress enacted CIPA to protect children from exposure to harmful material while accessing the Internet from a school or library,[450] and CIPA prohibits certain schools and libraries having computers with Internet access from receiving funding under section 254(h)(1)(B) of the Act unless they comply with specific Internet safety requirements.[451] Our determination that CIPA is applicable to the Pilot Program is consistent with past Commission decisions in the E-Rate program[452] and E-Rate ESLs which have included both basic firewall services provided as a standard component of a vendor's Internet access service as category one Internet access services, and standalone basic firewall

[447] CIS Comments at 11.

[448] Cisco Comments at 15.

[449] *See* 47 CFR § 54.520; *Emergency Connectivity Fund Report and Order*, 36 FCC Rcd at 8748, para. 111.

[450] *See* S. Rep. No. 106-141, at 1 (1999), https://www.congress.gov/106/crpt/srpt141/CRPT-106srpt141.pdf ("The purpose of the bill is to protect America's children from exposure to obscene material, child pornography, or other material deemed inappropriate for minors while accessing the Internet from a school or library receiving Federal Universal Service assistance for provisions of Internet access, Internet service, or internal connection[s].").

[451] 47 U.S.C. § 254(h)(5)(A)(i) and 254(h)(6)(A)(i). CIPA requires each covered school and library that receives funding for the provision of Internet access, Internet services, and internal connections to certify that the school or library is: (1) "enforcing a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access [by both adults and minors] through such computers" to visual depictions that are (i) obscene; (ii) child pornography; or, (iii) with respect to use of the computers by minors, harmful to minors; and (2) "enforcing the operation of such technology protection measure during any use of such computers" by minors and adults. 47 U.S.C. §§ 254(h)(5)(B)(i),(ii) and (C)(i),(ii), (h)(6)(B)(i)(ii) and (C)(i)(ii), and (l); 47 CFR §§ 54.520(c)(1)(i), (c)(2)(i).

[452] *See Sixth Report and Order*, 25 FCC Rcd at 18808-18809, para. 105 (retaining support for basic firewalls because they protect against unauthorized access to schools' and libraries' networks); *First 2014 E-Rate Order*, 29 FCC Rcd at 8917-8919, paras. 119 (providing internal connections support for firewall services to help deploy [the] LANs/WANs necessary to permit digital learning in schools and libraries throughout the nation); 120-21 (moving firewalls into the list of eligible category two internal connections components necessary to help deploy the LANs/WLANs needed to improve digital learning in schools and libraries); *see also Modernizing the E-Rate Program for Schools and Libraries et al.*, WC Docket No. 13-184 et al., Order, 29 FCC Rcd 13404, 13422 (WCB Oct. 28, 2014) (*FY 2015 ESL Order*) (including as eligible for E-Rate support those internal connections components necessary to *help deploy* internal broadband connections (e.g. firewall services and components, racks, uninterruptible power supply/battery back-up)). In reaching this determination, we agree with CCSD who states that CIPA compliance should be a requirement of the Pilot for a seamless shift to E-Rate. CCSD Comments at 1-2.

services and components as category two internal connections services.[453] Because the cybersecurity services and equipment we make eligible under the Pilot Program serve functions equivalent to that of the basic firewall services currently supported by the E-Rate program, we treat them similarly, either as standalone internal connections or as components of Internet access. We therefore conclude that the provision of Pilot support is also governed by sections 254(h)(5)(A)(i) and 254(h)(6)(A)(i) of the Act, and compliance with the CIPA Internet safety requirements is a condition of the receipt of Pilot Program support.[454] As with the E-Rate and ECF programs, we also conclude that CIPA does not apply where schools or libraries have purchased services to be used only in conjunction with student-, school staff-, or library patron-owned computers.[455] Also, consistent with the ECF program, we find that a Pilot participant need not complete additional CIPA compliance certifications if it has already certified its CIPA compliance for E-Rate support for the funding year preceding the start of the Pilot (i.e., it has certified its compliance in an E-Rate FCC Form 486 or FCC Form 479).[456] If a Pilot participant has not previously certified its CIPA compliance in the E-Rate program, it will need to do so to qualify for Pilot Program support or certify that it is taking actions to come into compliance with the CIPA requirements.[457]

M. Delegations of Authority to the Bureau and the Office of Managing Director

122. In order to ease program administration, we delegate to the Bureau, consistent with the goals of the Pilot Program, the authority to waive certain program deadlines, clarify any inconsistencies or ambiguities in the Pilot Program rules, adjust Pilot project funding commitments, or to perform other

[453] Early Commission orders and the corresponding E-Rate ESLs made firewalls eligible based on the underlying eligible services and equipment they support. *See, e.g., Universal Service First Report and Order*, 12 FCC Rcd at 9003, 9021, paras. 426, 460 (finding that Section 254 defines the services that are to be supported for schools and libraries in terms of telecommunications, special or additional services, and access to "advanced telecommunications and information services" and concluding that internal connections include "the software file servers need to operate"); *First 2014 E-Rate Order*, 29 FCC Rcd at 8917, para. 120 (retaining E-Rate support for priority two firewalls that had previously been listed under the E-Rate ESL Data Protection entry to ensure more E-Rate support was directed to deploy the LANs/WANs needed to improve digital learning in schools and libraries); *see also* USAC, *FY 1998 ESL*, https://www.usac.org/wp-content/uploads/e-rate/documents/ESL_archive/EligibleServicesList_032898.pdf (last visited May 13, 2024) (making firewalls eligible for E-Rate support as application software "when required for file server operations").

[454] This includes the adoption and enforcement of an Internet Safety Policy that requires the operation of a technology protection measure. 47 U.S.C. § 254(h)(5)(A)(i), (B), (h)(6)(A)(i), (B); *see also id*. § 254 (l) (setting forth other Internet Safety Policy requirements). By its text, CIPA applies to schools and libraries seeking "services at discount rates under paragraph(1)(B)" except for services other than the provision of Internet access, Internet service, or internal connections. *Id.* §§ 254(h)(5)(A)(i)-(ii), (h)(6)(A)(i)-(ii). The Commission has consistently interpreted these provisions to mean that CIPA "only applies to entities receiving Internet access, Internet service, or internal connections" and excludes schools and libraries receiving only telecommunications services. *See, e.g.*, *Children's Internet Protection Act*, CC Docket No. 96-45, Report and Order, 16 FCC Rcd 8182, *8195-96, para. 28 (2001) (2001 CIPA Order).* Schools, but not libraries, must also provide education about appropriate online behavior including cyberbullying. *Schools and Libraries Universal Service Support Mechanism et al.*, CC Docket No. 02-6, Report and Order, 26 FCC Rcd 11819, 11821, para. 5 (*2011 CIPA Order*).

[455] *See e.g.*, *Emergency Connectivity Fund Report and Order*, 36 FCC Rcd at 8749, para. 113 (discussing the applicability of CIPA and concluding that CIPA does not apply to the use of third-party owned devices). In reaching this conclusion, we agree with EPIC who states that CIPA does not extend to third-party devices that may connect with school- or library-owned broadband networks. EPIC Reply at 6.

[456] *See* 47 U.S.C. § 254(h)(5)(A)(i), (6)(A)(i) (requiring certifications concerning section 254(h)(5), (h)(6), and (l)). If an E-Rate applicant's existing certification states that CIPA does not apply because the applicant is receiving only telecommunications services, the participant will be required to provide CIPA certifications via the FCC Form 471 to participate and receive support through the Pilot Program.

[457] 47 CFR § 54.2013 (listing the required CIPA certifications to participate in the Pilot Program).

administrative tasks as may be necessary for the smooth implementation, administration, and operation of the Pilot Program. We also delegate to the Bureau the authority to grant limited extensions of deadlines to Pilot projects, and other authority as may be necessary to ensure a successful Pilot Program.

123. In addition, we delegate financial, information security, and privacy oversight of the Pilot Program to OMD and OGC and direct OMD and OGC to work in coordination with the Bureau to ensure that all financial, information security, and privacy aspects of the Pilot have adequate internal controls. These duties fall with OMD's current delegated authority to ensure that the Commission operates in accordance with federal financial statutes and guidance.[458] OMD performs this role with respect to USAC's administration of the Commission's Universal Service Programs[459] and we anticipate that OMD will leverage existing policies and procedures, to the extent practicable and consistent with the Pilot, to ensure the efficient and effective management of the program. Finally, we note OMD is required to consult with the Bureau on any policy matters affecting the Pilot Program, consistent with section 0.91(a) of the Commission's rules.

124. We direct the Bureau to conduct outreach to educate eligible schools and libraries about the Pilot Program, and to coordinate, as necessary, with other federal agencies, and state, local, and Tribal governments. As supported by the record in this proceeding, we also direct USAC to develop and implement a communications strategy, under the oversight of the Bureau, to provide training and information necessary for schools and libraries to successfully participate in the Pilot Program. Outreach, education, and engagement with Pilot Program applicants and, ultimately, selected Pilot participants will be an important tool in ensuring the Pilot Program is successful and meets its goals.

125. We recognize that once implementation of the Pilot Program begins, the Bureau may encounter unforeseen issues or problems with the administration of the program that may need to be resolved.[460] To promote maximum effectiveness and smooth administration of the Pilot Program, we delegate to Bureau staff the authority to address and resolve such unforeseen administrative issues or problems, provided that doing so is consistent with the decisions we reach here today.

IV. PROCEDURAL MATTERS

126. *Regulatory Flexibility Act.* The Regulatory Flexibility Act of 1980, as amended (RFA),[461] requires that an agency prepare a regulatory flexibility analysis for notice and comment rulemakings, unless the agency certifies that "the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities."[462] Accordingly, we have prepared a Final

[458] 47 CFR § 0.11(a)(3)-(4) (stating that the OMD will "[a]ssist the Chair[person] in carrying out the administrative and executive responsibilities" and "[a]dvise the Chair[person] and Commission on management, administrative, and related matters; review and evaluate the programs and procedures of the Commission; initiate action or make recommendations as may be necessary to administer the Communications Act most effectively in the public interest"); 47 CFR § 0.11(a)(8) (stating that OMD's current responsibility is to "[p]lan and manage the administrative affairs of the Commission with respect to the functions of . . . budget and financial management"); 47 CFR § 0.5(e) (requiring Bureau and Office coordination with the OMD on recommendations "that may affect agency compliance with Federal financial management requirements").

[459] *See, e.g.*, FCC/USAC MOU (stating that the Commission is responsible for the effective and efficient management and oversight of the USF, including USF policy decisions, and USAC is responsible for the effective administration of the programs).

[460] *See, e.g.*, E-Rate Central Comments at 3 (mentioning that the Commission may want to incorporate or apply the outcomes of other cybersecurity proceedings during the course of the Pilot).

[461] 5 U.S.C. §§ 601–612. The RFA has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[462] 5 U.S.C. § 605(b).

Regulatory Flexibility Analysis (FRFA) concerning the possible impact of the rule changes contained in this *Report and Order* on small entities. The FRFA is set forth in Appendix D.

127. *Paperwork Reduction Act.* This Report and Order contains new information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget (OMB) to comment on the information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. In addition, the Commission notes that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C. § 3506(c)(4), we previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees.

128. *Congressional Review Act.* The Commission will submit this draft Report and Order to the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget (OMB), for concurrence as to whether this rule is "major" or "non-major" under the Congressional Review Act, 5 U.S.C. § 804(2). The Commission will send a copy of this Report and Order to Congress and the Government Accountability Office pursuant to 5 U.S.C. § 801(a)(1)(A).

129. *OPEN Government Data Act*. The OPEN Government Data Act,[463] requires agencies to make "public data assets" available under an open license and as "open Government data assets," *i.e.*, in machine-readable, open format, unencumbered by use restrictions other than intellectual property rights, and based on an open standard that is maintained by a standards organization.[464] This requirement is to be implemented "in accordance with guidance by the Director" of the Office of Management and Budget. (OMB).[465] The term "public data asset" means "a data asset, or part thereof, maintained by the Federal Government that has been, or may be, released to the public, including any data asset, or part thereof, subject to disclosure under [the Freedom of Information Act (FOIA)]."[466] A "data asset" is "a collection of data elements or data sets that may be grouped together,"[467] and "data" is "recorded information, regardless of form or the media on which the data is recorded."[468] We delegate authority, including the authority to adopt rules, to the Wireline Competition Bureau, in consultation with the agency's Chief Data and Analytics Officer and after seeking public comment to the extent it deems appropriate, to determine whether any data assets maintained or created by the Commission pursuant to the rules adopted herein are "public data assets" and if so, to determine when and to what extent such information should be made publicly available to the extent the Commission has not done so. In doing so, WCB shall take into account the extent to which such data assets should not be made publicly available because they are not subject to disclosure under the FOIA.[469]

130. *People with Disabilities.* To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice).

---

[463] Congress enacted the OPEN Government Data Act as Title II of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435 (2019), §§ 201-202.

[464] 44 U.S.C. §§ 3502(20), (22) (definitions of "open Government data asset" and "public data asset"), 3506(b)(6)(B) (public availability).

[465] OMB has not yet issued final guidance.

[466] 44 U.S.C. § 3502(22).

[467] 44 U.S.C. § 3502(17).

[468] 44 U.S.C. § 3502(16).

[469] *See, e.g.*, 5 U.S.C. § 552(b)(4), (6)-(7) (exemptions concerning confidential commercial information, personal privacy, and information compiled for law enforcement purposes, respectively).

131. For additional information on this proceeding, contact Joseph Schlingbaum of the Telecommunications Access Policy Division, Wireline Competition Bureau at Joseph.Schlingbaum@fcc.gov or at (202) 418-0829.

V. ORDERING CLAUSES

132. ACCORDINGLY, IT IS ORDERED, that pursuant to the authority contained in sections 1 through 4, 201-202, 254, 303(r), and 403 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151-154, 201-202, 254, 303(r), and 403, this Report and Order IS ADOPTED effective thirty (30) days after the publication of this Report and Order and Further Notice of Proposed Rulemaking in the Federal Register.

133. IT IS FURTHER ORDERED, that pursuant to the authority contained in sections 1 through 4, 201 through 202, 254, 303(r), and 403 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151-154, 201-202, 254, 303(r), and 403, Part 54 of the Commission's rules, 47 CFR Part 54, is AMENDED as set forth in Appendix A, and such rule amendments shall be effective (30) days after the publication of this Report and Order in the Federal Register, except for sections 54.2004, 54.2005, 54.2006, and 54.2008, which contain information collection requirements that are not effective until approved by the Office of Management and Budget. The FCC will publish a document in the Federal Register announcing the effective date for those sections.

134. IT IS FURTHER ORDERED that the Commission's Office of the Secretary SHALL SEND a copy of the Report and Order, including the Final Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

135. IT IS FURTHER ORDERED that the Office of the Managing Director, Performance Program Management, SHALL SEND a copy of this Report and Order in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act, 5 U.S.C. § 801(a)(1)(A).

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

APPENDIX A

Final Rules

For the reasons discussed above, the Federal Communications Commission amends part 54 of Title 47 of the Code of Federal Regulations as follows:

PART 54 – UNIVERSAL SERVICE

The authority for part 54 continues to read as follows:

Authority: 47 U.S.C. 151, 154(i), 155, 201, 205, 214, 219, 220, 229, 254, 303(r), 403, 1004, 1302, 1601-1609, and 1752.

1. Add subpart T to read as follows:

Subpart T -- Schools and Libraries Cybersecurity Pilot Program

§ 54.2000 Terms and Definitions.

*Administrato*r. The term "Administrator" means the Universal Service Administrative Company.

Applicant. An "applicant" is a school, library, or consortium of schools and/or libraries that applies to participate in the Schools and Libraries Cybersecurity Pilot Program.

Billed Entity. A "billed entity" is the entity that remits payment to service providers for services rendered to eligible schools, libraries, or consortia of eligible schools and libraries.

Commission. The term "Commission" means the Federal Communications Commission.

Connected device. The term "connected device" means a laptop or desktop computer, or a tablet.

Consortium. A "consortium" is any local, Tribal, statewide, regional, or interstate cooperative association of schools and/or libraries eligible for Schools and Libraries Cybersecurity Pilot Program support that seeks competitive bids for eligible services or funding for eligible services on behalf of some or all of its members. A consortium may also include health care providers eligible under subpart G of this part, and public sector (governmental) entities, including, but not limited to, state colleges and state universities, state educational broadcasters, counties, and municipalities, although such entities are not eligible for support.

Cyber incident. An occurrence that actually or potentially results in adverse consequences to an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate or eliminate the consequences.

Cyber threat. A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

*Cyberattac*k. An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system or information integrity.

Doxing. The act of compiling or publishing personal information about an individual on the Internet, typically with malicious intent.

Educational Purposes. For purposes of this subpart, activities that are integral, immediate, and proximate to the education of students, or in the case of libraries, integral, immediate and proximate to the provision of library services to library patrons, qualify as "educational purposes."

