FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 54

[WC Docket No. 23–234; FCC 24–63; FRS ID 230286]

Schools and Libraries Cybersecurity Pilot Program

AGENCY: Federal Communications Commission.

ACTION: Final rule.

SUMMARY: In this document, the Federal Communications Commission (Commission or FCC) stablishes the Schools and Libraries Cybersecurity Pilot Program (Pilot or Pilot Program). The Pilot Program will enable the Commission to evaluate the impact that using Universal Service Fund (USF or Fund) support for eligible cybersecurity services and equipment will have on protecting school and library broadband networks and data. In so doing, the Commission seeks to address the apparent needs of schools and libraries for additional support for cybersecurity services and equipment, while evaluating the impact that providing that support would have on the USF.

DATES: Effective August 29, 2024, except for amendatory instruction 3 (adding §§ 54.2004, 54.2005, and 54.2006) and amendatory instruction 4 (adding § 54.2008), which are delayed indefinitely. The Commission will publish a document in the **Federal Register** announcing the effective date for those sections.

FOR FURTHER INFORMATION CONTACT: Kristin Berkland *Kristin.Berkland@fcc.gov* in the Telecommunications Access Policy Division, Wireline Competition Bureau, 202–418–7400 or TTY: 202–418–0484. Requests for accommodations should be made as soon as possible in order to allow the agency to satisfy such requests whenever possible. Send an email to *fcc504@fcc.gov* or call the Consumer and Governmental Affairs Bureau at (202) 418–0530.

SUPPLEMENTARY INFORMATION: This is a synopsis of the Commission's Schools and Libraries Cybersecurity Pilot Program, Report and Order (Order), in WC Docket No. 23–234; FCC 24–63, adopted June 6, 2024, and released June 11, 2024. The full text of this document is available at the following internet address: *https://www.fcc.gov/document/fcc-adopts-200m-cybersecurity-pilot-program-schools-libraries-0.*

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 Commission adopts a three-year pilot program within the USF to provide up to $200 million to support cybersecurity services and equipment for eligible schools and libraries.

2. The 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, the Commission notes that other Federal partners, including the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Department of Education (Education Department), have jurisdiction and deep expertise on cybersecurity matters, and the Commission expects 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 the Commission is able to select a large number of participants for the Pilot Program, it adopts per-student and per-library budgets, subject to a minimum funding floor, as well as an overall funding cap. Additionally, the Commission expects 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, the Commission expects to gain a better understanding about the cybersecurity needs of a wide range of schools and libraries.

4. In adopting this Pilot Program, the Commission is also mindful of the E-Rate program's longstanding goal of promoting connectivity, as well as its obligation to be a mindful and prudent steward of the Commission's limited universal service funds. To that end, the Commission must balance its 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. The Commission acknowledges 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. The Commission notes that the estimated costs for all types of cybersecurity services may exceed the funding available for this Pilot Program, and it further notes 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, the Commission finds that the Pilot Program will serve a vital role in informing the Commission, and the 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. Discussion

5. In the Order, the Commission establishes 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 access 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 Telecommunications Act of 1996 (1996 Act). Specifically, the Commission first adopts a three-year Pilot timeframe and $200 million cap to support cybersecurity services and equipment, including advanced firewalls, for eligible schools and libraries, and consortia of eligible schools and libraries, using the Connected Care Pilot Program as a model. Second, the Commission establishes 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, the Commission confirms 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. The Commission then adopts 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 it can select a broad pool of participants. In addition, the Commission establishes 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 its experience administering the E-Rate and Emergency Connectivity Fund (ECF) programs and will promote efficient program administration and reduce burdens on Pilot participants. The Commission also appoints 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 its responsibility to be a careful steward of the limited USF dollars. The Commission then adopts 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, the Commission concludes 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.

6. Pilot Program Timeframe. The Commission first adopts a Pilot Program duration of three years. In the *Cybersecurity Notice of Proposed Rulemaking (NPRM),* 88 FR 90141, December 29, 2023, the Commission sought comment on its proposed three-year term for the Pilot Program. The Commission sought comment specifically to understand whether (i) the proposed length of the program would be sufficient to provide the Commission with data to evaluate how effective the Pilot funding is in protecting K–12 schools and libraries, and their broadband networks and data, from cybersecurity threats and attacks; (ii) if it would be feasible to shorten the Pilot without compromising the integrity of the data collected; and (iii) if it 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.

7. While several commenters support the proposed Pilot duration of three years, many advocated for a shortened Pilot duration of either one year or eighteen months. 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. 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 (*i.e.,* funding years (FY) 2026 through FY 2030). 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. Finally, commenters recommended a shorter Pilot term or, alternatively, a higher cap, in order to increase the number and diversity of participants.

8. A three-year Pilot Program will give the Commission the time to evaluate whether universal service support should be used to fund cybersecurity services and equipment on a permanent basis and the Commission adopts 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 [would] allow the Commission to obtain sufficient, meaningful data from the selected pilot projects'' and the Commission finds the same reasoning applies here. As a responsible steward of the limited USF, the Commission is obliged to carefully evaluate any actions that would expand demands on the Fund. This is particularly important where, as here, the Commission is 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, the Commission thinks 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. The Commission believes that a three-year term will enable us to gather the necessary information.

9. The Commission recognizes 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, the Commission declines 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. Moreover, the Commission notes 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, the Commission disagrees with commenters that a three-year term would render any potential solutions or analysis obsolete. Given the flexibility the Commission provides to Pilot participants to select and modify the cybersecurity services and equipment they choose over the three-year period, the Commission expects 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 adopted herein, the Commission expects to keep pace with lessons learned from the Pilot as data is provided which, in turn, will help facilitate its analysis and determination of next steps. Finally, the Commission disagrees with commenters who suggest it shorten the Pilot term or allocate additional funding in order to fund a greater or wider array of participants. The Commission believes the $200 million cap will allow it 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.

10. *Pilot Program Cap.* The Commission also adopts a Pilot Program funding cap of $200 million over three years for the Pilot Program. In the *Cybersecurity NPRM,* the Commission 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.

11. Several commenters agree that the proposed $200 million funding cap is sufficient to fund a wide range of Pilot participants over a three-year period. Others suggested a higher amount in order to provide funding to a larger number of Pilot participants. Having reviewed the record in its entirety, the Commission adopts the proposed $200 million funding cap for the Pilot Program. For its 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 in the Order, the Commission believes the proposed cap of $200 million over three years will be sufficient.

12. To provide funding for the Pilot, and to minimize the impact on the contribution factor, the Commission will assign unused E-Rate funds from prior funding years to cover the full $200 million cap. In 2023, the Wireline Competition Bureau (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. Similarly, in 2024, the Bureau directed USAC to reserve $10 million of the available $500 million of carry forward funds for future use. With the Order, the Commission assigns that $200 million of carry forward funding to offset the collection requirements for the Pilot, thereby reducing any potential increase on the contribution factor. In the *Cybersecurity NPRM,* the Commission sought comment on other approaches that could be used to fund the Pilot, aside from directing USAC to separately collect the needed funds. No commenter addressed these approaches. Making use of carry forward funding in this way is consistent with its responsibility to be a careful steward of the USF, while at the same time allowing 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.