Elementary School. An "elementary school" means an elementary school as defined in 20 U.S.C. 7801(18), a non-profit institutional day or residential school, including a public elementary charter school, that provides elementary education, as determined under state law.

Library. A "library" includes:

(1) A public library;

(2) A public elementary school or secondary school library;

(3) A Tribal library;

(4) An academic library;

(5) A research library, which for the purpose of this section means a library that:

(i) Makes publicly available library services and materials suitable for scholarly research and not otherwise available to the public; and

(ii) Is not an integral part of an institution of higher education; and

(6) A private library, but only if the state in which such private library is located determines that the library should be considered a library for the purposes of this definition.

Library consortium. A "library consortium" is any local, statewide, Tribal, regional, or interstate cooperative association of libraries that provides for the systematic and effective coordination of the resources of schools, and public, academic, and special libraries and information centers, for improving services to the clientele of such libraries. For the purposes of these rules, references to library will also refer to library consortium.

National School Lunch Program. The "National School Lunch Program" is a program administered by the U.S. Department of Agriculture and state agencies that provides free or reduced price lunches to economically disadvantaged children. A child whose family income is between 130 percent and 185 percent of applicable family size income levels contained in the nonfarm poverty guidelines prescribed by the Office of Management and Budget is eligible for a reduced price lunch. A child whose family income is 130 percent or less of applicable family size income levels contained in the nonfarm income poverty guidelines prescribed by the Office of Management and Budget is eligible for a free lunch.

Pilot participant. A "Pilot participant" is an eligible school, library, or consortium of eligible schools and/or libraries selected to participate in the Schools and Libraries Cybersecurity Pilot Program.

Pre-discount price. The "pre-discount price" means, in this subpart, the price the service provider agrees to accept as total payment for its eligible services and equipment. This amount is the sum of the amount the service provider expects to receive from the eligible school, library, or

consortium, and the amount it expects to receive as reimbursement from the Schools and Libraries Cybersecurity Pilot Program for the discounts provided under this subpart.

Secondary school. A "secondary school" means a secondary school as defined in 20 U.S.C. 7801(38), a non-profit institutional day or residential school, including a public secondary charter school, that provides secondary education, as determined under state law except that the term does not include any education beyond grade 12.

Tribal. An entity is "Tribal" if it is a school operated by or receiving funding from the Bureau of Indian Education (BIE), or if it is a school or library operated by any Tribe, Band, Nation, or other organized group or community, including any Alaska native village, regional corporation, or village corporation (as defined in, or established pursuant to, the Alaska Native Claims Settlement Act (43 U.S.C. § 1601 *et seq*.) that is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians.

§ 54.2001 Cap, Budgets, and Duration.

(a) *Cap*. The Schools and Libraries Cybersecurity Pilot Program shall have a cap of $200 million.

(b) *Pilot Participant Budgets*. Each Pilot participant will be subject to a specific budget.

(1) *Schools*. At a minimum, each eligible school or school district will receive $15,000. Schools and school districts with 1,100 students or fewer will be eligible to receive the $15,000 funding floor. For schools and school districts with more than 1,100 students, the budget is calculated using the pre-discount price $13.60 per-student multiplier, subject a budget maximum of $1.5 million.

(2) *Libraries.* At a minimum, each eligible library will receive $15,000. Library systems with more than 11 sites will be eligible for support up to $175,000.

(3) *Consortia.* Consortia comprised of eligible schools and libraries will be eligible to receive funding based on student count, using the pre-discount $13.60 per student multiplier, and the number of library sites, using the $15,000 per library budget. Consortia solely comprised of schools or comprised of both eligible schools and libraries are subject to the $1.5 million budget maximum for schools and school districts. Consortia solely comprised of libraries will be subject to the $175,000 budget maximum for library systems.

(c) *Duration*. The Schools and Libraries Cybersecurity Pilot Program shall make funding available to selected Pilot participants (in accordance with § 54.2004 of this subpart) for three years, to begin when selected Pilot participants are first eligible to receive eligible services and equipment (i.e., from the date of the first funding commitment decision letter).

(d) *Rules of prioritization*. If total demand for the Schools and Libraries Cybersecurity Pilot Program exceeds the Pilot Program cap of $200 million, funding will be made available as follows:

(1) Schools and libraries eligible for a 90 percent discount shall receive first priority for funds, as determined by the schools and libraries discount matrix in § 54.2007. Funding shall next be made available for schools and libraries eligible

for an 80 percent discount, then for a 70 percent discount, and continuing at each descending discount level until there are no funds remaining.

(2) If funding is not sufficient to support all of the funding requests within a particular discount level, funding will be allocated at that discount level using the percentage of students eligible for the National School Lunch Program. Thus, if there is not enough support to fund all requests at the 90 percent discount level, funding shall be allocated beginning with those applicants with the highest percentage of NSLP eligibility for that discount level, and shall continue at each descending percentage of NSLP until there are no funds remaining.

§ 54.2002 Eligible Recipients.

(a) *Schools.*

(1) Only schools meeting the statutory definition of "elementary school" or "secondary school" as defined in § 54.2000, and not excluded under paragraphs (a)(2) or (3) of this section shall be eligible for discounts on supported services under this subpart.

(2) Schools operating as for-profit businesses shall not be eligible for discounts under this subpart.

(3) Schools with endowments exceeding $50,000,000 shall not be eligible for discounts under this subpart.

(b) *Libraries*.

(1) Only libraries eligible for assistance from a State library administrative agency under the Library Services and Technology Act (20 U.S.C. 9122) and not excluded under paragraph (b)(2) or (3) of this section shall be eligible for discounts under this subpart.

(2) Except as provided in paragraph (b)(4) of this section, a library's eligibility for discounts under this subpart shall depend on its funding as an independent entity. Only libraries whose budgets are completely separate from any schools (including, but not limited to, elementary and secondary schools, colleges, and universities) shall be eligible for discounts as libraries under this subpart.

(3) Libraries operating as for-profit businesses shall not be eligible for discounts under this subpart.

(4) A Tribal college or university library that serves as a public library by having dedicated library staff, regular hours, and a collection available for public use in its community shall be eligible for discounts under this subpart.

(c) *Consortia*.

(1) *Consortium Leader*. Each consortium seeking support under this subpart must identify an entity or organization that will the lead the consortium (the "Consortium Leader"). The Consortium Leader may be an eligible school or library participating in the consortium; a state organization; public sector governmental entity, including a Tribal government entity; or a non-profit entity

that is ineligible for support under this subpart. Ineligible state organizations, public sector entities, or non-profit entities may serve as Consortium Leaders or provide consulting assistance to consortia only if they do not participate as potential service providers during the competitive bidding process. An ineligible entity that serves as the Consortium Leader must pass through the full value of any discounts, funding, or other program benefits secured to the eligible schools and libraries that are members of the consortium.

(2) For consortia, discounts under this subpart shall apply only to the portion of eligible services and equipment used by eligible schools and libraries.

(3) Service providers shall keep and retain records of rates charged to and discounts allowed for eligible schools and libraries on their own or as part of a consortium. Such records shall be available for public inspection.

§ 54.2003 Eligible Services and Equipment.

(a) *Supported services and equipment*. All supported services and equipment are identified in the Schools and Libraries Cybersecurity Pilot Program Eligible Services List. The services and equipment in this subpart will be supported in addition to all reasonable charges that are incurred by taking such services, such as state and federal taxes. Charges for termination liability, penalty surcharges, and other charges not included in the cost of taking such service shall not be covered by universal service support.

(b) *Prohibition on resale*. Eligible supported services and equipment shall not be sold, resold, or transferred in consideration of money or any other thing of value, until the conclusion of the Schools and Libraries Cybersecurity Pilot Program, as provided in § 54.2001.

§ 54.2004 Application for Pilot Program Selection and Reporting of Information.

(a) The Wireline Competition Bureau shall announce the opening of the Pilot Participant Selection Application Window for applicants to submit a Pilot Participant Selection Application.

(b) The Wireline Competition Bureau shall announce those eligible applicants who have been selected to participate in the Schools and Libraries Cybersecurity Pilot Program following the close of the Pilot Participant Selection Application Window.

(c) *Filing the FCC Form 484 to be considered for selection in the Pilot Program*.

(1) Schools, libraries, or consortia of eligible schools and libraries to be considered for participation in the Schools and Libraries Cybersecurity Pilot Program shall submit the first part of an FCC Form 484 to the Administrator, via a portal established by the Administrator, that contains, at a minimum, the following information:

(i) Name, entity number, FCC registration number, employer identification number, addresses, and telephone number for each school, library, and consortium member that will participate in the proposed Pilot project, including the identity of the lead site for any proposals involving a consortium.

(ii) Contact information for the individual(s) who will be responsible for the management and operation of the proposed Pilot project, including name, title or position, telephone number, mailing address, and email address.

(iii) Applicant number and entity type(s), including Tribal information, if applicable, and current E-Rate participation status and discount percentage, if applicable.

(iv) A broad description of the proposed Pilot project, including a description of the applicant's goals and objectives for the proposed Pilot project, a description of how Pilot funding will be used for the proposed project, and the cybersecurity risks the proposed Pilot project will prevent or address.

(v) The cybersecurity equipment and services the applicant plans to request as part of its proposed project, the ability of the project to be self-sustaining once established, and whether the applicant has a cybersecurity officer or other senior-level staff member designated to be the cybersecurity officer for its Pilot project.

(vi) Whether the applicant has previous experience implementing cybersecurity protections or measures, how many years of prior experience the applicant has, whether the applicant has experienced a cybersecurity incident within a year of the date of its application, and information about the applicant's participation or planned participation in cybersecurity collaboration and/or information-sharing groups.

(vii) Whether the applicant has implemented, or begun implementing, any U.S. Department of Education or Cybersecurity and Infrastructure Security Agency recommendations, a description of any U.S. Department of Education or Cybersecurity and Infrastructure Security Agency free or low-cost cybersecurity resources that an applicant currently utilizes or plans to utilize, or an explanation of what is preventing an applicant from utilizing these available resources.

(viii) An estimate of the total costs for the proposed Pilot project, information about how the applicant will cover the non-discount share of costs for the Pilot-eligible services, and information about other cybersecurity funding the applicant receives, or expects to receive, from other federal, state, local, or Tribal programs or sources.

(ix) Whether any of the non-cybersecurity services and equipment the applicant proposes to purchase with Pilot funding will capture data on cybersecurity threats and attacks, free or low-cost cybersecurity resources that service providers will be required to include in their bids, and whether the applicant will require its selected service provider(s) to capture and measure cost-effectiveness and cyber awareness/readiness data.

(x) A description of the applicant's proposed metrics for the Pilot project, how they align with the applicant's cybersecurity goals, how those metrics will be collected, and whether the applicant is prepared to share and report its cybersecurity metrics as part of the Pilot Program.

(2) The first part of the FCC Form 484 shall be signed by a person authorized to submit the application to participate in the Schools and Libraries Cybersecurity Pilot Program on behalf of the eligible school, library, or consortium including such entities.

(i) A person authorized to submit the first part of the FCC Form 484 application on behalf of the entities listed on an FCC Form 484 shall certify under oath that:

(A) "I am authorized to submit this application on behalf of the above-named applicant and that based on information known to me or provided to me by employees responsible for the data being submitted, I hereby certify that the data set forth in this form has been examined and is true, accurate, and complete. I acknowledge that any false statement on this application or on other documents submitted by this applicant can be punished by fine or forfeiture under the Communications Act (47 U.S.C. §§ 502, 503(b)), or fine or imprisonment under Title 18 of the United States Code (18 U.S.C. § 1001), or can lead to liability under the False Claims Act (31 U.S.C. §§ 3729–3733)."

(B) "In addition to the foregoing, this applicant is in compliance with the rules and orders governing the Schools and Libraries Cybersecurity Pilot Program, and I acknowledge that failure to be in compliance and remain in compliance with those rules and orders may result in the denial of funding, cancellation of funding commitments, and/or recoupment of past disbursements. I acknowledge that failure to comply with the rules and orders governing the Schools and Libraries Cybersecurity Pilot Program could result in civil or criminal prosecution by law enforcement authorities."

(C) "By signing this application, I certify that the information contained in this form is true, complete, and accurate, and the projected expenditures, disbursements, and cash receipts are for the purposes and objectives set forth in the terms and conditions of the Federal award. I am aware that any false, fictitious, or fraudulent information, or the omission of any material fact, may subject me to criminal, civil, or administrative penalties for fraud, false statements, false claims, or otherwise. (U.S. Code Title 18, §§ 1001, 286–287, and 1341, and Title 31, §§ 3729–3730 and 3801–3812)."

(D) The applicant recognizes that it may be audited pursuant to its application, that it will retain for ten years any and all records related to its application, and that, if audited, it shall produce such records at the request of any representative (including any auditor) appointed by a state education department, the Administrator, the Commission and its Office of Inspector General, or any local, state, or federal agency with jurisdiction over the entity.

(E) I certify and acknowledge, under penalty of perjury, that if selected, the schools, libraries, and consortia in the application will comply with all applicable Schools and Libraries Cybersecurity Pilot Program rules, requirements, and procedures, including the competitive bidding rules and the requirement to pay the required share of the costs for the supported items from eligible sources.

(F) I certify under penalty of perjury, to the best of my knowledge, that the schools, libraries, and consortia listed in the application are not already receiving or expecting to receive other funding (from any source, federal, state, Tribal, local, private, or other) that will pay for the same equipment and/or services, or the same portion of the equipment and/or services, for which I am seeking funding under the Schools and Libraries Cybersecurity Pilot Program.

(G) I certify under penalty of perjury, to the best of my knowledge, that all requested equipment and services funded by the Schools and Libraries Cybersecurity Pilot Program will be used for their intended purposes.

(d) *Filing the FCC Form 484 once selected to be in the Pilot Program*.

(1) Schools, libraries, or consortia of eligible schools and libraries selected for participation in the Schools and Libraries Cybersecurity Pilot Program shall submit to the Administrator, via a portal established by the Administrator, a second part to the FCC Form 484 that contains, at a minimum, the following information, as applicable:

(i) Information about correcting known security flaws and conducting routine backups, developing and exercising a cyber incident response plan, and any cybersecurity changes or advancements the participant plans to make outside of the Pilot-funded services and equipment.

(ii) A description of the participant's current cybersecurity posture, including how the school or library is currently managing and addressing its current cybersecurity risks through prevention and mitigation tactics.

(iii) Information about a participant's planned use(s) for other federal, state, or local cybersecurity funding (i.e., funding obtained outside of the Pilot).

(iv) Information about a participant's history of cyber threats and attacks within a year of the date of its application; the date range of the incident, a description of the unauthorized access; a description of the impact to the school or library, a description of the vulnerabilities exploited and the techniques used to access the system, and identifying information for each actor responsible for the incident, if known.

(v) A description of the specific U.S. Department of Education or Cybersecurity and Infrastructure Security Agency recommendations that the participant has implemented or begun to implement.

(vi) Information about a participant's current cybersecurity training policies and procedures, such as the frequency with which a participant trains its school and library staff and, separately, information about student cyber training sessions, and participation rates.

(vii) Information about any non-monetary or other challenges a participant may be facing in developing a more robust cybersecurity posture.

(2) The second part of the FCC Form 484 shall be signed by a person authorized to submit the second part as a participant in the Schools and Libraries Cybersecurity Pilot Program on behalf of the eligible school, library, or consortium including such entities.

(i) A person authorized to submit the second part of the FCC Form 484 application on behalf of the Pilot participants listed on an FCC Form 484 shall certify under oath that:

(A) "I am authorized to submit this application on behalf of the above-named participant and based on information known to me or provided to me by employees responsible for the data being submitted, I hereby certify that the data set forth in this form has been examined and is true, accurate, and complete. I acknowledge that any false statement on this application or on other documents submitted by this participant can be punished by fine or forfeiture under the Communications Act (47 U.S.C. §§ 502, 503(b)), or fine or imprisonment under Title 18 of the United States Code (18 U.S.C. § 1001), or can lead to liability under the False Claims Act (31 U.S.C. §§ 3729–3733)."

(B) "In addition to the foregoing, this participant is in compliance with the rules and orders governing the Schools and Libraries Cybersecurity Pilot Program, and I acknowledge that failure to be in compliance and remain in compliance with those rules and orders may result in the denial of funding, cancellation of funding commitments, and/or recoupment of past disbursements. I acknowledge that failure to comply with the rules and orders governing the Schools and Libraries Cybersecurity Pilot Program could result in civil or criminal prosecution by law enforcement authorities."

(C) "By signing this application, I certify that the information contained in this form is true, complete, and accurate, and the projected expenditures, disbursements, and cash receipts are for the purposes and objectives set forth in the terms and conditions of the Federal award. I am aware that any false, fictitious, or fraudulent information, or the omission of any material fact, may subject me to criminal, civil, or administrative penalties for fraud, false statements, false claims, or otherwise. (U.S. Code Title 18, §§ 1001, 286–287, and 1341, and Title 31, §§ 3729–3730 and 3801–3812)."