13. The Commission next adopts fixed per-student and per-library budgets to determine the amount of funding that participants may receive during the Pilot. In the *Cybersecurity NPRM,* the Commission sought comment on how to evaluate funding requests and whether to establish a maximum amount of funding that an individual participant could receive. Among other things, the Commission 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. In particular, the Commission sought comment on whether it 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. Additionally, the Commission sought comment on whether it should require Pilot participants to contribute a portion of the eligible costs of cybersecurity services and equipment in order to receive funding. The Commission 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 comment on requiring participants to instead contribute a fixed percentage of the costs of the cybersecurity services and equipment purchased. Finally, the Commission 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.

14. A 2021 cost study submitted jointly by Funds For Learning, LLC (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. 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. Based on its review of the cost estimates submitted by commenters, and consistent with its goal to provide funding to a wide variety of participants, as discussed in the Order, the Commission adopts fixed budgets to determine the amount of funding that a Pilot participant can receive. While these budgets, including associated maximums and floors, are specified in terms of annualized dollar amounts, participants' expenses are capped based on the full three-year duration of the Pilot and not on an annual basis. Thus, Pilot participants may request reimbursement for expenses as they are incurred even if it means that the amount of funding disbursed to a participant in a given year of the program exceeds their annual budget, so long as the total amount disbursed to a participant over the three-year term does not exceed three times that annual budget. In establishing these budgets, which account for the estimated costs of different types of advanced cybersecurity solutions, the Commission expects to provide a meaningful benefit to a substantial number of schools, libraries, and consortia. In

implementing this approach, the Commission declines to award support based on a percentage of a participant's category one or category two budget, as suggested by some commenters. The Commission finds that a more tailored approach, grounded in the estimated cost of implementing specific types of cybersecurity solutions, would best achieve its goals in a targeted and cost-effective manner. Furthermore, the Commission notes that because it does not limit Pilot participation to current E-Rate applicants, it would be difficult to implement an approach based on category one or category two budgets. When implementing these budgets, the Commission will categorize Pilot applicants and consider their funding needs in combination with their applicant type, as discussed in greater detail below.

15. *Schools and School Districts.* Schools and school districts will be eligible to receive up to $13.60 per student, annually, on a pre-discount basis, to purchase eligible cybersecurity services and equipment over the three-year Pilot duration. The Commission finds that a pre-discount annual budget of $13.60 per student strikes an appropriate balance between supporting the various types of cybersecurity services and equipment needed to protect school networks and data, and its desire to provide funding to as many schools and school districts as possible in the limited-term Pilot Program. Additionally, the Commission notes that this per-student annual budget is sufficient to support the majority of the total annual costs related to any one of the three types of security measures FFL and CoSN identified in their cost estimate, and is also consistent with the Commission's analysis in the *First 2014 E-Rate Order,* 80 FR 167, January 5, 2015, that established per-student budgets for category two equipment and services.

16. The Commission recognizes that for many schools a pre-discount annual 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. Given the limited Pilot funding available, its approach instead ensures that each participating school will receive funding to prioritize implementation of solutions within one major technological category requested by commenters, enabling the school to make meaningful progress toward its own cybersecurity goals and providing flexibility for schools with differing cybersecurity strengths and vulnerabilities. The Commission finds 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. The Commission also finds that this approach represents a strategic and cost-effective way to spend the 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.

17. Schools and school districts selected for the Pilot Program will be eligible to receive, at a minimum, $15,000 in annual support, on a pre-discount basis, over the three-year Pilot duration. The Commission establishes 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. The Commission sets the annual funding floor at $15,000, pre-discount, because it aligns with the annual cost estimate submitted by FFL and CoSN, which found that that the approximate per-site annual cost for advanced firewalls is $15,994. The Commission notes 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 pre-discount $15,000 annual funding floor. The Commission also establishes an annual budget maximum of $1.5 million, pre-discount, 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 annual budget maximum of $1.5 million, over the three-year Pilot duration. The Commission finds that a $1.5 million annual maximum reflects the greater purchasing power of larger schools, school districts, and consortia, and the associated reduction in the cost-per-student amount. Additionally, the Commission establishes the annual budget maximum to best ensure that Pilot funds are able to support cybersecurity services and equipment for as many participants as possible, and also to ensure that a disproportionate amount of funding is not awarded to any one participant.

18. *Libraries and Library Systems.* Rather than adopt a per-user budget, as the Commission has for schools and school districts, or a budget based on library square footage as it does for category two E-Rate funding requests, it adopts a budget that provides a set amount of funding per library to purchase cybersecurity services and equipment. In particular, the Commission establishes a pre-discount annual budget of $15,000 per library up to 11 libraries/sites, consistent with its analysis regarding the per-site funding amount needed to support advanced firewalls. Library systems with more than 11 libraries/sites will be eligible for support up to $175,000 annually, pre-discount, which approximately reflects the cost of providing advanced firewalls to an entity with between 10 and 24 locations. The Commission believes using a per-site methodology and funding caps for calculating library budgets is more appropriate than using library square footage, as it does 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. The Commission also finds 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 as many participants as possible.

19. *Consortia.* Consortia participants comprised of eligible schools and libraries will be eligible to receive funding based on student count (using the annual pre-discount $13.60 per student multiplier and $1.5 million, pre-discount, annual cap) and the number of library sites (using the pre-discount $15,000 per library annual budget up to 11 libraries/sites and the $175,000, pre-discount, annual cap). Consortia that are solely comprised of schools will be subject to the pre-discount annual $1.5 million budget maximum applicable to schools. Consortia that are solely comprised of libraries will be subject to the pre-discount $175,000 annual budget maximum for library systems. Consortia comprised of both eligible

schools and libraries will be subject to the pre-discount $1.5 million annual budget maximum applicable to schools. The Commission finds these budget maximums are an important mechanism to ensure that Pilot funding is widely disbursed. The Commission will also require each consortium to select a consortium leader.

20. *Non-discount Share of Costs.* The Commission 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. The Commission agrees with the Dallas Independent School District that requiring participants to contribute some portion of the costs of eligible services and equipment, as it has in E-Rate, will be ''successful in aligning the interests of applicants to minimizing waste, fraud, and abuse.'' In the *Cybersecurity NPRM,* the Commission proposed using a participant's category two discount rate to determine the portion of costs a participant will be required to contribute. The Commission establishes in the Order, 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 its 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. The Commission finds that this approach is preferable to establishing a uniform contribution percentage like the one adopted for the Connected Care Pilot Program 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.

21. *Disbursement of Support.* The Commission will permit Pilot participants to request reimbursement as expenses are incurred, even if it means that a greater amount of funding is disbursed earlier in the three-year Pilot term than is specified by its annual budgets, so long as the overall disbursement to a participant over the course of the three-year Pilot term does not exceed three times the annual budget. In doing so, the Commission acknowledges 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, or some combination of both. The Commission agrees with Cisco that it should not adopt a ''static'' funding approach, as well as with Palo Alto Networks, Inc. that a flexible approach would ''ensure a stronger runway for the deployment and configuration of eligible solutions and products under the Pilot.'' However, the Commission declines to adopt the recommendation of Advanced Technology Academic Research Center Cybersecurity Higher Education and Workforce Development Working Group that it abandon its traditional reimbursement structure to provide ''seed'' money at the outset of the Pilot. The reimbursement process the Commission adopts here is consistent with the reimbursement processes used in the E-Rate and other universal service programs 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 the Commission is mindful of the importance of establishing a predictable cap that minimizes the contribution burden on consumers, it expects that the limited nature of the Pilot cap relative to the overall size of the Fund, as well as its planned use of the reserved $200 million in carry forward funding, will minimize any burden to the overall Fund for any given quarter.

22. *Pilot Benefits will Exceed Costs.* The Commission expects the benefits of the Pilot Program to exceed the costs. As a threshold matter, the Commission notes that program participation by applicants, participants, and service providers is voluntary, and it expects 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, the Commission notes 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. 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. The Pilot Program caps support at a pre-discount, annual level of $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. The Commission expects 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 school staff, and the safeguarding of intellectual property. Despite these benefits, the Commission is also concerned about the overall cost to the Fund if it were to provide cybersecurity funding to all E-Rate participants, which CoSN estimates could cost the Fund $2.389 billion annually. 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.

23. The Commission next make eligibility for participation in the Pilot Program open to all eligible schools and libraries, including those that do not currently participate in the E-Rate program. In the *Cybersecurity NPRM,* the Commission sought comment on the types of entities that should be eligible to participate in the Pilot Program. The Commission 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. Specifically, the Commission 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. The Commission proposed to adopt the same definitions for schools and libraries as used in the E-Rate

program, when determining the eligibility of Pilot participants.

24. 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. For example, 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.'' Several commenters urged the Commission to make consortia eligible, consistent with the E-Rate program. These commenters noted that consortia ''can provide valuable services at scale,'' which would allow the Commission to ''stretch the limited proposed Pilot funding and increase the impact to more students and schools.'' Others suggested that it expand eligibility to include local and other government entities and Educational Service Agencies (ESAs).

25. The Commission has determined that it 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. The Commission adopts the definitions of elementary school, secondary school, library, and library consortium contained in Final Rules section of the Order, which mirror the definitions that it uses for the E-Rate program. In taking these steps, the Commission declines to adopt suggestions from commenters that it limit Pilot eligibility to only those schools and libraries that currently participate in the E-Rate program. The Commission observes 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 the Commission appreciates the concern raised by NCTA and others that the Pilot should focus on protecting E-Rate-funded networks, it believes that, on balance, opening the Pilot Program to a wider pool of participants would best ensure that it has 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, the Commission anticipates that the overwhelming majority of Pilot participants will also be E-Rate participants.

26. Consistent with the Commission E-Rate rules, it further clarifies that it will also permit eligible schools and libraries that apply as a consortium to participate in the Pilot Program. The Commission agrees with commenters that consortia have buying power that can help bring down costs and that including consortia in the Pilot would allow larger, better-resourced schools and libraries to partner with smaller, less technically savvy participants. Given the limited funding for the Pilot Program and the Commission's objective to select as many participants as possible, it will allow a school or library to apply and participate only once in the Pilot Program, either individually or as part of a consortium. The Commission declines 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 § 54.2000 of the Commission's rules adopted. 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 as in the Rural Health Care, E-Rate, and Connected Care Pilot programs, will 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. While the Commission recognizes 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). As its legal authority for the Pilot stems from the same source, the Commission declines to expand Pilot eligibility to include governmental and other entities that would be ineligible under the E-Rate or Rural Health Care programs; however, it recognizes the expertise and value of these entities by allowing them to serve as ineligible consortium leaders that pass through the benefits, discounts, and support from the Pilot Program to their eligible school and library consortium members. The Commission directs the Bureau and USAC to provide additional training and guidance on creating a Pilot consortium and serving as a consortium leader in the Pilot. The Commission also directs the Bureau and USAC to establish measures to prevent eligible schools and libraries from receiving duplicative Pilot support as individual Pilot participants and as Pilot consortium members.

27. The Commission adopts a Pilot Eligible Services List (P–ESL) which specifies eligible cybersecurity services and equipment for the Pilot. In the *Cybersecurity NPRM,* the Commission sought comment on the ''equipment and services . . . that should be made eligible to participants in the Pilot'' and on whether it should specify eligible services and equipment using ''general criteria'' or a ''list of specific technologies.'' Based on the record, the Commission adopts a flexible approach for the P–ESL as it 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.'' At the same time, the Commission provides 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 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, the Commission provides a non-exhaustive list of examples of eligible services and equipment in the P–ESL. Through the list of examples, the Commission confirms that the wide range of services and equipment it had proposed for inclusion in the *Cybersecurity NPRM,* or that commenters had otherwise requested, are eligible. The Commission designates the eligible services and equipment for the duration of the Pilot through the P–ESL. The Commission also delegates authority to the Bureau, as needed, to clarify and make technical changes to the P–ESL consistent with the standards it established herein, to promote efficient program administration and account for technological evolution.

28. The Commission agrees 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. Its approach is consistent with Rubrik's view that it ''provide general guidance for applicants, but not lock them into specific technology products.'' Its 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. At the same time, by enumerating four non-limiting categories of eligible technology, the Commission finds that its approach also meets the recommendations of commenters that it ''establish general categories of eligible offerings'' without ''specify[ing] the precise technologies or solutions that must be relied upon'' and allow ''[p]ilot participants to select any product and/or services that fall into any of the eligible categories.'' Its 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 the extent to which any of these specific measures would be most cost-effective for them to implement. While the Commission declines to make these or other Federal recommendations the sole basis for determining eligibility for the purposes of the Pilot, it strongly encourages 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. The Commission directs the Bureau to identify these Federal recommendations, and it directs 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. The Commission further directs the Bureau and USAC to periodically update the information provided on their respective websites and in the training materials to reflect relevant updates to the recommendations that may issue during the duration of the Pilot.

29. The Commission finds 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. The Commission further finds that its approach, in which it declines 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 cybersecurity threats and attacks. Its 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, the Commission makes eligible both the specific services and equipment identified in the P–ESL, as well as ones that have ''substantially similar features or their equivalents.'' The Commission also makes eligible security updates and patches, which will help to ensure that participants are protected even as threat vectors evolve over the course of the Pilot. The Commission finds 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. Finally, consistent with the flexible approach the Commission adopts, it clarifies that applicants are permitted to seek funding for multi-year licenses for eligible recurring services that are longer than three years, however, only services delivered within the Pilot Program period can be reimbursed using Pilot funds. Similarly, the costs of eligible services that will be incurred during the Pilot Program period are eligible, subject to compliance with procurement requirements and limitations on duplicative funding, even if prior years' costs were paid with another funding source.

30. The Commission further finds its 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. Moreover, its 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.