(D) The participant recognizes that it may be audited pursuant to its application, that it will retain for ten years any and all records

related to its application, and that, if audited, it shall produce such records at the request of any representative (including any auditor) appointed by a state education department, the Administrator, the Commission and its Office of Inspector General, or any local, state, or federal agency with jurisdiction over the entity.

(E) I certify and acknowledge, under penalty of perjury, that if selected, the schools, libraries, and consortia in the application will comply with all applicable Schools and Libraries Cybersecurity Pilot Program rules, requirements, and procedures, including the competitive bidding rules and the requirement to pay the required share of the costs for the supported items from eligible sources.

(F) I certify under penalty of perjury, to the best of my knowledge, that the schools, libraries, and consortia listed in the application are not already receiving or expecting to receive other funding (from any source, federal, state, Tribal, local, private, or other) that will pay for the same equipment and/or services, or the same portion of the equipment and/or services, for which I am seeking funding under the Schools and Libraries Cybersecurity Pilot Program.

(G) I certify under penalty of perjury, to the best of my knowledge, that all requested equipment and services funded by the Schools and Libraries Cybersecurity Pilot Program will be used for their intended purposes.

(3) In order for a school, library, or consortia of eligible schools and libraries selected for participation in the Schools and Libraries Cybersecurity Pilot Program to retain its status as a Pilot participant and receive Pilot Program support, it will be required to submit the information required by the second part of the FCC Form 484 in the form specified by the Wireline Competition Bureau.

(4) The Wireline Competition Bureau may waive, reduce, modify, or eliminate from the second part of the FCC Form 484, information requirements that prove unnecessary for the sound and efficient administration of the Pilot.

(5) Failure to submit the information required by the second part of the FCC Form 484 may result in removal as a participant in the Pilot Program and/or a referral to the Enforcement Bureau.

(e) *Data reporting requirements for participants*.

(1) In order for a Pilot participant to receive and continue receiving Pilot Program support and retain its status as a Pilot participant, it will be required to submit initial and annual reports, followed by a final report at the completion of the program with the information and in the form specified by the Wireline Competition Bureau.

(2) Prior to the start of the Pilot Program, the Wireline Competition Bureau shall announce the timing and form of the initial, annual, and final reports that Pilot participants must submit.

(3) The Wireline Competition Bureau may waive, reduce, modify, or eliminate Pilot

participant reporting requirements that prove unnecessary and require additional reporting requirements that the Bureau deems necessary to the sound and efficient administration of the Pilot.

(4) Failure to submit initial, annual, and final reports may result in a referral to the Enforcement Bureau, a hold on future disbursements, recission of committed funds, and/or recovery of disbursed funds.

§ 54.2005 Competitive Bidding Requirements.

(a) All participants in the Schools and Libraries Cybersecurity Pilot Program must conduct a fair and open competitive bidding process, consistent with all requirements set forth in this subpart.

(b) *Competitive bid requirements*. All participants in the Schools and Libraries Cybersecurity Pilot Program shall seek competitive bids, pursuant to the requirements established in this subpart, for all services and equipment eligible for support under § 54.2003. These competitive bidding requirements apply in addition to any applicable state, Tribal, and local competitive bidding requirements and are not intended to preempt such state, Tribal, or local requirements.

(c) *Posting of FCC Form 470.*

(1) Participants in the Schools and Libraries Cybersecurity Pilot Program shall submit a completed FCC Form 470 to the Administrator to initiate the competitive bidding process. The FCC Form 470 shall include, at a minimum, the following information:

(i) A list of specified services and/or equipment for which the school, library, or consortium requests bids;

(ii) Sufficient information to enable bidders to reasonably determine the needs of the applicant;

(2) The FCC Form 470 shall be signed by a person authorized to request bids for eligible services and equipment for the eligible school, library, or consortium, including such entities, and shall include that person's certification under penalty of perjury that:

(i) "I am authorized to submit this application on behalf of the above-named participant in the Schools and Libraries Cybersecurity Pilot Program and based on information known to me or provided to me by employees responsible for the data being submitted, I hereby certify that the data set forth in this form has been examined and is true, accurate, and complete. I acknowledge that any false statement on this application or on other documents submitted by this participant can be punished by fine or forfeiture under the Communications Act (47 U.S.C. §§ 502, 503(b)), or fine or imprisonment under Title 18 of the United States Code (18 U.S.C. § 1001), or can lead to liability under the False Claims Act (31 U.S.C. §§ 3729–3733)."

(ii) "In addition to the foregoing, this participant is in compliance with the rules and orders governing the Schools and Libraries Cybersecurity Pilot Program, and I acknowledge that failure to be in compliance and remain in compliance with those rules and orders may result in the denial of

funding, cancellation of funding commitments, and/or recoupment of past disbursements. I acknowledge that failure to comply with the rules and orders governing the Schools and Libraries Cybersecurity Pilot Program could result in civil or criminal prosecution by law enforcement authorities."

(iii) "By signing this application, I certify that the information contained in this form is true, complete, and accurate. I am aware that any false, fictitious, or fraudulent information, or the omission of any material fact, may subject me to criminal, civil or administrative penalties for fraud, false statements, false claims or otherwise. (U.S. Code Title 18, §§ 1001, 286–287, and 1341 and Title 31, §§ 3729–3730 and 3801–3812)."

(iv) The schools meet the statutory definition of "elementary school" or "secondary school" as defined in § 54.2000, do not operate as for-profit businesses, and do not have endowments exceeding $50 million.

(v) Libraries or library consortia eligible for assistance from a State library administrative agency under the Library Services and Technology Act of 1996 do not operate as for-profit businesses and, except for the limited case of Tribal college or university libraries, have budgets that are completely separate from any school (including, but not limited to, elementary and secondary schools, colleges, and universities).

(vi) The services and/or equipment that the school, library, or consortium purchases at discounts will not be sold, resold, or transferred in consideration for money or any other thing of value, except as allowed by § 54.2003(b).

(vii) The school(s) and/or library(ies) listed on this FCC Form 470 will not accept anything of value, other than services and equipment sought by means of this form, from the service provider, or any representatives or agent thereof or any consultant in connection with this request for services.

(viii) All bids submitted for eligible equipment and services will be carefully considered, with price being the primary factor, and the bid selected will be for the most cost-effective service offering consistent with paragraph (e) of this section.

(ix) The school, library, or consortium acknowledges that support under the Schools and Libraries Cybersecurity Pilot Program is conditional upon the school(s) and/or library(ies) securing access, separately or through this program, to all of the resources necessary to effectively use the requested equipment and services. The school, library, or consortium recognizes that some of the aforementioned resources are not eligible for support and certifies that it has considered what financial resources should be available to cover these costs.

(x) I will retain required documents for a period of at least 10 years (or whatever retention period is required by the rules in effect at the time of this certification) after the later of the last day of the applicable funding year or the service delivery deadline for the associated funding request. I

also certify that I will retain all documents necessary to demonstrate compliance with the statute (47 U.S.C. § 254) and Commission rules regarding the form for, receipt of, and delivery of equipment and services receiving Schools and Libraries Cybersecurity Pilot Program discounts. I acknowledge that I may be audited pursuant to participation in the Pilot Program.

(xi) I certify that the equipment and services that the participant purchases at discounts will be used primarily for educational purposes and will not be sold, resold, or transferred in consideration for money or any other thing of value, except as permitted by the Commission's rules at 47 C.F.R. § 54.2003(b). Additionally, I certify that the entity or entities listed on this form will not accept anything of value or a promise of anything of value, other than services and equipment sought by means of this form, from the service provider, or any representative or agent thereof or any consultant in connection with this request for services.

(xii) I acknowledge that support under this Pilot Program is conditional upon the school(s) and/or library(ies) I represent securing access, separately or through this program, to all of the resources necessary to effectively use the requested equipment and services. I recognize that some of the aforementioned resources are not eligible for support. I certify that I have considered what financial resources should be available to cover these costs.

(xiii) I certify that I have reviewed all applicable Commission, state, Tribal, and local procurement/competitive bidding requirements and that the participant will comply with all applicable requirements.

(3) The Administrator shall post each FCC Form 470 that it receives from a participant in the Schools and Libraries Cybersecurity Pilot Program on its Web site designated for this purpose.

(4) After posting on the Administrator's Web site an FCC Form 470, the Administrator shall send confirmation of the posting to the participant requesting services and/or equipment. The participant shall then wait at least four weeks from the date on which its description of services and/or equipment is posted on the Administrator's Web site before making commitments with the selected providers of services and/or equipment. The confirmation from the Administrator shall include the date after which the participant may sign a contract with its chosen provider(s).

(d) *Gift Restrictions*.

(1) Subject to paragraphs (d)(3) and (4) of this section, a participant in the Schools and Libraries Cybersecurity Pilot Program may not directly or indirectly solicit or accept any gift, gratuity, favor, entertainment, loan, or any other thing of value from a service provider participating in or seeking to participate in the Schools and Libraries Cybersecurity Pilot Program. No such service provider shall offer or provide any such gift, gratuity, favor, entertainment, loan, or other thing of value except as otherwise provided herein. Modest refreshments not offered as part of a meal, items with little intrinsic value intended solely for presentation, and items worth $20 or less, including meals, may be offered or provided, and

accepted by any individuals or entities subject to this rule, if the value of these items received by any individual does not exceed $50 from any one service provider per year. The $50 amount for any service provider shall be calculated as the aggregate value of all gifts provided during a year by the individuals specified in paragraph (d)(2)(ii) of this section.

(2) For purposes of this paragraph:

(i) The term "participant in the Schools and Libraries Cybersecurity Pilot Program" includes all individuals who are on the governing boards of such entities (such as members of a school committee), and all employees, officers, representatives, agents, consultants, or independent contractors of such entities involved on behalf of such school, library, or consortium with the Schools and Libraries Cybersecurity Pilot Program, including individuals who prepare, approve, sign, or submit applications, or other forms related to the Schools and Libraries Cybersecurity Pilot Program, or who prepare bids, communicate, or work with Schools and Libraries Cybersecurity Pilot Program service providers, Schools and Libraries Cybersecurity Pilot Program consultants, or with the Administrator, as well as any staff of such entities responsible for monitoring compliance with the Schools and Libraries Cybersecurity Pilot Program; and

(ii) The term "service provider" includes all individuals who are on the governing boards of such an entity (such as members of the board of directors), and all employees, officers, representatives, agents, consultants, or independent contractors of such entities.

(3) The restrictions set forth in this paragraph shall not be applicable to the provision of any gift, gratuity, favor, entertainment, loan, or any other thing of value, to the extent given to a family member or a friend working for an eligible school, library, or consortium that includes an eligible school or library, provided that such transactions:

(i) Are motivated solely by a personal relationship,

(ii) Are not rooted in any service provider business activities or any other business relationship with any such participant in the Schools and Libraries Cybersecurity Pilot Program, and

(iii) Are provided using only the donor's personal funds that will not be reimbursed through any employment or business relationship.

(4) Any service provider may make charitable donations to a participant in the Schools and Libraries Cybersecurity Pilot Program in the support of its programs as long as such contributions are not directly or indirectly related to Schools and Libraries Cybersecurity Pilot Program procurement activities or decisions and are not given by service providers to circumvent competitive bidding and other Schools and Libraries Cybersecurity Pilot Program rules.

(e) *Selecting a provider of eligible services*. In selecting a provider of eligible services and equipment, participants in the Schools and Libraries Cybersecurity Pilot Program shall carefully consider all bids submitted and must select the most cost-effective service

offering. In determining which service offering is the most cost-effective, entities may consider relevant factors other than the pre-discount prices submitted by providers, but price should be the primary factor considered.

§ 54.2006 Requests for Funding.

(a) *Filing of the FCC Form 471.*

(1) A participant in the Schools and Libraries Cybersecurity Pilot Program shall, upon entering into a signed contract or other legally binding agreement for eligible services and/or equipment, submit a completed FCC Form 471 to the Administrator.

(2) The FCC Form 471 shall be signed by the person authorized to order eligible services or equipment for the participant in the Schools and Libraries Cybersecurity Pilot Program and shall include that person's certification under penalty of perjury that:

(i) "I am authorized to submit this application on behalf of the above-named participant and that based on information known to me or provided to me by employees responsible for the data being submitted, I hereby certify that the data set forth in this application has been examined and is true, accurate, and complete. I acknowledge that any false statement on this application or on other documents submitted by this participant can be punished by fine or forfeiture under the Communications Act (47 U.S.C. §§ 502, 503(b)), or fine or imprisonment under Title 18 of the United States Code (18 U.S.C. § 1001), or can lead to liability under the False Claims Act (31 U.S.C. §§ 3729–3733)."

(ii) "In addition to the foregoing, this participant is in compliance with the rules and orders governing the Schools and Libraries Cybersecurity Pilot Program, and I acknowledge that failure to be in compliance and remain in compliance with those rules and orders may result in the denial of funding, cancellation of funding commitments, and/or recoupment of past disbursements. I acknowledge that failure to comply with the rules and orders governing the Schools and Libraries Cybersecurity Pilot Program could result in civil or criminal prosecution by law enforcement authorities."

(iii) "By signing this application, I certify that the information contained in this application is true, complete, and accurate, and the projected expenditures, disbursements and cash receipts are for the purposes and objectives set forth in the terms and conditions of the federal award. I am aware that any false, fictitious, or fraudulent information, or the omission of any material fact, may subject me to criminal, civil or administrative penalties for fraud, false statements, false claims or otherwise. (U.S. Code Title 18, §§ 1001, 286–287, and 1341 and Title 31, §§ 3729–3730 and 3801–3812)."

(iv) The school meets the statutory definition of "elementary school" or "secondary school" as defined in § 54.2000, does not operate as for-profit businesses, and does not have endowments exceeding $50 million.

(v) The library or library consortia is eligible for assistance from a State library administrative agency under the Library Services and Technology Act, does not operate as for-profit businesses and, except for the limited case of Tribal college and university libraries, have budgets that are completely separate from any school (including, but not limited to, elementary and secondary schools, colleges, and universities).

(vi) The school, library, or consortium listed on the FCC Form 471 application will pay the non-discount portion of the costs of the eligible services and/or equipment to the Service Provider(s).

(vii) The school, library, or consortium listed on the FCC Form 471 application has conducted a fair and open competitive bidding process and has complied with all applicable state, Tribal, or local laws regarding procurement of the equipment and services for which support is being sought.

(viii) An FCC Form 470 was posted and that any related request for proposals (RFP) was made available for at least 28 days before considering all bids received and selecting a service provider. The school, library, or consortium listed on the FCC Form 471 application carefully considered all bids submitted and selected the most-cost-effective bid in accordance with § 54.2005(e), with price being the primary factor considered.

(ix) The school, library, or consortium listed on the FCC Form 471 application is only seeking support for eligible services and/or equipment.

(x) The school, library, or consortia is not seeking Schools and Libraries Cybersecurity Pilot Program support or reimbursement for eligible services and/or equipment that have been purchased and reimbursed in full with other federal, state, Tribal, or local funding, or are eligible for discounts from the schools and libraries universal service support mechanism or another universal service support mechanism.

(xi) The services and equipment the school, library, or consortium purchases using Schools and Libraries Cybersecurity Pilot Program support will be used primarily for educational purposes and will not be sold, resold, or transferred in consideration for money or any other thing of value, except as allowed by § 54.2003(b).

(xii) The school, library, or consortium will create and maintain an equipment and service inventory as required by § 54.2010(a).

(xiii) The school, library, or consortium has complied with all program rules and acknowledges that failure to do so may result in denial of funding and/or recovery of funding.

(xiv) The school, library, or consortium acknowledges that it may be audited pursuant to its application, that it will retain for ten years any and all records related to its application, and that, if audited, it shall produce such records at the request of any representative (including any auditor) appointed by a state education department, the Administrator, the

Commission and its Office of Inspector General, or any local, state, or federal agency with jurisdiction over the entity.

(xv) No kickbacks, as defined in 41 U.S.C. § 8701, were paid to or received by the participant from anyone in connection with the Schools and Libraries Cybersecurity Pilot Program or the schools and libraries universal service support mechanism.

(xvi) The school, library, or consortium acknowledges that Commission rules provide that persons who have been convicted of criminal violations or held civilly liable for certain acts arising from their participation in the universal service support mechanisms are subject to suspension and debarment from the program. The school, library, or consortium will institute reasonable measures to be informed, and will notify the Administrator should it be informed or become aware that any of the entities listed on this application, or any person associated in any way with this entity and/or the entities listed on this application, is convicted of a criminal violation or held civilly liable for acts arising from their participation in the universal service support mechanisms.

(b) *Service or Equipment Substitution.*

(1) A request by a Schools and Libraries Cybersecurity Pilot Program participant to substitute a service or piece of equipment for one identified in its FCC Form 471 must be in writing and certified under penalty of perjury by an authorized person.

(2) The Administrator shall approve such written request where:

(i) The service or equipment has the same functionality;

(ii) The substitution does not violate any contract provisions or state, Tribal, or local procurement laws; and

(iii) The Schools and Libraries Cybersecurity Pilot Program participant certifies that the requested change is within the scope of the controlling FCC Form 470.

(3) In the event that a service or equipment substitution results in a change in the pre-discount price for the supported service or equipment, support shall be based on the lower of either the pre-discount price of the service or equipment for which support was originally requested or the pre-discount price of the new, substituted service or equipment after the Administrator has approved a written request for the substitution.

(c) *Mixed eligibility services and equipment*. A request for discounts for services or equipment that includes both eligible and ineligible components must remove the cost of the ineligible components of the service or equipment from the request for funding submitted to the Administrator.

(d) *Application Filing Window*. The Wireline Competition Bureau will announce the opening of the Pilot Participant Selection Application Window for participants to submit FCC Form 471 applications. The filing period shall begin and conclude on dates to the

determined by the Wireline Competition Bureau. The Wireline Competition Bureau may implement additional filing periods as it deems necessary.

§ 54.2007 Discounts.

(a) *Discount mechanism*. Discounts for participants in the Schools and Libraries Cybersecurity Pilot Program shall be set as a percentage discount from the pre-discount price.

(b) *Discount percentages*. The discounts available to participants in the Schools and Libraries Cybersecurity Pilot Program shall range from 20 percent to 90 percent of the pre-discount price for all eligible services provided by eligible providers. The discounts available shall be determined by indicators of poverty and urban/rurality designation.

(1) For schools and school districts, the level of poverty shall be based on the percentage of the student enrollment that is eligible for a free or reduced price lunch under the National School Lunch Program or a federally-approved alternative mechanism. School districts shall divide the total number of students eligible for the National School Lunch Program within the school district by the total number of students within the school district to arrive at a percentage of students eligible. This percentage rate shall then be applied to the discount matrix to set a discount rate for the supported services purchased by all schools within the school district. Independent charter schools, private schools, and other eligible educational facilities should calculate a single discount percentage rate based on the total number of students under the control of the central administrative agency.

(2) For libraries and library consortia, the level of poverty shall be based on the percentage of the student enrollment that is eligible for a free or reduced price lunch under the National School Lunch Program or a federally-approved alternative mechanism in the public school district in which they are located and should use that school district's level of poverty to determine their discount rate when applying as a library system or as an individual library outlet within that system. When a library system has branches or outlets in more than one public school district, that library system and all library outlets within that system should use the address of the central outlet or main administrative office to determine which school district the library system is in, and should use that school district's level of poverty to determine its discount rate when applying as a library system or as one or more library outlets. If the library is not in a school district, then its level of poverty shall be based on an average of the percentage of students eligible for the National School Lunch Program in each of the school districts that children living in the library's location attend.

(3) The Administrator shall classify schools and libraries as “urban” or “rural” according to the following designations. The Administrator shall designate a school or library as “urban” if the school or library is located in an urbanized area or urban cluster area with a population equal to or greater than 25,000, as determined by the most recent rural-urban classification by the Bureau of the Census. The Administrator shall designate all other schools and libraries as “rural.”

(4) Participants in the Schools and Libraries Cybersecurity Pilot Program shall calculate discounts on supported services described in § 54.2003 that are shared by two or more of their schools, libraries, or consortia members by calculating an

average discount based on the applicable district-wide discounts of all member schools and libraries. School districts, library systems, or other billed entities shall ensure that, for each year in which an eligible school or library is included for purposes of calculating the aggregate discount rate, that eligible school or library shall receive a proportionate share of the shared services for which support is sought. For schools, the discount shall be a simple average of the applicable district-wide percentage for all schools sharing a portion of the shared services. For libraries, the average discount shall be a simple average of the applicable discounts to which the libraries sharing a portion of the shared services are entitled.

(c) *Discount matrix*. The Administrator shall use the following matrix to set the discount rate to be applied to eligible services purchased by participants in the Schools and Libraries Cybersecurity Pilot Program based on the participant's level of poverty and location in an "urban" or "rural" area.

	Discount Level	
% of students eligible for National School Lunch Program	Urban Discount	Rural Discount
< 1	20	25
1-19	40	50
20-34	50	60
35-49	60	70
50-74	80	80
75-100	90	90

(d) *Payment for the non-discount portion of supported services and equipment*. A participant in the Schools and Libraries Cybersecurity Pilot Program must pay the non-discount portion of costs for the services or equipment purchased with universal service discounts, and may not receive rebates for services or equipment purchased with universal service discounts. For the purpose of this rule, the provision, by the provider of a supported service or equipment, of free services or equipment unrelated to the supported service or equipment constitutes a rebate of the non-discount portion of the costs for the supported services and equipment.

§ 54.2008 Requests for Reimbursement.

(a) *Submission of request for reimbursement (FCC Form 472 or FCC Form 474)*. Consistent with the invoicing selection made by the Pilot participant, reimbursement for the costs associated with eligible services and equipment shall be provided directly to the participant, or its service provider(s), seeking reimbursement from the Schools and Libraries Cybersecurity Pilot Program upon submission and approval of a completed FCC Form 472 (Billed Entity Applicant Reimbursement Form) or a completed FCC Form 474 (Service Provider Invoice) to the Administrator.

(1) The FCC Form 472 shall be signed by the person authorized to submit requests for reimbursement for the eligible school, library, or consortium and shall include that person's certification under penalty of perjury that:

(i) "I am authorized to submit this request for reimbursement on behalf of the above-named school, library or consortium and that based on information known to me or provided to me by employees responsible for the data being submitted, I hereby certify that the data set forth in this

request for reimbursement has been examined and is true, accurate, and complete. I acknowledge that any false statement on this request for reimbursement or on other documents submitted by this school, library, or consortium can be punished by fine or forfeiture under the Communications Act (47 U.S.C. §§ 502, 503(b)), or fine or imprisonment under Title 18 of the United States Code (18 U.S.C. § 1001), or can lead to liability under the False Claims Act (31 U.S.C. §§ 3729–3733)."

(ii) "In addition to the foregoing, the school, library, or consortium is in compliance with the rules and orders governing the Schools and Libraries Cybersecurity Pilot Program, and I acknowledge that failure to be in compliance and remain in compliance with those rules and orders may result in the denial of funding, cancellation of funding commitments, and/or recoupment of past disbursements. I acknowledge that failure to comply with the rules and orders governing the Schools and Libraries Cybersecurity Pilot Program could result in civil or criminal prosecution by law enforcement authorities."

(iii) "By signing this request for reimbursement, I certify that the information contained in this request for reimbursement is true, complete, and accurate, and the expenditures, disbursements and cash receipts are for the purposes and objectives set forth in the terms and conditions of the federal award. I am aware that any false, fictitious, or fraudulent information, or the omission of any material fact, may subject me to criminal, civil or administrative penalties for fraud, false statements, false claims or otherwise. (U.S. Code Title 18, sections §§ 1001, 286–287, and 1341 and Title 31, §§ 3729–3730 and 3801–3812)."

(iv) The funds sought in the request for reimbursement are for eligible services and/or equipment that were purchased in accordance with the Schools and Libraries Cybersecurity Pilot Program rules and requirements in this subpart and received by the school, library, or consortium. The equipment and/or services being requested for reimbursement were determined to be eligible and approved by the Administrator.

(v) The non-discounted share of costs amount(s) were billed by the Service Provider and paid for by the Billed Entity Applicant on behalf of the eligible schools, libraries, and consortia of those entities.

(vi) The school, library, or consortium is not seeking Schools and Libraries Cybersecurity Pilot Program reimbursement for eligible services and/or equipment that have been purchased and reimbursed in full with other federal, state, Tribal, or local funding or are eligible for discounts from the schools and libraries universal service support mechanism or other universal service support mechanisms.

(vii) The school, library, or consortium acknowledges that it must submit invoices detailing the items purchased along with the submission of its request for reimbursement as required by § 54.2008(b).

(viii) The equipment and/or services the school, library, or consortium purchased will not be sold, resold, or transferred in consideration for money or any other thing of value, except as allowed by § 54.2003(b).

(ix) The school, library, or consortium acknowledges that it may be subject to an audit, inspection, or investigation pursuant to its request for reimbursement, that it will retain for ten years any and all records related to its request for reimbursement, and will make such records and equipment purchased with Schools and Libraries Cybersecurity Pilot Program reimbursement available at the request of any representative (including any auditor) appointed by a state education department, the Administrator, the Commission and its Office of Inspector General, or any local, state, or federal agency with jurisdiction over the entity.

(x) No kickbacks, as defined in 41 U.S.C. § 8701, were paid to or received by the participant from anyone in connection with the Schools and Libraries Cybersecurity Pilot Program or the schools and libraries universal service support mechanism.

(xi) The school, library, or consortium acknowledges that Commission rules provide that persons who have been convicted of criminal violations or held civilly liable for certain acts arising from their participation in the universal service support mechanisms are subject to suspension and debarment from the program. The school, library, or consortium will institute reasonable measures to be informed, and will notify the Administrator should it be informed or become aware that any of the entities listed on this application, or any person associated in any way with this entity and/or the entities listed on this application, is convicted of a criminal violation or held civilly liable for acts arising from their participation in the universal service support mechanisms.

(xii) No universal service support has been or will be used to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by any company designated by the Federal Communications Commission as posing a national security threat to the integrity of communications networks or the communications supply chain since the effective date of the designations.

(xiii) No federal subsidy made available through a program administered by the Commission that provides funds to be used for the capital expenditures necessary for the provision of advanced communications services has been or will be used to purchase, rent, lease, or otherwise obtain, any covered communications equipment or service, or maintain, any covered communications equipment or service, or maintain any covered communications equipment or service previously purchased, rented, leased, or otherwise obtained, as required by § 54.10.

(2) The FCC Form 474 shall be signed by the person authorized to submit requests for reimbursement for the service provider and shall include that person's certification under penalty of perjury that:

(i) "I am authorized to submit this request for reimbursement on behalf of the above-named Service Provider and that based on information known

to me or provided to me by employees responsible for the data being submitted, I hereby certify that the data set forth in this request for reimbursement has been examined and is true, accurate and complete. I acknowledge that any false statement on this request for reimbursement or on other documents submitted by this Service Provider can be punished by fine or forfeiture under the Communications Act (47 U.S.C. §§ 502, 503(b)), or fine or imprisonment under Title 18 of the United States Code (18 U.S.C. § 1001), or can lead to liability under the False Claims Act (31 U.S.C. §§ 3729–3733)."

(ii) "In addition to the foregoing, the Service Provider is in compliance with the rules and orders governing the Schools and Libraries Cybersecurity Pilot Program, and I acknowledge that failure to be in compliance and remain in compliance with those rules and orders may result in the denial of funding, cancellation of funding commitments, and/or recoupment of past disbursements. I acknowledge that failure to comply with the rules and orders governing the Schools and Libraries Cybersecurity Pilot Program could result in civil or criminal prosecution by law enforcement authorities."

(iii) "By signing this request for reimbursement, I certify that the information contained in this request for reimbursement is true, complete, and accurate, and the expenditures, disbursements and cash receipts are for the purposes and objectives set forth in the terms and conditions of the federal award. I am aware that any false, fictitious, or fraudulent information, or the omission of any material fact, may subject me to criminal, civil or administrative penalties for fraud, false statements, false claims or otherwise. (U.S. Code Title 18, §§ 1001, 286–287, and 1341 and Title 31, §§ 3729–3730 and 3801–3812)."

(iv) The funds sought in the request for reimbursement are for eligible services and/or equipment that were purchased in accordance with the Schools and Libraries Cybersecurity Pilot Program rules and requirements in this subpart and received by the school, library, or consortium.

(v) The Service Provider is not seeking Schools and Libraries Cybersecurity Pilot Program reimbursement for eligible equipment and/or services for which it has already been paid.

(vi) The Service Provider certifies that the school's, library's, or consortium's non-discount portion of costs for the eligible equipment and services has not been waived, paid, or promised to be paid by this Service Provider. The Service Provider acknowledges that the provision of a supported service or free services or equipment unrelated to the supported equipment or services constitutes a rebate of the non-discount portion of the costs as stated in § 54.2007(d).

(vii) The Service Provider acknowledges that it must submit invoices detailing the items purchased along with the submission of its request for reimbursement as required by § 54.2008(b).

(viii) The Service Provider certifies that it is compliant with the Commission's

rules and orders regarding gifts and this Service Provider has not directly or indirectly offered or provided any gifts, gratuities, favors, entertainment, loans, or any other thing of value to any eligible school, library, or consortium, except as provided for at § 54.2005(d).

(ix) The Service Provider acknowledges that it may be subject to an audit, inspection, or investigation pursuant to its request for reimbursement, that it will retain for ten years any and all records related to its request for reimbursement, and will make such records and equipment purchased with Schools and Libraries Cybersecurity Pilot Program reimbursement available at the request of any representative (including any auditor) appointed by a state education department, the Administrator, the Commission and its Office of Inspector General, or any local, state, or federal agency with jurisdiction over the entity.

(x) No kickbacks, as defined in 41 U.S.C. § 8701, were paid by the Service Provider to anyone in connection with the Schools and Libraries Cybersecurity Pilot Program or the schools and libraries universal service support mechanism.

(xi) The Service Provider is not debarred or suspended from any Federal programs, including the universal service support mechanisms.

(xii) No universal service support has been or will be used to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by any company designated by the Federal Communications Commission as posing a national security threat to the integrity of communications networks or the communications supply chain since the effective date of the designations.

(xiii) No federal subsidy made available through a program administered by the Commission that provides funds to be used for the capital expenditures necessary for the provision of advanced communications services has been or will be used to purchase, rent, lease, or otherwise obtain, any covered communications equipment or service, or maintain any covered communications equipment or service, or maintain any covered communications equipment or service previously purchased, rented, leased, or otherwise obtained, as required by § 54.10.

(b) *Required documentation*. Along with the submission of a completed FCC Form 472 or a completed FCC Form 474, a participant, or service provider, seeking reimbursement from the Schools and Libraries Cybersecurity Pilot Program must submit invoices detailing the items purchased to the Administrator at the time the FCC Form 472 or FCC Form 474 is submitted.

(c) *Reimbursement and invoice processing*. The Administrator shall accept and review requests for reimbursement and invoices subject to the invoice filing deadlines provided in paragraph (d) of this section.

(d) *Invoice filing deadline*. Invoices must be submitted to the Administrator within ninety (90) days after the last date to receive service, in accordance with § 54.2001.

(e) *Invoice deadline extensions*. In advance of the deadline calculated pursuant to paragraph (d) of this section, billed entities or service providers may request a one-time extension of the invoice filing deadline. The Administrator shall grant a ninety (90) day extension of the invoice filing deadline, if the request is timely filed.

(f) *Choice of payment method*. Service providers providing discounted services under this subpart shall, prior to the submission of the FCC Form 471, permit the Schools and Libraries Cybersecurity Pilot Program participant to choose the method of payment for the discounted services from those methods offered by the Administrator, including making a full undiscounted payment and receiving subsequent reimbursement of the discount amount from the Administrator.

§ 54.2009 Audits, Inspections, and Investigations.

(a) *Audits*. Schools and Libraries Cybersecurity Pilot Program participants and service providers shall be subject to audits and other investigations to evaluate their compliance with the statutory and regulatory requirements of the Schools and Libraries Cybersecurity Pilot Program, including those requirements pertaining to what services and equipment are purchased, what services and equipment are delivered, and how services and equipment are being used.

(b) *Inspections and investigations*. Schools and Libraries Cybersecurity Pilot Program participants and service providers shall permit any representative (including any auditor) appointed by a state education department, the Administrator, the Commission, its Office of Inspector General, or any local, state, or federal agency with jurisdiction over the entity to enter their premises to conduct inspections for compliance with the statutory and regulatory requirements in this subpart of the Schools and Libraries Cybersecurity Pilot Program.

§ 54.2010 Records Retention and Production.

(a) *Recordkeeping requirements*. All Schools and Libraries Cybersecurity Pilot Program participants and service providers shall retain all documents related to their participation in the program sufficient to demonstrate compliance with all program rules for at least ten years from the last date of service or delivery of equipment. All Schools and Libraries Cybersecurity Pilot Program applicants shall maintain asset and inventory records of services and equipment purchased sufficient to verify the actual location of such services and equipment for a period of ten years after purchase.

(b) *Production of records*. All Schools and Libraries Cybersecurity Pilot Program participants and service providers shall produce such records upon request of any representative (including any auditor) appointed by a state education department, the Administrator, the Commission, its Office of the Inspector General, or any local, state, or federal agency with jurisdiction over the entity.

§ 54.2011 Administrator of the Schools and Libraries Cybersecurity Pilot Program.

(a) The Universal Service Administrative Company is appointed the Administrator of the Schools and Libraries Cybersecurity Pilot Program and shall be responsible for administering the Schools and Libraries Cybersecurity Pilot Program.