31. The Commission clarifies that its inclusion of a given technological category, equipment, or service in the P–ESL and/or any subsequent determination by the Bureau that a specific piece of equipment or service is eligible in the Pilot Program, is not an endorsement by the Commission, the Bureau, 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, the Commission expects participants to select equipment and services from among those that are eligible based on their own assessments of cost-effectiveness in addressing their specific needs. Accordingly, a participant may not rely on eligibility determinations made by the Commission or the Bureau in the Pilot as a defense or safe harbor should it experience a cyber incident, including a breach, a data loss, or other harm. Moreover, the Commission clarifies that the services and equipment listed in the 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. The Commission finds this clarification appropriate to ensure that it can satisfy the statutory purpose of the E-Rate program, as well as its goal of measuring the costs associated with cybersecurity services and equipment. The Commission also declines to limit eligible services and equipment for the Pilot to those that are used on E-Rate-funded broadband networks only. The Commission finds this step reasonable given that Pilot participants are not limited solely to current applicants in the E-Rate program.

32. In the *Cybersecurity NPRM,* the Commission 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. The Commission adopts this proposal to enable Pilot participants to protect their networks from outside cyber attackers by blocking malicious or unnecessary network traffic. For purposes of the Pilot, the Commission defines 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.'' This definition is reflected in the P–ESL.

33. The Commission agrees 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 it studies the potential use of universal service funding to protect eligible schools and libraries from cybersecurity threats and attacks. The Commission

also agrees 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. 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.'' The Commission disagrees 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 technologies, and it finds 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. The Commission further finds 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.

34. However, the Commission does agree that funding some level of training will help to ensure that the Pilot-funded equipment and services are used effectively and for maximum benefit. Accordingly, it makes training eligible on terms similar to those in E-Rate, namely, when the training is 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.'' The Commission finds that this approach balances the need to ensure that applicants have access to training that will enable them to effectively oversee, utilize, and supervise the use of 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, 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, it does not require that the training be provided ''[o]n-site'' to be eligible. The Commission finds 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. The Commission notes that there are numerous free cybersecurity training resources already available through its Federal Government partners. The Commission also expects, based on its 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.

35. The Commission also clarifies that for the purposes of the Pilot Program eligibility rules that ''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. Its approach reflects a definition of the term ''firewall'' endorsed by the National Institute of Standards and Technology (NIST) with a carve out for services and equipment that are already funded through the E-Rate program. The Commission finds it is appropriate to adopt a broad definition as this is consistent with its objective to determine the technological benefits and monetary costs associated with a wide and diverse range of tools for addressing cybersecurity threats and attacks. At the same time, the Commission finds it reasonable to exclude from its definition basic firewall services and equipment that are currently funded through the E-Rate program. The Commission finds 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. The Commission further finds that its 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. To further address commenter views, and as reflected in the P–ESL, the Commission confirms 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, virtual private network (VPN), Domain Name System (DNS) security, distributed denial-of-service (DDoS) protections, and content filtering technologies, are eligible for the Pilot.

36. The Commission declines 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, that it immediately makes advanced and/or next-generation firewalls eligible in the E-Rate program, even as it continues to study the benefits and costs of other services and equipment through the proposed Pilot. Making advanced and/or next-generation firewalls immediately eligible in the E-Rate program would run directly counter to its proposed purpose of the Pilot Program 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.'' 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.'' The Commission finds it reasonable, and consistent with its obligations to be a careful steward of the 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.

37. Next, the Commission makes 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 that connect to their networks. For the purposes of the Pilot, the Commission defines 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 cybersecurity threats and attacks.'' This definition is reflected in the P–ESL.

38. The Commission agrees with the many commenters who argue for the inclusion of the specific endpoint technologies that it makes eligible. The Commission also agrees 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. The Commission finds that its 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. Moreover, the Commission finds 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. No commenter objects to the Pilot funding endpoint protection. The Commission further finds that its 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.

39. The Commission also makes 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. 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, the Commission defines 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.'' This definition is reflected in the P–ESL.

40. The Commission agrees with the large number of commenters who argue for the inclusion of the specific identity protection and authentication technologies that it makes eligible. The Commission also agrees 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. No commenter objects to the Pilot funding identity protection and authentication technologies. Moreover, the Commission finds that its 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.

41. The Commission further makes 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. For purposes of the Pilot, the Commission defines 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.'' This definition is reflected in the P–ESL.

42. The Commission agrees with the large number of commenters who argue for the inclusion of the specific monitoring, detection, and response technologies that it makes eligible. The Commission also agrees with commenters who advocate for the inclusion of these services and equipment as an important approach to remediating cybersecurity threats and attacks, particularly given the limited resources of schools/libraries to hire or retain staff or other personnel to conduct these activities themselves. No commenter objects to the funding of network monitoring, detection, and response solutions.

43. The Commission imposes a number of limitations on eligibility to ensure the efficient and appropriate use of the limited Pilot funds, and to avoid duplicative funding, protect against waste, fraud, and abuse, and stretch the limited support available through the Pilot. First, the Commission makes ineligible for the Pilot funding any services, equipment, or associated cost that is already eligible through the E-Rate program. The Commission similarly makes 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. Participants may, however, use Pilot funding to support Pilot-eligible services and equipment that participants were previously paying for themselves, subject to its 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. The Commission finds 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, the Commission requires 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.

44. In the *Cybersecurity NPRM,* the Commission 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.'' The Commission adopts this proposal in the P–ESL with a clarification that ''network-based'' services include those that are cloud-based and server-based. In doing so, the Commission address concerns raised by some commenters by confirming that the term ''network-based'' solutions includes both cloud and server-based solutions. The Commission finds this clarification appropriate since both servers and cloud architectures are used in conjunction with a network.

45. In taking this action, the Commission disagrees with the view expressed by Clark County School District (CCSD) that limiting eligibility in the way it had proposed would ''not go far enough in protecting end-users.'' Contrary to CCSD's views, the Commission's consideration for eligibility specifically encompass ''end-user devices, where the devices are owned or leased by the school or library.'' The Commission also disagrees

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.'' While the Commission is sympathetic to this view on a technical level, it finds it administratively and financially impractical to expand eligibility to an even larger (and unknowable) number of additional devices that students, school staff, and library patrons may seek to connect to their networks over the duration of the Pilot Program. For purposes of the Pilot, the Commission 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. The Commission's 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 Pilot Program rules. 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. The Commission thus finds that its 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 its 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,* the Commission adopts its proposal as clarified.

46. To further protect the Pilot's limited funds, the Commission restricts eligibility in a number of ways. The Commission deems 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 the limited USF funds. The Commission expects that this action will provide similar benefits in the context of the Pilot. The Commission similarly deems ineligible insurance costs and any costs associated with responding to specific ransom demands. The Commission finds 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 it can gain maximum insight into the technical effectiveness of those offerings. The Commission finds it reasonable to exclude these enumerated uses from the Pilot, which has even more limited funding available as compared to the E-Rate program.

47. In the *Cybersecurity NPRM,* the Commission sought comment on ''whether it 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.'' The Commission 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. Accordingly, the Commission confirms that Pilot participants may request reimbursement for one-time purchases, as well as the recurring costs of eligible security measures. As discussed in this proceeding, 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 as well as funding commitments.