(b) The Administrator shall be responsible for reviewing applications for funding, recommending funding commitments, issuing funding commitment decision letters,

reviewing invoices and recommending payment of funds, as well as other administration related duties.

(c) The Administrator may not make policy, interpret unclear provisions of statutes or rules, or interpret the intent of Congress. Where statutes or the Commission's rules in this subpart are unclear, or do not address a particular situation, the Administrator shall seek guidance from the Commission.

(d) The Administrator may advocate positions before the Commission and its staff only on administrative matters relating to the Schools and Libraries Cybersecurity Pilot Program.

(e) The Administrator shall create and maintain a website, as defined in § 54.5, on which applications for services will be posted on behalf of schools and libraries.

(f) The Administrator shall provide the Commission full access to the data collected pursuant to the administration of the Schools and Libraries Cybersecurity Pilot Program.

(g) The Administrator shall provide performance measurements pertaining to the Schools and Libraries Cybersecurity Pilot Program as requested by the Commission by order or otherwise.

(h) The Administrator shall have the authority to audit all entities reporting data to the Administrator regarding the Schools and Libraries Cybersecurity Pilot Program. When the Commission, the Administrator, or any independent auditor hired by the Commission or the Administrator conducts audits of the participants of the Schools and Libraries Cybersecurity Pilot Program, such audits shall be conducted in accordance with generally accepted government auditing standards.

(i) The Administrator shall establish procedures to verify support amounts provided by the Schools and Libraries Cybersecurity Pilot Program and may suspend or delay support amounts if a party fails to provide adequate verification of the support amounts provided upon reasonable request from the Administrator or the Commission.

(j) The Administrator shall make available to whomever the Commission directs, free of charge, any and all intellectual property, including, but not limited to, all records and information generated by or resulting from its role in administering the support mechanisms, if its participation in administering the Schools and Libraries Cybersecurity Pilot Program ends. If its participation in administering the Schools and Libraries Cybersecurity Pilot Program ends, the Administrator shall be subject to close-out audits at the end of its term.

§ 54.2012 Appeal and waiver requests.

(a) *Parties permitted to seek review of Administrator decision*.

(1) Any party aggrieved by an action taken by the Administrator must first seek review from the Administrator.

(2) Any party aggrieved by an action taken by the Administrator under paragraph (a)(1) of this section may seek review from the Federal Communications Commission as set forth in paragraph (b) of this section.

(3) Parties seeking waivers of the Commission's rules in this subpart shall seek relief directly from the Commission and need not first file an action for review from the Administrator under paragraph (a)(1) of this section.

(b) *Filing deadlines*.

(1) An affected party requesting review of a decision by the Administrator pursuant to paragraph (a)(1) of this section shall file such a request within thirty (30) days from the date the Administrator issues a decision.

(2) An affected party requesting review by the Commission pursuant to paragraph (a)(2) of this section of a decision by the Administrator under paragraph (a)(1) of this section shall file such a request with the Commission within thirty (30) days from the date of the Administrator's decision. Further, any party seeking a waiver of the Commission's rules under paragraph (a)(3) of this section shall file a request for such waiver within thirty (30) days from the date of the Administrator's initial decision, or, if an appeal is filed under paragraph (a)(1) of this section, within thirty days from the date of the Administrator's decision resolving such an appeal.

(3) Parties shall adhere to the time periods for filing oppositions and replies set forth in § 1.45 of this chapter.

(c) *General filing requirements*.

(1) Except as otherwise provided in this section, a request for review of an Administrator decision by the Commission shall be filed with the Commission's Office of the Secretary in accordance with the general requirements set forth in part 1 of this chapter. The request for review shall be captioned "In the Matter of Request for Review by (name of party seeking review) of Decision of Universal Service Administrator" and shall reference the applicable docket numbers.

(2) A request for review pursuant to paragraphs (a)(1) through (3) of this section shall contain:

(i) A statement setting forth the party's interest in the matter presented for review;

(ii) A full statement of relevant, material facts with supporting affidavits and documentation;

(iii) The question presented for review, with reference, where appropriate, to the relevant Commission rule, Commission order, or statutory provision; and;

(iv) A statement of the relief sought and the relevant statutory or regulatory provision pursuant to which such relief is sought.

(3) A copy of a request for review that is submitted to the Commission shall be served on the Administrator consistent with the requirement for service of documents set forth in § 1.47 of this chapter.

(4) If a request for review filed pursuant to paragraphs (a)(1) through (3) of this section alleges prohibitive conduct on the part of a third party, such request for review shall be served on the third party consistent with the requirement for service of documents set forth in § 1.47 of this chapter. The third party may file a response to the request for review. Any response filed by the third party shall adhere to the time period for filing replies set forth in § 1.45 of this chapter and the requirement for service of documents set forth in § 1.47 of this chapter.

(d) *Review by the Wireline Competition Bureau or the Commission*.

(1) Requests for review of Administrator decisions that are submitted to the Federal Communications Commission shall be considered and acted upon by the Wireline Competition Bureau; provided, however, that requests for review that raise novel questions of fact, law, or policy shall be considered by the full Commission.

(2) An affected party may seek review of a decision issued under delegated authority by the Wireline Competition Bureau pursuant to the rules set forth in part 1 of this chapter.

(e) *Standard of review*.

(1) The Wireline Competition Bureau shall conduct *de novo* review of requests for review of decisions issued by the Administrator.

(2) The Commission shall conduct *de novo* review of requests for review of decisions by the Administrator that involve novel questions of fact, law, or policy; provided, however, that the Commission shall not conduct *de novo* review of decisions issued by the Wireline Competition Bureau under delegated authority.

(f) *Schools and Libraries Cybersecurity Pilot Program disbursements during pendency of a request for review and Administrator decision*. When a party has sought review of an Administrator decision under paragraphs (a)(1) through (3) of this section, the Commission shall not process a request for the reimbursement of eligible equipment and/or services until a final decision has been issued either by the Administrator or by the Commission; provided, however, that the Commission may authorize disbursement of funds for any amount of support that is not the subject of an appeal.

§ 54.2013 Children's Internet Protection Act certifications

(a) *Definitions.*

(1) *School.* For the purposes of the certification requirements of this section, school means school, school board, school district, local education agency or other authority responsible for administration of a school.

(2) *Library.* For the purposes of the certification requirements of this section, library means library, library board or authority responsible for administration of a library.

(3) *Billed entity. Billed entity is defined in § 54.2000. In the case of a consortium,*

the billed entity is the lead member of the consortium.

(b) A school or library that receives support for eligible services and equipment through the Schools and Libraries Cybersecurity Pilot Program must make the certifications as described in paragraph (c) of this section.

(c) *Certifications required under 47 U.S.C. §§ 254(h) and (l).*

(1) A Schools and Libraries Cybersecurity Pilot Program participant need not complete additional Children's Internet Protection Act (CIPA) compliance certifications if the participant has already certified its CIPA compliance for the schools and libraries universal support mechanism funding year preceding the start of the Schools and Libraries Cybersecurity Pilot Program (*i.e.,* has certified its compliance in an FCC Form 486 or FCC Form 479).

(2) Schools and Libraries Cybersecurity Pilot Program participants that have not already certified their CIPA compliance for the schools and libraries universal service support mechanism funding year preceding the start of the Schools and Libraries Cybersecurity Pilot Program (*i.e.,* have not completed a FCC Form 486 or FCC Form 479), will be required to certify:

(i) That they are in compliance with CIPA requirements under sections 254(h) and (l);

(ii) That they are undertaking the actions necessary to comply with CIPA requirements under sections 254 (h) and (l) as part of their request for support through the Schools and Libraries Cybersecurity Pilot Program, and will come into compliance within one year from the date of the submission of its FCC Form 471; or

(iii) That they are not required to comply with CIPA requirements under sections 254(h) and (l) because they are purchasing services to be used only in conjunction with student-, school staff- or library patron-owned computers.

(d) *Failure to provide certifications.*

(1) *Schools and libraries*. A school or library that knowingly fails to submit certifications as required by this section shall not be eligible for support through the Schools and Libraries Cybersecurity Pilot Program until such certifications are submitted.

(2) *Consortia*. A billed entity's knowing failure to collect the required certifications from its eligible school and library members or knowing failure to certify that it collected the required certifications shall render the entire consortium ineligible for support through the Schools and Libraries Cybersecurity Pilot Program.

(3) *Reestablishing eligibility.* At any time, a school or library deemed ineligible for equipment and services under the Schools and Libraries Cybersecurity Pilot Program because of failure to submit certifications required by this section may reestablish eligibility for support by providing the required certifications to the Administrator and the Commission.

(e) *Failure to comply with the certifications.*

(1) *Schools and libraries.* A school or library that knowingly fails to comply with the certifications required by this section must reimburse any funds and support received under the Schools and Libraries Cybersecurity Pilot Program for the period in which there was noncompliance.

(2) *Consortia*. In the case of consortium applications, the eligibility for support of consortium members who comply with the certification requirements of this section shall not be affected by the failure of other school or library consortium members to comply with such requirements.

(3) *Reestablishing compliance*. At any time, a school or library deemed ineligible for support through the Schools and Libraries Cybersecurity Pilot Program for failure to comply with the certification requirements of this section and that has been directed to reimburse the program for support received during the period of noncompliance may reestablish compliance by complying with the certification requirements under this section. Upon submittal to the Commission of a certification, the school or library shall be eligible for support through the Schools and Libraries Cybersecurity Pilot Program.

(f) *Waivers based on state or local procurement rules and regulations and competitive bidding requirements*. Waivers shall be granted to schools and libraries when the authority responsible for making the certifications required by this section cannot make the required certifications because its state or local procurement rules or regulations or competitive bidding requirements prevent the making of the certification otherwise required. The waiver shall be granted upon the provision, by the authority responsible for making the certifications on behalf of schools or libraries, that the schools or libraries will be brought into compliance with the requirements of this section by one year from the date the waiver was granted.

APPENDIX B

Cybersecurity Pilot Program Eligible Services List

The Federal Communications Commission's (FCC) rules provide that all equipment and services that are eligible to receive discounts under the Schools and Libraries Cybersecurity Pilot Program (Pilot or Pilot Program) are listed in this Pilot Eligible Services List (P-ESL). 47 CFR § 54.2003. The Pilot Program is administered by the Universal Service Administrative Company (USAC). 47 CFR § 54.2011. Eligible schools and libraries that are selected for participation in the Pilot Program may seek support for eligible equipment and services as identified herein. 47 CFR §§ 54.2000 *et seq*.

Additional guidance from USAC about the Pilot Program application process and about eligible equipment and services, including a glossary of terms, is available on USAC's website at [link to be added]. The documents on USAC's website are not incorporated by reference into the P-ESL and do not bind the Commission. Thus, they will not be used to determine whether a service or product is eligible for Pilot Program support. Pilot participants and service providers may refer to those documents, but they should do so only for informal guidance.

Equipment and services that constitute a protection designed to improve or enhance the cybersecurity of a K-12 school, library, or consortia are eligible. A non-exhaustive list of four eligible technological categories and, for each category, a non-exhaustive list of eligible equipment and services, follows.

Advanced/Next-Generation Firewalls

Equipment and services that implement advanced/next-generation firewalls, including software-defined firewalls and Firewall as a Service, are eligible. Specifically, equipment, services, or a combination of equipment and services that limits access between networks, excluding basic firewalls that are funded through the Commission's E-Rate program, are eligible.

Eligible equipment and services may include the following features, substantially similar features, or their equivalents:

- Advanced Threat Detection and Prevention
- AI/ML Threat Detection and Response
- Application Awareness & Control
- Cloud-Delivered Threat Intelligence
- Comprehensive Network Visibility Software-defined Firewalls
- Deep Packet Inspection (DPI)
- Distributed-denial-of-service (DDoS) protection
- Firewall as a Service (FWaaS)
- Integrated Intrusion Prevention Systems (IPS)
- Internet of Things (IoT) Security
- Intrusion prevention/detection
- Malware Detection
- Network Segmentation
- Patch Management Systems
- Virtual Private Network (VPN)

Endpoint Protection

Equipment and services that implement endpoint protection are eligible. Specifically, equipment, services, or a combination of equipment and services that implements safeguards to protect school- and library-owned end-user devices, including desktops, laptops, and mobile devices, against cyber threats and attacks are eligible.

Eligible equipment and services may include the following features, substantially similar features or their equivalents:

- Anti-malware
- Anti-ransomware
- Anti-spam
- Anti-virus
- Endpoint Detection & Response (EDR)
- Extended Detection & Response (XDR)
- Insider and privilege misuse
- Privileged Access Management
- Secure Sockets Layer (SSL) inspections
- Target intrusions
- Web application hacking

Identity Protection and Authentication

Equipment and services that implement identity protection and authentication are eligible. Specifically, equipment, services, or a combination of equipment and services that implements safeguards to protect a user's network identity from theft or misuse and/or provide assurance about the network identity of an entity interacting with a system is eligible.

Eligible equipment and services may include the following features, substantially similar features, or their equivalents:

- Active Countermeasure Tools
- Cloud application protection
- Cloud Services
- Credential stuffing
- Content blocking and filtering/uniform resource locator (URL) filtering
- Content Caching Systems and Service
- Customer portal services
- Digital identity tools
- Distributed-denial-of-service (DDoS) protection
- Domain Name System (DNS)/DNS-layer security, blocking, and filtering
- Email and Web security
- Identity governance & technologies
- Intrusion Detection Systems (IDS)
- Logging practices / event logging
- Network access control
- Offsite/Immutable back-ups
- Mult-Factor Authentication (MFA)/phishing-resistant MFA
- Patching
- Password spraying
- Privileged identity management
- Secure Access Service Edge (SASE)
- Secure-By-Design equipment and services
- Security Information and Event Management (SIEM)
- Security Updates
- Single sign-on (SSO)
- Trusted Platform Module (TPM) and products with TPM chips

- Web Content Controls
- Wireless access controllers
- Zero Trust Architecture

Monitoring, Detection, and Response

Equipment and services that implement monitoring, detection and response are eligible. Specifically, equipment, services, or a combination of equipment and services that monitor and/or detect threats to a network and that take responsive action to remediate or otherwise address those threats is eligible.

Eligible equipment and services may include the following features, substantially similar features, or their equivalents:

- Bug bounty solutions & services
- Compliance assessment
- Dark web scanning
- Data Loss Prevention
- Internal/external vulnerability scanning
- Network/device monitoring & response
- Network Security Audit
- Network traffic analysis
- Managed detection & response (MDR)
- Managed Service Providers
- Maturity models
- Network Detection Response (NDR)
- Penetration testing
- Security Operations Center (SOC) for around the clock (24/7/365) monitoring, detection, and response
- Threat hunting/Updates and threat intelligence
- Vulnerability management

Notes:

- Certain technologies (e.g., DDoS protection) are listed in multiple categories above, reflecting the multiple ways they are categorized in the marketplace.
- Eligible costs include maintenance, operation and support charges, monthly charges, special construction, installation and activation charges, software, modulating electronics, and other equipment necessary to make eligible equipment and services functional. All eligible equipment and services and related costs, including maintenance and operation, must be competitively bid.
- A manufacturer's multi-year warranty for a period up to three years that is provided as an integral part of an eligible component, without a separately identifiable cost, may be included in the cost of the component.
- Eligibility is limited to equipment that is network-based (i.e., that excludes end-user devices, including, for example, tablets, smartphones, and laptops) and services that are network-based and/or locally installed on end-user devices, where the devices are owned or leased by the school or library, and where equipment and services are designed to identify and/or remediate threats that could otherwise directly impair or disrupt a school's or library's network, including to threats from users accessing the network remotely.
- Ineligible costs include:
    - Any equipment, service, or other related cost that is eligible in the Commission's E-Rate eligible services list program in the funding year for which Pilot reimbursement is sought.

- Any equipment, service, or other related cost for which a participant has already received reimbursement, or plans to apply for reimbursement, through any other USF or federal, state, or local program in the funding year for which Pilot reimbursement is sought.
- Staff salaries and labor costs for personnel of the participant or underlying beneficiary are not eligible.
- Consulting services that are not related to the installation and configuration of the eligible equipment and services are not eligible. These include services related to application assistance, program advice, and other activities not tied directly to actual installation and initial configuration of eligible equipment and services.
- Long-term planning and risk assessment surveys, including threat intelligence analysis and costs associated with incident response plans
- Security cameras, asset tracking tags, insurance costs, threat responses exercises, training, and any costs associated with responding to specific ransom demands are ineligible.
- Any equipment or services prohibited by the Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609) (Secure Networks Act) or the Commission's rules, including Commission rules 54.9 and 54.10, that implement the Secure Networks Act.

Training. Training is eligible as a part of installation of the equipment and services only if it is basic instruction on the use of eligible equipment and services, directly associated with equipment and services installation, and is part of the contract or agreement for the equipment and services. Training must occur coincidently or within a reasonable time after installation.

APPENDIX C

Cybersecurity NPRM Commenters and Reply Commenters

Comments

Commenter	Abbreviation
ActZero	
Alliance for Digital Innovation	ADI
American Library Association	ALA
Apptegy, Inc.	Apptegy
Center for Internet Security, Inc.	CIS
Cisco Systems, Inc.	Cisco
Clark County School District	CCSD
Clear Creek Amana CSD	Clear Creek
Consortium for School Networking, American Library Association, Schools, Health & Libraries Coalition, National Association of State Boards of Education, All4Ed, Pacific Northwest Gigapop, State Educational Technology Directors Association, Council of the Great City Schools, National School Board Association, Council of Chief State School Officers, Link Oregon, Common Sense	CoSN
Council of the Great City Schools	Council GCS
CrowdStrike	CrowdStrike
Crown Castle Fiber LLC	Crown Castle
Cybersecurity Coalition and Information Technology Industry Council	Cybersecurity Coalition/ITI
Dallas Independent School District	Dallas ISD
E-Rate Central on behalf of the New York State E-Rate Coordinator	E-Rate Central
Funds For Learning, LLC	FFL
Illinois Office of Broadband	IOB
Juniper Networks	JN
K12 Security Information eXchange	K12 SIX
K12 Tech Talk Podcast	K12 Tech Talk
K12TechPro	K12TechPro
Mendocino County Office of Education	MCOE
Michigan Statewide Educational Network Michigan Statewide Educational Technology Leaders, MiSecure Operations Center	MISEN
Microsoft Corporation	Microsoft
Northwestern Consolidated School District of Shelby County	Shelby County
NCTA – The Internet & Television Association	NCTA
Ohio Information Technology Centers	
Palo Alto Networks, Inc.	Palo Alto Networks
Robert Frisby	
Rubrik, Inc.	Rubrik
The Friday Institute for Education Innovation	Friday Institute
Tim Roemer/Global Market Innovators	GMI
Tribal Ready, PBC	Tribal Ready
Union County Public Schools	Union County
Questar III BOCES	Questar

Reply Comments

Commenter	Abbreviation
Allendale Public Schools	Allendale
American Library Association	ALA
Association of California School Administrators and the California School Boards Association	ACSA-CSBA Federal Partnership
ATARC Cybersecurity Higher Education and Workforce Development Working Group	ATARC
City of New York Office of Technology and Innovation	City of NY OTI
CTIA	
Electronic Privacy Information Center	EPIC
Extreme Networks	Extreme
Fortinet, Inc.	Fortinet
Funds For Learning, LLC	FFL
Internet2	
Learning Technology Center of Illinois	LTC
Lumen Technologies, Inc.	Lumen
National Education Organizations	EdGroup
State Associations Representing Public School Superintendents	ASE
State E-Rate Coordinators' Alliance	SECA
The Quilt	Quilt
Vector Resources Inc., d/b/a VectorUSA	Vector
Wayne RESA[1]	
Wilson School District[2]	Wilson
Wisconsin Department of Public Instruction	WI DPI
Zscaler, Inc.	Zscaler

[1] The following commenters filed reply comments using the same or a substantially similar form letter: Covenant Schools; Genesee Intermediate School District; Michigan Association for Computer Users in Learning (MACUL); Midland County Educational Service Agency; REMC Association of Michigan; St. Joseph County Intermediate School District et al.; Shiawassee Regional Education Service District.

[2] The following commenters filed reply comments using the same or a substantially similar form letter: Arizona Technology in Education Association – AzTEA; Kellog & Sovereign Consulting; Kiski Area School District (KASD); City of Woburn / Woburn Public Schools; Danvers Public Schools; EdTech Leaders Alliance- Ohio CoSN; Massachusetts Educational Technology Administrators Association (METAA); Nebraska Council of School Administrators (NCSA); NCTIES/NCCoSN; Twin Valley School District Technology Department (Twin Valley); California Association of School Business Officials.

APPENDIX D

Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] an Initial Regulatory Flexibility Analysis (IRFA) was incorporated in the *Schools and Libraries Cybersecurity Pilot Program Notice of Proposed Rulemaking* (*Cybersecurity NPRM*), released in November of 2023.[2] The Federal Communications Commission (Commission) sought written public comment on the proposals in the *Cybersecurity NPRM*, including comment on the IRFA. No comments were filed addressing the IRFA. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.[3]

A. Need for, and Objectives of, the Report and Order

2. The nation's K-12 schools and libraries increasing rely on remote, digital learning technologies to connect students, teachers, and library patrons to information, jobs, and other vital learning opportunities. This shift has increased the extent to which schools and libraries rely on networks to connect with student and patrons. This shift has also made school and library networks prime targets for cyber threats and attacks. When these attacks occur, they have the potential to disrupt school and library operations, resulting in a loss of learning, reductions in available bandwidth, significant monetary losses, and the potential for the leak and theft of personal information and confidential data associated with students, school staff and library patrons.

3. The nation's eligible schools, libraries, and consortia (comprised of eligible schools and libraries) may request universal service discounts for services and equipment to support their network connectivity, including telecommunications services, Internet access, and internal connections, through the Commission's E-Rate program. The E-Rate program was created by the Commission in 1997 in response to the Telecommunications Act of 1996 (1996 Act).[4] The E-Rate program currently funds basic firewall service provided as part of the vendor's Internet service as a category one service and separately-priced basic firewalls as a category two service. The E-Rate program, however, does not currently fund advanced firewalls or other cybersecurity services and equipment that have increasingly been requested by commenters to protect school and library networks from cyber harms over the years.

4. In the *Report and Order*, the Commission establishes a three-year Pilot Program (Pilot or Pilot Program) funded at $200 million, within the Universal Service Fund (USF) but separate from the E-Rate program, to enable it to assess the costs and benefits of utilizing universal service funds to support schools' and libraries' cybersecurity needs and how other federal resources could be leveraged to ensure that these needs are addressed in the most efficient and effective manner. One objective of the Pilot is to help participants acquire cybersecurity services and equipment, including many of the equipment and services that have specifically been requested by commenters in the record, to improve the security of their broadband networks and data. Another objective of the Pilot is to measure the costs and effectiveness of cybersecurity services and equipment. By making a wide range of cybersecurity services and equipment eligible for USF support, the Pilot will enable the Commission to gather data on the associated cost and effectiveness of various solutions. A further objective of the Pilot is to evaluate how to best leverage other available low cost and free federal resources to help schools and libraries proactively address K-12 cybersecurity risks. To ensure that these objectives can be met, the Commission also adopts requirements that Pilot participants provide initial, annual, and final reports so that Pilot

[1] 5 U.S.C. § 603. The RFA, 5 U.S.C. §§ 601-612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[2] *Schools and Libraries Cybersecurity Pilot Program*, WC Docket No. 23-234, Notice of Proposed Rulemaking, FCC 23-92, 2023 WL 8605080 (Nov. 13, 2023).

[3] 5 U.S.C. § 604.

[4] Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified at 47 U.S.C. § 151 *et seq.*).

participants can be evaluated for their cybersecurity readiness before they begin participation in, during, and after the conclusion of the Pilot Program. By taking these actions, the Commission will be able to better to fulfill its obligation to ensure that schools and libraries have access to advanced telecommunications, as provided for by Congress in the 1996 Act.

5. In addition, the *Report and Order* finalizes several aspects of the structure and administration of the Pilot based on the proposals made in the *Cybersecurity NPRM*. For example, the Pilot establishes: (1) that schools and school districts will be eligible to receive up to $13.60 per student, on a pre-discounted basis, to purchase eligible cybersecurity services and equipment, with a funding floor of $15,000 and a funding maximum of $1.5 million; (2) a budget of $15,000 per library, with the provision that library systems with more than 11 sites will be eligible for support up to $175,000; and (3) that consortia participants comprised of eligible schools and libraries are eligible to receive funding based on student count (using the $13.60 per student multiplier) and the number of library sites (using the $15,000 per library budget) subject to either the $175,000 budget maximum for library systems or $1.5 million budget maximum for schools depending on the consortium's constituency. In addition, the Pilot requires participants to contribute a portion of the costs of the cybersecurity services and equipment they seek to purchase with Pilot Program support, similar to the non-discount share that E-Rate applicants are required to contribute to the cost of their eligible services and equipment. We also permit Pilot participants to request reimbursement as expenses are incurred during the Pilot's term. We also permit all eligible schools and libraries, including those that do not currently participate in the E-Rate program, to apply to participate in the Pilot.

6. We also adopt a Pilot Eligible Services List (P-ESL) in the *Report and Order*, which specifies eligible cybersecurity services and equipment for the Pilot. The P-ESL deems services and/or equipment eligible if they constitute a protection designed to improve or enhance the cybersecurity of a K-12 school, library or consortia. To provide clarity and specificity to small entity and other participants, the P-ESL also enumerates as eligible, in a non-limiting manner, four categories of technology raised by commenters as effective in combatting cyber threats, namely, (i) advanced/next-generation firewalls; (ii) endpoint protection; (iii) identity protection and authentication; and (iv) monitoring, detection and response. For purposes of the Pilot, we define: (i) an "advanced" or "next-generation" firewall as equipment, services, or a combination of equipment and services, that limits access between networks, excluding basic firewalls that are funded through the Commission's E-Rate program; (ii) endpoint protection as equipment, services, or a combination of equipment and services that implements safeguards to protect school- and library-owned end-user devices, including desktops, laptops, and mobile devices, against cyber threats and attacks; (iii) identity protection and authentication as equipment, services, or a combination of equipment and services that implements safeguards to protect a user's network identity from theft or misuse and/or provide assurance about the network identity of an entity interacting with a system; and (iv) monitoring, detection and response as equipment, services, or a combination of equipment and services that monitor and/or detect threats to a network and that take responsive action to remediate or otherwise address those threats. Through the list of examples provided in the P-ESL, we confirm that a wide range of services and equipment that we had proposed for inclusion in the *Cybersecurity NPRM*, or that commenters had otherwise requested, are eligible. In the *Report and Order*, we describe that eligibility is limited to equipment that is network-based (i.e., that excludes end-user devices, including, for example, tablets, smartphones, and laptops) and services that are network-based and/or locally installed on end-user devices, where the devices are owned or leased by the school or library, and where equipment and services are designed to identify and/or remediate threats that could otherwise directly impair or disrupt a school's or library's network, including to threats from users accessing the network remotely.

7. In the *Report and Order*, we explain that ineligible costs include, among other things, (i) any equipment, service, or other related cost that is eligible in the Commission's E-Rate eligible services list program in the funding year for which Pilot reimbursement is sought, (ii) any equipment, service or other related cost for which a participant has already received reimbursement, or plans to apply for reimbursement, through any other USF or federal, state, or local program in the funding year for which

Pilot reimbursement is sought, and (iii) any equipment or services prohibited by the Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609) (Secure Networks Act) or the Commission's rules, including Commission rules 54.9 and 54.10, that implement the Secure Networks Act.

8. We designate USAC to be the administrator for the Pilot. We require applicants to submit part one of a FCC Form 484 application describing its proposed Pilot project and providing information to facilitate the evaluation and eventual selection of high-quality projects for inclusion in the Pilot. To facilitate the inclusion of a diverse set of Pilot projects and to target Pilot funds to the populations most in need of cybersecurity support, we anticipate selecting projects from, and providing funding to, a combination of large and small and urban and rural schools, libraries, and consortia, with an emphasis on funding proposed Pilot projects that include low-income and Tribal applicants. Further, we encourage participation in the Pilot by a broad range of service providers and do not discourage new companies from participating, nor do we require service providers to have preexisting service provider identification numbers (SPIN) before submitting cybersecurity bids or previous E-Rate experience before participating in the Pilot.

9. In the *Report and Order*, we describe that we will direct funding to: (1) the neediest eligible schools, libraries, and consortia who will benefit most from cybersecurity funding (i.e., those at the highest discount rate percentages); (2) as many eligible schools, libraries, and consortia as possible; (3) those schools, libraries, and consortia that include Tribal entities; and (4) a mix of large and small and urban and rural, schools, libraries, and consortia. This will ensure that the Pilot contains a diverse cross-section of applicants with differing cybersecurity postures and experiences. In the event that number of FCC Form 484 applications received exceeds the number of projects that can be funded through the Pilot, we will prioritize selection of Pilot participants by considering their funding needs in combination with the funding needs of the same type(s) of applicants with an eye toward selecting Pilot participants with differing levels of exposure to cybersecurity threats and attacks. In the event that there is insufficient funding to select all of the Pilot participants at a particular discount rate, we will prioritize the selection of Pilot participants within the discount rate using the percentage of students who are eligible for free and reduced lunches within each applicant's school district. Funding for libraries will be prioritized based on the percentage of free and reduced lunch eligible students in the school district that is used to calculate the library's discount rate. Funding for individual schools that are not affiliated financially or operationally with a school district, such as private or charter schools that apply individually, will be prioritized based on each school's individual free and reduced student lunch eligible population.

10. In the *Report and Order*, we direct the Bureau and the Universal Service Administration Company (USAC or the Administrator) to model the Pilot processes and forms on existing E-Rate and Emergency Connectivity Fund (ECF) programs' processes and forms to the extent possible for the Pilot Program. We expect the Bureau and USAC to leverage Pilot forms, that will mirror existing E-Rate and ECF forms: (1) FCC Form 470 (Description of Services Requested and Certification Form); (2) FCC Form 471 (Description of Services Ordered and Certification Form); (3) FCC Form 472 (Billed Entity Applicant Reimbursement (BEAR) Form); and (4) FCC Form 474 (Service Provider Invoice (SPI) Form).

11. To protect the integrity of the Pilot, and safeguard universal service funds, we implement a number of program integrity protections. For example, we implement document retention requirements and a prohibition on gifts, and we require applicants provide certain certifications and be subject to auditing. We have modeled these provisions after our E-Rate processes to protect the Pilot and ensure the limited program funding is used for its intended purposes. We also apply our existing suspension are debarment rules to the Pilot. We also delegate to Bureau and USAC the authority to address and resolve a number of matters, including unforeseen administrative issues or problems, provided that doing so is consistent with the decisions we reach in the *Report and Order*. We expect that this action will allow the Bureau and USAC to reduce any undue burdens on applicants and other individual and entities involved in the Pilot Program, while ensuring that all program goals are efficient and effectively satisfied.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

12. There were no comments filed that specifically address the proposed rules and policies presented in the IRFA.

C. Response to Comments by the Chief Counsel for Advocacy of the Small Business Administration

13. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration (SBA), and to provide a detailed statement of any change made to the proposed rules as a result of those comments.[5] The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

D. Description and Estimate of the Number of Small Entities to Which the Rules Will Apply

14. The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of small entities that may be affected by the rules adopted herein.[6] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[7] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[8] A small business concern is one that: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the Small Business Administration (SBA).[9]

15. *Small Businesses, Small Organizations, Small Governmental Jurisdictions.* Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe, at the outset, three broad groups of small entities that could be directly affected herein.[10] First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, in general a small business is an independent business having fewer than 500 employees.[11] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 33.2 million businesses.[12]

16. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."[13] The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual

[5] 5 U.S.C. § 604(a)(3).

[6] *Id.* § 604 (a)(4).

[7] *Id.* § 601(6).

[8] *Id.* § 601(3) (incorporating by reference the definition of "small business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[9] 15 U.S.C. § 632.

[10] 5 U.S.C. § 601(3)-(6).

[11] *See* SBA, Office of Advocacy, "What's New With Small Business?," https://advocacy.sba.gov/wp-content/uploads/2023/03/Whats-New-Infographic-March-2023-508c.pdf (Mar. 2023).

[12] *Id*.

[13] 5 U.S.C. § 601(4).

electronic filing requirements for small exempt organizations.[14] Nationwide, for tax year 2022, there were approximately 530,109 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.[15]

17. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[16] U.S. Census Bureau data from the 2022 Census of Governments[17] indicate there were 90,837 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.[18] Of this number, there were 36,845 general purpose governments (county,[19] municipal, and town or township[20]) with populations of less than 50,000 and 11,879 special purpose governments (independent school districts[21]) with enrollment

[14] The IRS benchmark is similar to the population of less than 50,000 benchmark in 5 U.S.C § 601(5) that is used to define a small governmental jurisdiction. Therefore, the IRS benchmark has been used to estimate the number of small organizations in this small entity description. *See* Annual Electronic Filing Requirement for Small Exempt Organizations – Form 990-N (e-Postcard), "Who must file," https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard. We note that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.

[15] *See* Exempt Organizations Business Master File Extract (EO BMF), "CSV Files by Region," https://www.irs.gov/charities-non-profits/exempt-organizations-business-master-file-extract-eo-bmf. The IRS Exempt Organization Business Master File (EO BMF) Extract provides information on all registered tax-exempt/non-profit organizations. The data utilized for purposes of this description was extracted from the IRS EO BMF data for businesses for the tax year 2022 with revenue less than or equal to $50,000 for Region 1-Northeast Area (71,897), Region 2-Mid-Atlantic and Great Lakes Areas (197,296), and Region 3-Gulf Coast and Pacific Coast Areas (260,447) that includes the continental U.S., Alaska, and Hawaii. This data includes information for Puerto Rico (469).