48. *Supply Chain Restrictions.* In the *Cybersecurity NPRM,* the Commission 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. The Commission also sought comment on whether ''there are any other restrictions or requirements that it 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.'' The Commission adopts its 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 §§ 54.9 and 54.10 of the Commission's rules, that implement the Secure and Trusted Communications Networks Act. Accordingly, Pilot participants are prohibited by § 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,'' including Huawei Technologies Company and ZTE Corporation, and their parents, affiliates, and subsidiaries. Pilot participants are also prohibited by § 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. The Commission notes 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. 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. The Commission finds 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, and no commenter opposes it.

49. *Application Process for Pilot Program.* The Commission adopts 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 of the Pilot Program. In the *Cybersecurity NPRM,* the Commission proposed to structure the Pilot Program in a manner similar to the Connected Care Pilot Program. In particular, the Commission 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. The Commission 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. The Commission further proposed that USAC be appointed the Administrator of the Pilot Program. Two commenters specifically expressed support for its proposal to structure the Pilot in a manner similar to the Connected Care Pilot Program. Only one commenter, the American Library Association (ALA), addressed its proposal that USAC be appointed the Administrator of the Pilot Program, agreeing that the application process and other aspects of the Pilot Program should be administered by USAC.

50. The Commission also proposed in the *Cybersecurity NPRM* that entities interested in participating in the Pilot be required to submit a 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. While there was minimal opposition to the collection of general information, 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. Still others recommended that applicants not be required to provide details regarding their cybersecurity postures, network environments, or current protection measures (or lack thereof). Several commenters recommended that the FCC Form 484 application process be minimally burdensome, and a few commenters recommended that it align with E-Rate tools and concepts that are familiar to E-Rate applicants wherever possible.

51. Finally, The Commission 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. The Commission also asked how it could best leverage its prior experience in other USF and congressionally-appropriated programs and sought comment on lessons learned. For administrative efficiency, the Commission 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. The Commission 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. 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. Comments related to past experience and lessons learned focused on the requests for reimbursement and invoicing processes, are discussed in the Order. Many commenters supported the Commission's legal authority to conduct the Pilot Program, 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.

52. Based on the record, the Commission adopts several of the proposals from the *Cybersecurity NPRM.* Specifically, the Commission adopts the application, selection, and administrative proposals, and it designates USAC to be the Administrator of the Pilot. In doing so, the Commission is 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. To that end, 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 selected as Pilot participants. The Commission 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.

53. 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. 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. The Commission anticipates 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, the Commission expects 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.

54. *Part One Application Information.* For the first part of the FCC Form 484 application, the Commission directs 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.
- 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)), whether the applicant has experienced a cybersecurity incident within a year of the date of its application (answered on a yes/no basis), and 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 best practices 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, particularly those with minimal or no cybersecurity protections today, the Commission anticipates 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. Similarly, and addressing concerns expressed by ActZero, the Commission encourages participation in the Pilot by a broad range of service providers and note that the rules and requirements it adopts here do not discourage new companies from participating. Nor does it 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.

55. 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 10 years; and, if audited, it will produce those records at the request of the appropriate officials. 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. The Commission emphasizes that it is 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.

56. While the Commission understands the desire by some commenters to keep the initial application as streamlined as possible, in order to evaluate the proposed Pilot projects and select well-defined and sustainable projects, it is incumbent on us to require certain information at the application stage. Thus, the Commission disagrees 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. 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, the 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. 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.

57. *Selection Process for Pilot Program.* To select Pilot participants, the Commission directs 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. In the *Cybersecurity NPRM,* the Commission sought comment on how to evaluate and prioritize Pilot applications. In particular, the Commission sought comment on what prerequisites, if any, the Commission should adopt to select participants. For example, it 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. 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. 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. No 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. Some commenters thought requiring Pilot participants to join cybersecurity information-sharing groups was too onerous, while others found such a requirement beneficial. 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, though at least one commenter expressed reservations about the Commission doing so. 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.'' Clear Creek Amana CSD (Clear Creek), however, cautioned against relying on Federal resources outside of a limited incident response plan following the NIST frameworks. 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. However, others called for selection based on a holistic view of an applicant's cybersecurity expertise and risk. 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. The Alliance for Digital Innovation (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 within organizations.''

58. The Commission 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, it 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*). The Commission 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. 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. 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. 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. Similarly, other commenters encouraged the Commission to enable school districts to work across district and community boundaries to participate in the Pilot Program.

59. For subjective Pilot selection factors, the Commission 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. Relatedly, the Commission also sought comment on how it could ensure that schools and libraries that lack funding, expertise, or are otherwise under-resourced could meaningfully participate in the Pilot. The Commission asked commenters to address whether Pilot participants should be required to demonstrate that they have started to take actions to improve their cybersecurity posture. Conversely, the Commission 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. Commenters generally agreed that the Pilot would most benefit from including participants with a mix of cybersecurity expertise and varying cybersecurity postures. 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, including providing technical and other assistance to those applicants who are likely to need it most. 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.

60. Along these same lines, the Commission 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. In particular, it 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 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. The Commission also asked what role, if any, cybersecurity risk, geographic or socioeconomic factors, staffing constraints or financial need, or technical challenges should play in Pilot participant selection. 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. 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.

61. The Commission agrees with commenters who support using a broad and objective set of evaluation factors to select Pilot Program participants. After reviewing the record, the Commission concludes 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 its 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 its goal of ensuring that the Pilot contains a diverse cross-section of applicants with differing cybersecurity postures and experiences. The Commission directs the Bureau to weigh these considerations during the Pilot application review and participant selection processes.

62. The Commission has considered commenters' suggestions regarding the potential application factors and have determined that the considerations outlined will provide us with meaningful information with which it can select Pilot projects and participants. The Commission acknowledges that commenters suggested it weighs other considerations, but it believes that the considerations listed best enable it 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.

63. The Commission directs the Bureau and USAC to review the applications and select Pilot projects and participants based on applicants' responses, weighing the considerations listed, in combination with the applicants' category one discount rates. 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. 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. The Commission declines to require Pilot applicants or participants to join information-sharing organizations like MS–ISAC, though it highly encourages all applicants or participants to do so. 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, and ensuring that the selected Pilot participants include schools and libraries that currently have limited cybersecurity protections. Although applicants' responses will be considered consistent with the considerations listed when evaluating proposed Pilot projects, the considerations are not determinative of whether a Pilot project will be selected because the Commission recognizes that each proposed Pilot project will have its own unique strengths and potential challenges. The Commission's 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 in the Order.

64. *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, the Commission directs 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. 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. 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 eligible services than those with lower levels of eligibility for such programs. The Commission's priority rules for the Pilot provide that funds shall be allocated first to requests for support at the 90 percent discount rate. 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. 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. 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. 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 and their funding prioritized consistent with the prioritization rules for the Pilot described in this paragraph. 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'' 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.