[16] 5 U.S.C. § 601(5).

[17] 13 U.S.C. § 161. The Census of Governments survey is conducted every five (5) years compiling data for years ending with "2" and "7". *See also* Census of Governments, https://www.census.gov/programs-surveys/economic-census/year/2022/about.html.

[18] *See* U.S. Census Bureau, 2022 Census of Governments – Organization Table 2. Local Governments by Type and State: 2022 [CG2200ORG02], https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html. Local governmental jurisdictions are made up of general purpose governments (county, municipal and town or township) and special purpose governments (special districts and independent school districts). *See also* tbl.2. CG2200ORG02 Table Notes_Local Governments by Type and State_2022.

[19] *See id.* at tbl.5. County Governments by Population-Size Group and State: 2022 [CG2200ORG05], https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html. There were 2,097 county governments with populations less than 50,000. This category does not include subcounty (municipal and township) governments.

[20] *See id.* at tbl.6. Subcounty General-Purpose Governments by Population-Size Group and State: 2022 [CG2200ORG06], https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html. There were 18,693 municipal and 16,055 town and township governments with populations less than 50,000.

[21] *See id.* at tbl.10. Elementary and Secondary School Systems by Enrollment-Size Group and State: 2022 [CG2200ORG10], https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html. There were 11,879 independent school districts with enrollment populations less than 50,000. *See also* tbl.4. Special-Purpose Local Governments by State Census Years 1942 to 2022 [CG2200ORG04], CG2200ORG04 Table Notes_Special Purpose Local Governments by State_Census Years 1942 to 2022.

populations of less than 50,000.[22] Accordingly, based on the 2022 U.S. Census of Governments data, we estimate that at least 48,724 entities fall into the category of "small governmental jurisdictions."[23]

1. Schools and Libraries

18. *Schools.* The closest applicable industry with a SBA small business size standard is Elementary and Secondary Schools.[24] This industry comprises establishments primarily engaged in furnishing academic courses and associated course work that comprise a basic preparatory education.[25] A basic preparatory education ordinarily constitutes kindergarten through 12th grade.[26] The SBA small business size standard for Elementary and Secondary Schools classifies firms with annual receipts of $17.5 million or less as small.[27] The Commission does not have a size standard for small entities specifically applicable to schools. The Commission's definition of schools pertains to entities that participate in the E-Rate program which provides support to eligible schools and libraries to enable access to high-speed Internet access and telecommunications services at affordable rates, consistent with the objectives of universal service.

19. Under the E-Rate program an elementary school is generally "a non-profit institutional day or residential school that provides elementary education, as determined under state law."[28] A secondary school is generally defined as "a non-profit institutional day or residential school that provides secondary education, as determined under state law," and not offering education beyond grade 12.[29] For-profit schools, and schools with endowments in excess of $50,000,000, are not eligible to receive discounts under the E-Rate program.[30] In calendar year 2017, the E-rate program provided funding to approximately 104,722 schools throughout the U.S. and its territories.[31] While we do not have financial information that would allow us to estimate the number of schools that would qualify as small entities under SBA's small business size standard, because of the nature of these entities we estimate that the majority of schools in the E-Rate program are small entities under the SBA size standard.

20. *Libraries.* The closest applicable industry with a SBA small business size standard is Libraries and Archives.[32] This industry comprises establishments primarily engaged in providing library

[22] While the special purpose governments category also includes local special district governments, the 2022 Census of Governments data does not provide data aggregated based on population size for the special purpose governments category. Therefore, only data from independent school districts is included in the special purpose governments category.

[23] This total is derived from the sum of the number of general purpose governments (county, municipal and town or township) with populations of less than 50,000 (36,845) and the number of special purpose governments - independent school districts with enrollment populations of less than 50,000 (11,879), from the 2022 Census of Governments - Organizations tbls. 5, 6 & 10.

[24] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*611110 Elementary and Secondary Schools,*" https://www.census.gov/naics/?input=611110&year=2017&details=611110.

[25] *Id*.

[26] *Id*.

[27] *See* 13 CFR § 121.201, NAICS Code 611110.

[28] 47 CFR § 54.500.

[29] *Id.*

[30] 47 CFR § 54.501.

[31] *See* Universal Service Administrative Company, Annual Report, at 7, https://www.usac.org/wp-content/uploads/about/documents/annual-reports/2017/USAC-2017-Annual-Report.pdf.

[32] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*519120 Libraries and Archives,"* https://www.census.gov/naics/?input=519120&year=2017&details=519120.

or archive services.[33] These establishments are engaged in maintaining collections of documents (e.g., books, journals, newspapers, and music) and facilitating the use of such documents (recorded information regardless of its physical form and characteristics) as required to meet the informational, research, educational, or recreational needs of their user.[34] These establishments may also acquire, research, store, preserve, and generally make accessible to the public historical documents, photographs, maps, audio material, audiovisual material, and other archival material of historical interest.[35] All or portions of these collections may be accessible electronically.[36] The SBA small business size standard for Libraries and Archives classifies firms with annual receipts of $18.5 million or less as small.[37] For this industry, U.S. Census Bureau data for 2017 show that there were 1,864 firms that operated for the entire year.[38] Of this number, 1,228 firms had revenues of less than $10 million.[39] Based on this data, the majority of firms in this industry can be considered small.

21. The Commission does not have a size standard for small entities specifically applicable to libraries. The Commission's definition of libraries pertains to entities that participate in the E-Rate program which provides support to eligible schools and libraries to enable access to high-speed Internet access and telecommunications services at affordable rates, consistent with the objectives of universal service. Under the E-Rate program, a library includes "(1) a public library, (2) a public elementary school or secondary school library, (3) an academic library, (4) a research library [] and (5) a private library, but only if the state in which such private library is located determines that the library should be considered a library for the purposes of this definition."[40] For-profit libraries, are not eligible to receive discounts under the program, nor are libraries whose budgets are not completely separate from any schools.[41] In calendar year 2017, the E-rate program provided funding to approximately 11,475 libraries throughout the U.S. and its territories.[42] While we do not have financial information which would allow us to estimate the number of libraries that would qualify as small entities under SBA's small business size standard, because of the nature of these entities we estimate that the majority of libraries in the E-Rate program are small entities under the SBA size standard.

---

[33] *Id*.

[34] *Id*.

[35] *Id*.

[36] *Id*.

[37] *See* 13 CFR § 121.201, NAICS Code 519120 (as of 10/1/22 NAICS Code 519210).

[38] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 519120, https://data.census.gov/cedsci/table?y=2017&n=519120&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[39] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We note that the U.S. Census Bureau withheld publication of the number of firms that operated with sales/value of shipments/revenue in the individual category for less than $100,000, to avoid disclosing data for individual companies (see Cell Notes for the sales/value of shipments/revenue in this category). Therefore, the number of firms with revenue that meet the SBA size standard would be higher than noted herein. We also note that the U.S. Census Bureau economic data includes sales, value of shipments or revenue information reported by firms. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[40] 47 CFR § 54.500.

[41] 47 CFR § 54.501.

[42] *See* Universal Service Administrative Company, Annual Report, at 7, https://www.usac.org/wp-content/uploads/about/documents/annual-reports/2017/USAC-2017-Annual-Report.pdf.

2. Telecommunications Service Providers

22. *Telecommunications Resellers*. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households.[43] Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[44] Mobile virtual network operators (MVNOs) are included in this industry.[45] The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[46] U.S. Census Bureau data for 2017 show that 1,386 firms operated in this industry for the entire year.[47] Of that number, 1,375 firms operated with fewer than 250 employees.[48] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 666 providers that reported they were engaged in the provision of local or toll resale services.[49] Of these providers, the Commission estimates that 640 providers have 1,500 or fewer employees.[50] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

23. *Local Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Local Resellers. Telecommunications Resellers is the closest industry with a SBA small business size standard.[51] The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households.[52] Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[53] Mobile virtual network operators (MVNOs) are included in this industry.[54] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[55] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[56] Of that number, 1,375

[43] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[44] *Id.*

[45] *Id.*

[46] *See* 13 CFR § 121.201, NAICS Code 517911 (as of 10/1/22, NAICS Code 517121).

[47] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[48] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[49] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[50] *Id.*

[51] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[52] *Id.*

[53] *Id.*

[54] *Id.*

[55] *See* 13 CFR § 121.201, NAICS Code 517911 (as of 10/1/22, NAICS Code 517121).

[56] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911,

(continued….)

firms operated with fewer than 250 employees.[57] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 207 providers that reported they were engaged in the provision of local resale services.[58] Of these providers, the Commission estimates that 202 providers have 1,500 or fewer employees.[59] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

24. *Wired Telecommunications Carriers.* The U.S. Census Bureau defines this industry as establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks.[60] Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband Internet services.[61] By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry.[62] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[63]

25. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[64] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[65] Of this number, 2,964 firms operated with fewer than 250 employees.[66] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 4,590 providers that reported they were engaged in the provision of fixed local services.[67] Of these providers, the Commission estimates that 4,146

(Continued from previous page)
https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[57] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[58] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[59] *Id.*

[60] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[61] *Id.*

[62] *Id.*

[63] Fixed Local Service Providers include the following types of providers: Incumbent Local Exchange Carriers (ILECs), Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, and Other Local Service Providers. Local Resellers fall into another U.S. Census Bureau industry group and therefore data for these providers is not included in this industry.

[64] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[65] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[66] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[67] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022),
(continued….)

providers have 1,500 or fewer employees.[68] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

26. *All Other Telecommunications.* This industry is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation.[69] This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems.[70] Providers of Internet services (e.g. dial-up ISPs) or Voice over Internet Protocol (VoIP) services, via client-supplied telecommunications connections are also included in this industry.[71] The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small.[72] U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year.[73] Of those firms, 1,039 had revenue of less than $25 million.[74] Based on this data, the Commission estimates that the majority of "All Other Telecommunications" firms can be considered small.

27. *Wireless Telecommunications Carriers (except Satellite).* This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves.[75] Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless Internet access, and wireless video services.[76] The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[77] U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year.[78] Of that number, 2,837 firms employed fewer than 250

(Continued from previous page)
https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf. https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf.

[68] *Id.*

[69] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517919 All Other Telecommunications,*" https://www.census.gov/naics/?input=517919&year=2017&details=517919.

[70] *Id.*

[71] *Id.*

[72] *See* 13 CFR § 121.201, NAICS Code 517919 (as of 10/1/22, NAICS Code 517810).

[73] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517919, https://data.census.gov/cedsci/table?y=2017&n=517919&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[74] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[75] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[76] *Id.*

[77] *See* 13 CFR § 121.201, NAICS Code 517312 (as of 10/1/22, NAICS Code 517112).

[78] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

employees.[79] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 594 providers that reported they were engaged in the provision of wireless services.[80] Of these providers, the Commission estimates that 511 providers have 1,500 or fewer employees.[81] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

28. *Wireless Carriers and Service Providers.* Wireless Telecommunications Carriers (*except* Satellite) is the closest industry with a SBA small business size standard applicable to these service providers.[82] The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[83] U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year.[84] Of this number, 2,837 firms employed fewer than 250 employees.[85] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 594 providers that reported they were engaged in the provision of wireless services.[86] Of these providers, the Commission estimates that 511 providers have 1,500 or fewer employees.[87] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

3. Internet Service Providers (ISPs)

29. *Wired Broadband Internet Access Service Providers (Wired ISPs).*[88] Providers of wired broadband Internet access service include various types of providers except dial-up Internet access providers. Wireline service that terminates at an end user location or mobile device and enables the end user to receive information from and/or send information to the Internet at information transfer rates exceeding 200 kilobits per second (kbps) in at least one direction is classified as a broadband connection under the Commission's rules.[89] Wired broadband Internet services fall in the Wired Telecommunications Carriers industry.[90] The SBA small business size standard for this industry

[79] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[80] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[81] *Id.*

[82] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers* (*except Satellite*)," https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[83] *See* 13 CFR § 121.201, NAICS Code 517312 (as of 10/1/22, NAICS Code 517112).

[84] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[85] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[86] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[87] *Id.*

[88] Formerly included in the scope of the Internet Service Providers (Broadband), Wired Telecommunications Carriers and All Other Telecommunications small entity industry descriptions.

[89] *See* 47 CFR § 1.7001(a)(1).

[90] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

classifies firms having 1,500 or fewer employees as small.[91] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[92] Of this number, 2,964 firms operated with fewer than 250 employees.[93]

30. Additionally, according to Commission data on Internet access services as of June 30, 2019, nationwide there were approximately 2,747 providers of connections over 200 kbps in at least one direction using various wireline technologies.[94] The Commission does not collect data on the number of employees for providers of these services, therefore, at this time we are not able to estimate the number of providers that would qualify as small under the SBA's small business size standard. However, in light of the general data on fixed technology service providers in the Commission's *2022 Communications Marketplace Report*,[95] we believe that the majority of wireline Internet access service providers can be considered small entities

31. *Wireless Broadband Internet Access Service Providers (Wireless ISPs or WISPs).*[96] Providers of wireless broadband Internet access service include fixed and mobile wireless providers. The Commission defines a WISP as "[a] company that provides end-users with wireless access to the Internet[.]"[97] Wireless service that terminates at an end user location or mobile device and enables the end user to receive information from and/or send information to the Internet at information transfer rates exceeding 200 kilobits per second (kbps) in at least one direction is classified as a broadband connection under the Commission's rules.[98] Neither the SBA nor the Commission have developed a size standard specifically applicable to Wireless Broadband Internet Access Service Providers. The closest applicable industry with an SBA small business size standard is Wireless Telecommunications Carriers (except Satellite).[99] The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer

[91] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[92] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[93] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[94] *See* Federal Communications Commission, Internet Access Services: Status as of June 30, 2019 at 27, Fig. 30 *(IAS Status 2019)*, Industry Analysis Division, Office of Economics & Analytics (March 2022). The report can be accessed at https://www.fcc.gov/economics-analytics/industry-analysis-division/iad-data-statistical-reports. The technologies used by providers include aDSL, sDSL, Other Wireline, Cable Modem and FTTP). Other wireline includes: all copper-wire based technologies other than xDSL (such as Ethernet over copper, T-1/DS-1 and T3/DS-1) as well as power line technologies which are included in this category to maintain the confidentiality of the providers.

[95] *See Communications Marketplace Report*, GN Docket No. 22-203, 2022 WL 18110553 at 10, paras. 26-27, Figs. II.A.5-7. (2022) (*2022 Communications Marketplace Report*).

[96] Formerly included in the scope of the Internet Service Providers (Broadband), Wireless Telecommunications Carriers (except Satellite) and All Other Telecommunications small entity industry descriptions.

[97] Federal Communications Commission, Internet Access Services: Status as of June 30, 2019 at 27, Fig. 30 *(IAS Status 2019)*, Industry Analysis Division, Office of Economics & Analytics (March 2022). The report can be accessed at https://www.fcc.gov/economics-analytics/industry-analysis-division/iad-data-statistical-reports.

[98] *See* 47 CFR § 1.7001(a)(1).

[99] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

employees.[100] U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year.[101] Of that number, 2,837 firms employed fewer than 250 employees.[102]

32. Additionally, according to Commission data on Internet access services as of June 30, 2019, nationwide there were approximately 1,237 fixed wireless and 70 mobile wireless providers of connections over 200 kbps in at least one direction.[103] The Commission does not collect data on the number of employees for providers of these services, therefore, at this time we are not able to estimate the number of providers that would qualify as small under the SBA's small business size standard. However, based on data in the Commission's *2022 Communications Marketplace Report* on the small number of large mobile wireless nationwide and regional facilities-based providers, the dozens of small regional facilities-based providers and the number of wireless mobile virtual network providers in general,[104] as well as on terrestrial fixed wireless broadband providers in general,[105] we believe that the majority of wireless Internet access service providers can be considered small entities.

33. *Internet Service Providers (Non-Broadband).* Internet access service providers using client-supplied telecommunications connections (e.g., dial-up ISPs) as well as VoIP service providers using client-supplied telecommunications connections fall in the industry classification of All Other Telecommunications.[106] The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small.[107] For this industry, U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year.[108] Of those firms, 1,039 had revenue of less than $25 million.[109] Consequently, under the SBA size standard a majority of firms in this industry can be considered small.

4. Vendors of Internal Connections

34. *Vendors of Infrastructure Development or Network Buildout.* The Commission nor the SBA have developed a small business size standard specifically directed toward manufacturers of network facilities. There are two applicable industries in which manufacturers of network facilities could

[100] *See* 13 CFR § 121.201, NAICS Code 517312 (as of 10/1/22, NAICS Code 517112).

[101] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[102] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[103] *See IAS Status 2019,* Fig. 30.