65. *Part Two Application Information.* For the second part of the FCC Form 484 application, the Commission directs the Bureau and USAC to collect more detailed cybersecurity information from applicants who are selected to participate in the Pilot Program. The Commission has 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. The Commission requires Pilot participants to provide such information to help establish a baseline that will enable it to effectuate the Performance Goals and Data Reporting discussed. 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, 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.
- 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.
- Information about a participant's planned use(s) for other Federal, state, or local cybersecurity funding (*i.e.,* funding obtained outside of the Pilot).
- Information about a participant's history of cybersecurity 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.
- A description of the specific Education Department or CISA cybersecurity best practices recommendations that the participant has implemented or begun to implement.
- 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.
- Information about any non-monetary or other challenges a participant may be facing in developing a more robust cybersecurity posture.

66. *Instructions for Filing Applications.* Iin order to facilitate the application process, the Commission plans 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. The Commission directs the Bureau to issue a Public Notice subsequent to the release of the 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, the Commission is only requiring more general information at the application stage of the Pilot. The more detailed, cybersecurity-related information will only be provided by Pilot participants. Some commenters have expressed concerns that this type of information is sensitive and could be used by malicious cybersecurity actors for nefarious purposes. The Commission agrees 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, the Commission will treat it as presumptively confidential under its rules and will withhold it from public inspection. The Commission further notes that FCC Form 484 data will be protected by security protections built into USAC's Pilot portal.

67. *Instructions for Establishing Application Schedule and Reviewing Applications.* The Commission delegates to the Bureau the authority to establish an application schedule consistent with the direction provided in the Order; review Pilot FCC Form 484 applications; and select Pilot projects and participants, doing so in an efficient and expedited manner. The Commission further directs 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. After selecting the Pilot participants, the Commission directs 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 submitting the second part of the Form 484 application, 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.

68. *Establishing an Application Filing Window.* To facilitate an efficient and equitable application review process, the Commission directs the Bureau to establish an application filing window, after which it will review applications from all eligible applicants by weighing the considerations discussed. Establishing a single filing window was well received by those commenters who addressed the proposal and opening a single window will allow the Bureau to review all applications before making selections. The Commission expects that adopting a single FCC Form 484 application filing window and proceeding in this manner will assist with its 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. To further assist under-resourced applicants, the Commission directs the Bureau and USAC to offer dedicated training and office hours for applicants and participants who are less experienced with cybersecurity services and equipment, or with the E-Rate and ECF program forms and processes.

69. The Commission next adopts 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. The Commission directs 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. In particular, the Commission expects the Bureau and USAC to leverage the following FCC forms for the Pilot 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). The Commission requires Pilot participants and service providers to make certain certifications on Pilot Program forms to protect the integrity of the Pilot. The Commission also requires 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, the Commission expects to save Pilot participants time needed to familiarize themselves with the new forms and reduce administrative cost and burden.

70. As in the E-Rate program, the Commission adopts 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, and 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. 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. Applicants begin the competitive bidding process by filing a completed E-Rate FCC Form 470 with USAC. USAC, in turn, posts the form on its website for potential competing service providers to review and submit bids. 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. 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.

71. In the *Cybersecurity NPRM,* the Commission proposed a competitive bidding process and rules for Pilot participants that mirror the existing E-Rate competitive bidding process and rules. 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, it concludes that its proposal is reasonable and adopts it here. To begin, the Commission adopts 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, the Commission adopts competitive bidding requirements modeled on § 54.503 of the Commission's rules, with which Pilot participants must comply to ensure they conduct an open and fair competitive bidding process. 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. 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. Finally, it includes a restriction on the receipt of gifts 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 competitive bidding process).

72. 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, the Commission declines 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. Likewise, the Commission declines to provide an exemption to competitive bidding for costs that Pilot participants may be currently cost-allocating in E-Rate funding requests for advanced firewall services. Similarly, because an open and fair competitive bidding process hinges on all bidders being on equal footing, the Commission also declines 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. Finally, to enable participants to select the services and equipment that best meets their needs, it clarifies, as SECA requests, that participants are permitted to require that the services or equipment to be purchased are interoperable with and/or compatible with existing services and equipment that have already been purchased.

73. The Commission does, however, establish a limited exemption to competitive bidding for Pilot participants who may be eligible to purchase services and equipment from master services agreements (MSAs) or their equivalent. Specifically, Pilot participants will not be required to seek competitive bids when seeking support for services and equipment purchased from MSAs negotiated by Federal, state, Tribal, or local governmental entities on behalf of such Pilot participants, if such MSAs were awarded pursuant to the E-Rate Form 470 process, as well as applicable Federal, state, Tribal, or local competitive bidding requirements. The Commission agrees with SECA that these MSAs or state master contracts are ''efficient contract vehicles'' and reflect

''cost-effective solutions for different components and different manufacturers.'' Pilot participants will be required to use the mini-bid process if required by the relevant MSA or state master contract. The Commission finds that this exemption, which was similarly included in the Connected Care Pilot Program, will enable Pilot participants to benefit from competitively bid state master contracts and MSAs, and in so doing, will streamline the competitive bidding process and minimize the burden on Pilot participants.

74. As proposed in the *Cybersecurity NPRM,* the Commission adopts the Pilot FCC Form 471, modeled after the E-Rate FCC Form 471, for Pilot participants and their service provider(s). In the E-Rate program, applicants file an FCC Form 471 to request discounts on eligible services and equipment for the upcoming funding year. The E-Rate FCC Form 471 requires detailed descriptions of the services and 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. 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 their E-Rate FCC Forms 471. 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). Following the issuance of the RAL, and after USAC conducts its 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.

75. Similar to the E-Rate program, Pilot participants must file a Pilot FCC Form 471 to request discounts on eligible services and equipment. 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 their costs and service dates; and certifications regarding compliance with Pilot rules. Pilot participants will be required to wait until the ACD to certify and submit the Pilot FCC Form 471. 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.

76. The Commission directs 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. During this application filing window, selected Pilot participants may submit their Pilot FCC Form(s) 471 to request eligible equipment and services that are needed to implement their Pilot project through the online system implemented by USAC. As the Commission is adopting forms, processes, and procedures that are used in the E-Rate and ECF programs, it expects 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. Pilot participants will be required to report on the progress of their Pilot projects and how the Pilot funding is being used to improve their cybersecurity postures throughout the three-year term, consistent with the annual reporting requirements discussed in the Order. The Commission further expects 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, the Commission delegates 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.

77. *Invoicing.* Consistent with the E-Rate program, and pursuant to the *Second Report and Order,* 68 FR 36931, June 20, 2003, the Commission permits both Pilot participants and service providers to submit requests for reimbursement using the Pilot FCC Forms 472 and 474, respectively. The Commission agrees 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. The Commission concludes 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. Consistent with E-Rate program rules, Pilot participants must be permitted to select the method of invoicing. For administrative simplicity, Pilot participants must also specify on their Pilot FCC Form(s) 471 whether the participant or the service provider will be conducting the invoicing for each funding request. 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. Requests for reimbursement must be submitted to USAC within 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.

78. *Invoicing Documentation.* As in the ECF program, to protect the integrity of the Pilot and protect against potential waste, fraud, and abuse, the Commission requires Pilot participants and service providers to submit, along with their reimbursement requests, invoices detailing the items purchased. Invoices must support the amounts requested and approved in the Pilot FCC Form 471 application. The Commission disagrees with Lumen Technologies, Inc. and NCTA that the submission of invoices with reimbursement requests would limit flexibility for Pilot participants and serves no purposes in this context. 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 the Commission 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 its 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, as well as retain and provide upon request by USAC, the Commission

(including Commission staff) and its Office of 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 10 years from the last date of service or delivery of equipment.

79. Consistent with the terms of the Memorandum of Understanding (MOU) between the Commission and USAC, and pursuant to the rules adopted, the Commission designates USAC as the Administrator of the Pilot Program. The Commission will use USAC's services to review, process, and approve the Pilot FCC Forms 470, 471, 472, 474, 484, and 488, as well as recommend funding commitments, issue FCDLs, review requests for reimbursement and invoices, and payment of funds, as well as other administration-related duties. The one commenter that directly addressed the issue supported using USAC and its processes for the efficient and effective administration of the Pilot Program, and the Commission agrees 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 the Commission notes that USAC may not make policy, interpret unclear statutes or rules relied upon to implement and administer the Pilot Program, or interpret the intent of Congress. In its administration of the Pilot Program, the Commission also directs 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, relevant provisions of the Federal Information Security Modernization Act of 2014, NIST publications, and Office of Management and Budget (OMB) guidance.

80. The Commission notifies 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. The Commission directs USAC to perform such audits pursuant to the Commission's and USAC's respective roles and responsibilities as set forth in the MOU and § 54.2011 of the Commission's rules. The Commission is 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. While it does 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, it notes that the Commission, USAC, and any contractors or vendors will be required to abide by all applicable Federal and state privacy laws. The Commission also directs 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. The Commission additionally delegates 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.

81. The Commission takes seriously its obligation to be a careful steward of the USF and to protect the integrity of the Pilot Program. The commission is committed to ensuring the integrity of the Pilot and will pursue instances of waste, fraud, or abuse under its own procedures and in cooperation with the Commission's OIG and other law enforcement agencies. The specific procedures the Commission adopts regarding document retention requirements, the prohibition on gifts, certifications, audits, suspension and debarment, and the treatment of eligible services and equipment are modeled after its E-Rate processes and are tools at its disposal to protect the Pilot and 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.

82. In the *Cybersecurity NPRM,* the Commission 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.'' The Commission adopts this proposal. Specifically the Commission includes a new § 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.'' The Commission also includes a new § 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 OIG, or any local, state, or federal agency with jurisdiction over the entity.'' This rule requires that Pilot participants must retain documents regarding participation in the Pilot, including asset and inventory records, accumulated during the Pilot, for a period of 10 years.

83. While commenters generally did not opine on these issues, the Commission finds that this new rule, § 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. The Commission finds that this new rule, § 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. The Commission finds its 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. The Commission also finds that the 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, the Commission finds 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 § 54.516 of the Commission's rules with only clarifying amendments reflective of the structure of the Pilot. The Commission has found the E-Rate rules to be effective over the course of its 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 document retention and production requirement, appropriately balance the need to have pertinent documentation available for review with corresponding administrative burdens and storage costs borne by E-Rate applicants and service providers. The Commission expects similar benefits to accrue in relation to the Pilot.

84. In balancing the longstanding goal of fair and open procurement with the disbursement of USF support for eligible equipment and services, the Commission adopts gift restrictions for the Pilot. Consistent with the E-Rate program, the Commission prohibits 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. 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.

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

86. *Duplicate Funding Certification.* The Commission confirms that it 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. No commenters opposed adopting this limitation to stretch the Pilot's limited funds. To implement this prohibition on requesting or receiving duplicative funding, the Commission 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. The Commission takes 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 are fully reimbursed through other sources, participants and service providers should not be seeking funding for them through the Pilot Program.

87. *Additional Certification Requirements.* The Commission also requires Pilot participants, when submitting their Pilot FCC Form 470 competitive bidding forms, and Pilot participants and service providers when submitting their FCC Forms 472 and 474 requests for reimbursement (*i.e.,* invoicing forms), respectively, to provide several additional certifications. For example, Pilot 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.

88. Support provided for cybersecurity services and equipment funded through the Pilot will be subject to audits and reviews consistent with the procedures currently used for the USF programs (*e.g.,* Beneficiary and Contributor Audit Program audits and Payment Integrity Assurance (PIA) reviews), and could be subject to recovery measures should the Commission and/or USAC find a violation of its rules and deem it appropriate. Specifically, applicants, participants, 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 it adopted. The Commission considers audits and other review mechanisms in the Pilot program to be important tools in ensuring compliance with its rules and identifying instances of waste, fraud, and abuse. Considering the action it took to create the Pilot Program using universal service funding, the Commission expects that these tools will continue to be paramount to its ability to ensure that these finite funds are used appropriately and consistent with its rules.

89. Consistent with its proposals in the *Cybersecurity NPRM,* the Commission will apply its existing USF suspension and debarment rules to the Pilot. In addition, to the extent that the Commission adopts updated and final suspension and debarment rules in a separate and pending proceeding, it will apply the updated rules to the Pilot Program.''

90. While commenters did not opine on these issues, the Commission finds it beneficial to apply its USF suspension and debarment rules, which are applicable to existing USF programs and codified at § 54.8 of its rules, to the Pilot as well. The Commission's 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. The Commission also finds 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 its 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, the Commission finds it reasonable to apply its existing USF suspension and debarment rules to the Pilot as well. The Commission finds 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, the Commission finds that its actions will support its mission to maintain the Pilot's integrity and protect it from waste, fraud, and abuse.

91. Similarly, the Commission finds 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. The Pilot incorporates administrative processes, forms, and rules from E-Rate and other USF programs. The Commission therefore finds it reasonable to apply any new suspension and debarment rules developed for those programs to the Pilot as well.

92. The Commission adopts three performance goals to enable it to evaluate the Pilot Program. The Commission expects 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. The Commission also adopts 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.

93. In the *Cybersecurity NPRM,* the Commission proposed three performance goals for the Pilot Program. Specifically, the Commission 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. Additionally, the Commission proposed and sought comment on how it can best measure progress towards these goals, to ensure that the limited Pilot funds are used most impactfully and effectively. The Commission also sought comment on how to evaluate the Pilot, including whether participants should submit periodic reports and other assessments and evaluations.

94. Based on the record, the Commission adopts its three proposed performance goals for the Pilot. The Commission notes 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.

95. *First Performance Goal: Improving the Security and Protection of E-Rate-Funded Broadband Networks and Data.* First, the Commission adopts 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. 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.'' 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, the Commission emphasizes that it is 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, the Commission is 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, the Commission seeks to gather data that will help it evaluate how best to safeguard E-Rate-funded networks now and in the future.

96. *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, the Commission adopts 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. 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 the Commission 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.'' With such recommendations in mind, the Commission adopts 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, the Commission disagrees with commenters who suggest that, in collecting data to evaluate the Pilot, its goals should be focused on determining ''how to best modernize the E-rate Category 2 to include cybersecurity permanently'' or adopting concurrent changes to its category two rules to permit funding for advanced firewalls and MFA. Although the Commission hopes to learn more about whether and how to best fund cybersecurity services and equipment at the conclusion of the Pilot, it does 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.