[104] *See Communications Marketplace Report*, GN Docket No. 22-203, 2022 WL 18110553 at 27, paras. 64-68. (2022) (*2022 Communications Marketplace Report*).

[105] *Id.* at 8, para. 22.

[106] *See* U.S. Census Bureau, *2017 NAICS Definition, "517919 All Other Telecommunications,*" https://www.census.gov/naics/?input=517919&year=2017&details=517919.

[107] *See* 13 CFR § 121.201, NAICS Code 517919 (as of 10/1/22, NAICS Code 517810).

[108] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517919, https://data.census.gov/cedsci/table?y=2017&n=517919&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[109] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

fall and each have different SBA business size standards. The applicable industries are "Radio and Television Broadcasting and Wireless Communications Equipment"[110] with a SBA small business size standard of 1,250 employees or less,[111] and "Other Communications Equipment Manufacturing"[112] with a SBA small business size standard of 750 employees or less."[113] U.S. Census Bureau data for 2017 show that for Radio and Television Broadcasting and Wireless Communications Equipment there were 656 firms in this industry that operated for the entire year.[114] Of this number, 624 firms had fewer than 250 employees.[115] For Other Communications Equipment Manufacturing, U.S. Census Bureau data for 2017 show that there were 321 firms in this industry that operated for the entire year.[116] Of that number, 310 firms operated with fewer than 250 employees.[117] Based on this data, we conclude that the majority of firms in this industry are small.

35. *Telephone Apparatus Manufacturing*. This industry comprises establishments primarily engaged in manufacturing wire telephone and data communications equipment.[118] These products may be stand-alone or board-level components of a larger system. Examples of products made by these establishments are central office switching equipment, cordless and wire telephones (except cellular), PBX equipment, telephone answering machines, LAN modems, multi-user modems, and other data communications equipment, such as bridges, routers, and gateways.[119] The SBA small business size standard for Telephone Apparatus Manufacturing classifies businesses having 1,250 or fewer employees as small.[120] U.S. Census Bureau data for 2017 show that there were 189 firms in this industry that operated for the entire year.[121] Of this number, 177 firms operated with fewer than 250 employees.[122] Thus, under the SBA size standard, the majority of firms in this industry can be considered small.

---

[110] *See* U.S. Census Bureau, *2017 NAICS Definition, "334220 Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing,"* https://www.census.gov/naics/?input=334220&year=2017&details=334220.

[111] *See* 13 CFR § 121.201, NAICS Code 334220.

[112] *See* U.S. Census Bureau, *2017 NAICS Definition, "334290 Other Communications Equipment Manufacturing,"* https://www.census.gov/naics/?input=334290&year=2017&details=334290.

[113] *See* 13 CFR § 121.201, NAICS Code 334290.

[114] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 334220, https://data.census.gov/cedsci/table?y=2017&n=334220&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[115] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[116] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 334290, https://data.census.gov/cedsci/table?y=2017&n=334290&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[117] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[118] *See* U.S. Census Bureau, *2017 NAICS Definition, "334210 Telephone Apparatus Manufacturing,"* https://www.census.gov/naics/?input=334210&year=2017&details=334210.

[119] *Id.*

[120] *See* 13 CFR § 121.201, NAICS Code 334210.

[121] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 334210,

(continued….)

5. Other Service Providers

36. *Custom Computer Programming Services.* This industry is comprises establishments primarily engaged in writing, modifying, testing, and supporting software to meet the needs of a particular customer.[123] The industry includes firms engaged in applications software programming, computer program or software development, computer programming services, computer software analysis and design services, computer software programming services, computer software support services, and Web (i.e., Internet) page design services.[124] The SBA small business size standard for this industry classifies firms having annual receipts of $30 million or less as small.[125] According to 2017 U.S. Census Bureau data there were 46,636 firms that operated in this industry for the entire year.[126] Of this number, 45,394 firms had revenue of less than $25 million.[127] Based on this data, the Commission concludes that the majority of the businesses engaged in this industry are small.

37. *Other Computer Related Services (Except Information Technology Value Added Resellers).* This industry comprises establishments primarily engaged in providing computer related services (except custom programming, systems integration design, and facilities management services).[128] Establishments providing computer disaster recovery services or software installation services are included in this industry.[129] The SBA small business size standard for this industry classifies firms with annual receipts of $30 million or less as small.[130] The 2017 Economic Census indicates that 6,228 firms in this industry operated for the entire year.[131] Of that number, 6,104 firms had revenue of less than $25 million.[132] Based on this data, we conclude that a majority of firms in this industry are small.

38. *Information Technology Value Added Resellers*. Information Technology Value Added

(Continued from previous page)
https://data.census.gov/cedsci/table?y=2017&n=334210&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[122] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[123] *See U.S. Census Bureau*, *2017 NAICS Definition, "541511 Custom Computer Programming Services,"* https://www.census.gov/naics/?input=541511&year=2017&details=541511.

[124] *Id.*

[125] *See* 13 CFR § 121.201, NAICS Code 541511.

[126] *See U.S. Census Bureau*, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 541511, https://data.census.gov/cedsci/table?y=2017&n=541511&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[127] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[128] *See* U.S. Census Bureau, *2017 NAICS Definition, "541519 Other Computer Related Services*," https://www.census.gov/naics/?input=541519&year=2017&details=541519.

[129] *Id*.

[130] *See* 13 CFR § 121.201, NAICS Code *541519*.

[131] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code *541519*, https://data.census.gov/cedsci/table?y=2017&n=541519&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[132] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

Resellers (ITVARs) fall with the Other Computer Related Services industry.[133] ITVARs are a subgroup of this industry which the SBA describes as providing a total solution to information technology acquisitions by providing multi-vendor hardware and software along with significant value added services.[134] Significant value added services consist of, but are not limited to, configuration consulting and design, systems integration, installation of multi-vendor computer equipment, customization of hardware or software, training, product technical support, maintenance, and end user support.[135] The SBA small business size standard for ITVARs classifies a business as small if it has 150 or fewer employees.[136] According to U.S. Census Bureau data for 2017, 6,228 firms in this industry operated for the entire year. [137] Of this number, 6,086 firms operated with fewer than 100 employees.[138] Based on this data, the Commission estimates that the majority of information technology value added resellers can be considered small.

39. *Software Publishers.* This industry comprises establishments primarily engaged in computer software publishing or publishing and reproduction.[139] Establishments in this industry carry out operations necessary for producing and distributing computer software, such as designing, providing documentation, assisting in installation, and providing support services to software purchasers.[140] These establishments may design, develop, and publish, or publish only.[141] The SBA small business size standard for this industry classifies businesses having annual receipts of $41.5 million or less as small.[142] U.S. Census Bureau data for 2017 indicate that 7,842 firms in this industry operated for the entire year. [143] Of this number 7,226 firms had revenue of less than $25 million.[144] Based on this data, we conclude that a majority of firms in this industry are small.

---

[133] *See* U.S. Census Bureau, *2017 NAICS Definition, "541519 Other Computer Related Services,"* https://www.census.gov/naics/?input=541519&year=2017&details=541519.

[134] *See* 13 CFR § 121.201, NAICS Code 541519_Except note 18.

[135] *Id.*

[136] *Id.*

[137] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 541519, https://data.census.gov/cedsci/table?y=2017&n=541519&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[138] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[139] *See* U.S. Census Bureau, *2017 NAICS Definition, "511210 Software Publishers,"* https://www.census.gov/naics/?input=511210&year=2017&details=511210.

[140] *Id.*

[141] *Id.*

[142] *See* 13 CFR § 121.201, NAICS Code 511210 (as of 10/1/22 NAICS Code 513210).

[143] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 511210, https://data.census.gov/cedsci/table?y=2017&n=511210&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[144] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

E. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

40. While the Commission sought to minimize compliance burdens on small entities where practicable, the rules adopted in the *Report and Order* will impose new or additional reporting, recordkeeping, and/or other compliance obligations on small entities that participate in the Pilot Program. The adopted rules encompass a broad range of Pilot-related compliance requirements that are summarized in further detail below.

41. *Application process.* The purpose of the Pilot Program is to better assess the costs and benefits of utilizing universal service funds to support schools' and libraries' cybersecurity needs and how other federal resources could be leveraged to ensure that these needs are addressed in the most efficient and effective manner. To do so, we require Pilot applicants to submit, as part of their application to participate in the Pilot, part one (out of two parts) of a new FCC Form 484 application, including by completing appropriate certifications. In this first part of the application, an applicant will provide a general level of cybersecurity information about itself and its proposed Pilot project, and will use pre-populated data, as well as a number of "yes/no" questions and questions with a predetermined set of responses (i.e., multiselect questions with predefined answers). The applicant will explain how its proposed project meets a number of criteria outlined in the *Report and Order*. In addition, the applicant must present a clear strategy for addressing the cybersecurity needs of its K-12 school(s) and/or library(ies) pursuant to its proposed Pilot project, and clearly articulate how the project will accomplish the applicant's cybersecurity objectives. After selection for participation Pilot, participants shall submit to USAC a second part to the FCC Form 484, including by completing appropriate certifications. The second part will require that participants provide more detailed cybersecurity data and Pilot project information, including a description of the Pilot participant's current cybersecurity posture, information about the participant's planned use(s) for other federal, state, or local cybersecurity funding (i.e., funding obtained outside of the Pilot) and information about a participant's history of cyber threats and attacks within a year of the date of its application. Moreover, we permit applications to be submitted through an online Pilot portal on USAC's website and we direct the Bureau to issue a Public Notice that includes details and instructions on how to submit an application using the Pilot portal on USAC's website.

42. *Competitive Bidding, Requests for Services, and Invoicing and Reimbursement Processes*. We require Pilot participants to provide information related to competitive bidding, requests for services and invoice and reimbursement information, including associated and appropriate certifications, using new Pilot Program forms that will mirror existing E-Rate and ECF forms: (1) FCC Form 470 (Description of Services Requested and Certification Form);(2) FCC Form 471 (Description of Services Ordered and Certification Form); (3) FCC Form 472 (Billed Entity Applicant Reimbursement (BEAR) Form); and (4) FCC Form 474 (Service Provider Invoice (SPI) Form).

43. *Reporting Requirements.* We require Pilot participants to submit initial, annual and final reports. Applicants must provide an initial baseline assessment using information that includes the reporting requirements for the second part of the application process described above.

44. *Document Retention Requirements*. We require Pilot participants to retain all documents related to their participation in the Pilot Program sufficient to demonstrate compliance with all program rules for at least 10 years from the last date of service or delivery of equipment and to maintain asset and inventory records of services and equipment purchased sufficient to verify the actual location of such services and equipment for a period of 10 years after purchase. We also require Pilot participants to present such records upon request of any representative (including any auditor) appointed by a state education department, the Administrator, the Commission, its Inspector General, or any local, state or federal agency with jurisdiction over the entity.

45. *Pilot Program Certifications.* As noted above, we require participants to provide several certifications as part of their FCC Form 484 application, competitive bidding requirements, requests for services, and invoicing processes. Similarly, we require their selected service providers to provide certifications related to invoicing processes. We also require Pilot participants and service providers to

certify that they are not seeking support or reimbursement for Pilot-eligible services and equipment that has been purchased and reimbursed from other federal, state, Tribal, or local funding sources or that is eligible for discounts from E-Rate or another universal service program. Pilot participants and service providers must certify that they are seeking funding for only Pilot-eligible services and equipment.

46. *Other Delegations*. As part of the *Report and Order*, we also delegate to Bureau and USAC the authority to address and resolve a number of procedural or administrative matters, including unforeseen administrative issues or problems, provided that doing so is consistent with the decisions we reach in the *Report and Order*.

47. The record does not include a detailed cost/benefit analysis that would allow us to quantify the costs of compliance for small entities, including whether it will be necessary for small entities to hire professionals to comply with the adopted rules. However, as program participation by applicants and service providers is voluntary, and we expect that Pilot participants will carefully weigh the benefits, costs, and burdens of participation to ensure that the benefits outweigh their costs. We expect that there may be additional benefits that cannot be easily quantified, such as a reduction in learning downtime caused by cyberattacks, reputational benefits from increased trust in school and library systems, increased digital and cybersecurity literacy among students and staff, and the safeguarding of intellectual property. This limited Pilot Program will enable the Commission to evaluate the benefits of using universal service funding to fund cybersecurity services and equipment against the costs before deciding whether to support it on a permanent basis.

F. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

48. The RFA requires an agency to provide, "a description of the steps the agency has taken to minimize the significant economic impact on small entities…including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected."[145]

49. In the *Report and Order,* we take multiple steps that minimize economic impact on small entities related to the final rules we adopt. We have sought to minimize economic impact on eligible small schools, libraries and consortia by dividing the process of completing the application form for participation in the Pilot (FCC Form 484) into two parts. By requiring that an applicant only complete the first part of the application form, which seeks more general information, with their initial application (i.e., prior to our decision about whether to approve the entity as a participant in the Pilot), we minimize the economic impacts associated with filling out the second part of the form in at least two ways. First, applicants that are not selected for participation in the Pilot will never be required to fill out the second portion of the form. Second, applicants that are selected will have additional time to gather and prepare their answers, as compared to an alternate approach where we could have required that the entire form be completed with the initial application.

50. We have also significantly minimized economic impacts on eligible small schools, libraries, consortia and service providers by modeling the Pilot processes and forms, including those related to competitive bidding, requests for services, and invoicing and reimbursement processes, on existing E-Rate and ECF processes and forms. This includes submitting applications using the Pilot portal on USAC's website. We expect this action will meaningfully reduce any economic impact on small entities associated with completing information requested via these forms. First, we expect that many small entity participants, including their potential consultants and advisors, and service providers will be familiar with the substance of the forms from their involvement with the Commission's E-Rate and ECF processes and forms. Second, we expect that even those small entities that may not be involved

[145] 5 U.S.C. § 604(a)(6).

with the E-Rate and ECF programs may benefit from the significant guidance and information that the Commission and USAC have issued over the years in those programs (e.g., trainings and instructions materials), that could also be relevant to the Pilot, including future guidance the Bureau will provide about the Pilot Program requirements through a Public Notice. Third, we expect that these forms will generally be easy to use and efficient to complete based on our observation, made over many years, that forms with similar substance have proven effective in the Commission's E-Rate and ECF programs. We thus expect our actions will significantly minimize any economic impact on small entities compared to an alternative approach where we developed Pilot processes and forms that were not related to those already developed in the Commission's E-Rate and ECF programs.

51. We have also designed our reporting requirements to minimize the economic impact on small entities while ensuring that we gather the information necessary to achieve the goals and ensure the success of the Pilot. In particular, have required only annual reporting from participants during the duration of the Pilot rather than alternate approaches where we could have required either per-incident "real-time" reports based on the occurrence of certain notable cyber events or regular but more frequent (e.g., quarterly) reporting. To further reduce economic impacts on small entities we have also directed the Bureau to consider the development of a standardized reporting form for use by Pilot participants.

52. Additionally, we have also delegated authority to the Bureau and USAC to address and resolve a number of matters, including unforeseen administrative issues or problems, provided that doing so is consistent with the decisions we reach in the *Report and Order*. We expect that that these delegations of authority will permit the Bureau and Administrator to take procedural actions, based on their experience gained managing the Pilot Program, to further reduce, wherever possible, economic impacts on small entities while still ensuring that all Pilot Program goals are effectively and efficiently satisfied.

53. We also will not require the use of specific federal government tools and resources in the Pilot as initially suggested in the *Cybersecurity NPRM*. Further, while several commenters support a shortened Pilot duration of either one year or eighteen months, we adopt our proposed three-year Pilot Program because it will allow us a better opportunity to evaluate whether universal service support should be used to fund cybersecurity services and equipment on a permanent basis. In determining the share of costs, participants will use their category one discount rate to determine the non-discount share of costs, instead of the category two discount proposed in the *Cybersecurity NPRM*, allowing participants with the highest discount rate to be eligible for support for 90 percent of their costs.

54. We considered, but declined to adopt, proposals to abandon the traditional E-Rate reimbursement structure and instead provide "seed" money at the start of the Pilot, because requiring participants to contribute their funds toward eligible equipment and services helps to safeguard the integrity of the program and is consistent with processes in E-Rate and other universal service programs. However, for the Pilot, we modify the time to request appeal and waiver of an action by USAC to 30 days instead of the 60-day timeframe in the existing programs. Though commenters assert this will limit flexibility for participants, we think the change is appropriate for the Pilot Program because it will allow for faster decisions in a program that has a limited duration.

G. Report to Congress

55. The Commission will send a copy of the *Report and Order*, including this FRFA, in a report to Congress pursuant to the Congressional Review Act.[146] In addition, the Commission will send a copy of the *Report and Order*, including the FRFA, to the Chief Counsel for Advocacy of the SBA. A copy of the *Report and Order* and FRFA (or summaries thereof) will also be published in the *Federal Register*.[147]

[146] *Id.*. § 801(a)(1)(A).

[147] *Id*. § 604(b).