97. *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, the Commission adopts a goal of evaluating how to best leverage other available and low-cost and free Federal resources to better equip K–12 schools and libraries to proactively address their cybersecurity risks, though it does not go so far as to require the use of specific Federal Government tools and resources as initially discussed in the *Cybersecurity NPRM.* Commenters generally agreed with this goal. The Friday Institute for Education Innovation (Friday Institute), for example, stated that its 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.'' CTIA emphasized the importance of collaborating with other agencies to pursue and implement shared cybersecurity objectives. Commenters emphasize that collaboration with other Federal partners is ''vital,'' 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.' '' The Commission agrees with commenters on the importance of leveraging the expertise of its Federal, state, and local partners, and adopting this goal for the Pilot Program signals its intent to continue to work collaboratively on shared objectives to streamline its efforts to address schools' and libraries' cybersecurity challenges. To this end, the Commission agrees with commenters that, where possible, it should align its Pilot with the cybersecurity goals of its Federal partners.

98. *Data reporting requirements for participants.* To measure the Pilot's success in meeting the aforementioned goals, the Commission adopts initial, annual, and final reporting requirements for participants. In the *Cybersecurity NPRM,* the Commission 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. The Commission also proposed that these 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. The Commission sought comment on these proposals, as well as the best ways for it to evaluate the Pilot and measure progress towards the proposed performance goals.

99. Commenters generally agreed with its proposal to establish data reporting requirements. 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.'' 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. CTIA suggested that the reporting requirements use standardized metrics to obtain a common baseline of data across participants to aid in program evaluation.

100. 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. 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. 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.''

101. Based on the record, the Commission adopts 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 and it directs the Bureau to add a certification as part of the data collection requirements that will require participants to certify to the accuracy of the information reported and define mechanisms for enforcement. Specifically, after providing an initial baseline assessment using information that includes the reporting requirements for the second part of the application process, 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. The Commission finds that tracking and evaluating 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. Information contained in initial, annual, and final reports will be presumptively confidential; however, the Commission does plan to use school or library data as a tool to evaluate the Pilot and determine next steps. Additionally, at its discretion, the Commission 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. The Commission requires Pilot participants to submit each annual report no later than 60 days following the conclusion of each year (*i.e.,* year one and year two) of the Pilot Program, and to submit their final report no later than 60 days following the conclusion of the last year (*i.e.,* year three) of the Pilot Program. To accomplish the goal of periodic reporting by Pilot participants, the Commission delegates 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. The Commission also directs the Bureau to release a Public Notice (or multiple Public Notices, as needed) detailing the specific information to be provided by Pilot participants, additional detail regarding 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, the Commission directs 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. The Bureau should, to the extent practicable, and subject to approval from OMB, make the data reporting requirements available to Pilot participants prior to the availability of the Pilot FCC Form 470 to enable participants to consider whether there is any required information that they may need to obtain from their vendor(s) during the competitive bidding process.

102. 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. The Commission is 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. Specifically, the Commission finds 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. The Commission therefore will treat this information as presumptively confidential under its rules and withhold it from public inspection. In addition, the Commission has 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. Taken together, the Commission expects that these measures will alleviate commenters' concerns about protecting Pilot applicants' and participants' sensitive information regarding cybersecurity threats and readiness.

103. *Pilot Program reports.* The Commission directs the Bureau, in consultation with OEA, to review the reports submitted by Pilot participants and publish one interim report during the three-year Pilot and a final report after the Pilot has concluded. The interim report will, at a minimum, provide a summary of funding commitments and disbursements to-date and provide an update on progress toward the Pilot Program's performance goals. The final report will, at a minimum, provide a summary of funding disbursements, evaluate the Pilot Program's success in meeting each performance goal, and identify lessons learned. Recognizing the sensitivity of the information provided by Pilot applicants and participants, the Commission directs the Bureau to follow procedures for confidential information, including aggregating the information as necessary. The Commission directs the Bureau to publish the interim report no later than 180 days after Pilot participants submit their second (*i.e.,* year two) annual reports and to publish the final report no later than 180 days after Pilot participants submit their final (*i.e.,* year three) reports.

104. The Commission provides a path for recourse to parties aggrieved by decisions issued by USAC as a result of, or during, the Pilot. Specifically, the Commission adopts appeal and waiver request rules consistent with those that govern USAC's administration of the USF programs, including the E-Rate program. The Commission finds these existing processes sufficient to provide a meaningful review of decisions issued by USAC and the Commission regarding the Pilot. However, the Commission makes 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, or to request the review of a decision by USAC or a waiver of the Commission's rules. Despite assertions from some commenters that modifying the rules in this manner would limit Pilot participant flexibility and is unnecessary in this context, the Commission thinks 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, the Commission finds that a 30-day timeframe is appropriate given the limited three-year duration of the Pilot Program.

105. The Commission concludes 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,* it 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. The Commission 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.'' Additionally, the Commission 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. The Commission 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. In the *Cybersecurity NPRM,* the Commission 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, and the limits and restrictions that it should place on recipients of Pilot funds to remain within the statutory authority.

106. Commenters generally supported its conclusion that sufficient legal authority exists for the creation of this Pilot Program. In particular, commenters agreed that universal service is an ''evolving level of telecommunications services,'' and noted that the Pilot-supported services and equipment ''reflect ongoing advances in schools and libraries broadband networks and services.'' 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. Cisco also noted that the scale and number of cybersecurity 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.''

107. It agrees with these assessments, and affirm its 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, the Commission agrees that providing

support for cybersecurity services and equipment fulfills its mandate under section 254(c)(1) of the Act to periodically refine universal service to take into account advances in technology and services. As CoSN points out, the Pilot Program will provide support for new services and equipment that reflect advances in school networking technology. 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.

108. Second, the Commission finds that Pilot funds will be used for ''educational purposes,'' pursuant to section 254(h)(1)(B) of the Act. 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.'' 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, 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 its mandate under section 254(h)(1)(B) of the Act.

109. Furthermore, the Commission concludes 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. In the *First Universal Service Order,* 62 FR 32862, June 17, 1997, the Commission found that sections 254(h)(1)(B) through 254(c)(3) of the Communications Act authorizes universal service support for telecommunications services *and* additional services such as information services. The Commission therefore finds 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, sections 254(h)(1)(B) through 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.'' The Commission further distinguished between ineligible types of peripheral equipment (*e.g.,* laptops) and eligible equipment that is necessary to make the services functional. Therefore, the Commission also finds 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 it therefore concludes that the Commission has authority under sections 254(h)(1)(B) through 254(c)(3) of the Act to support the purchase of advanced firewall and cybersecurity equipment for educational purposes.

110. 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. In reaching this conclusion, the 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 its 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 its schools and libraries policies.'' 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.'' Consistent with this authority, the Commission 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.

111. Third, and separately, the Commission affirms its 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. 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. Specifically, the Commission 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.'' 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. The Commission finds this to be true even for use of school-owned devices used for educational purposes outside of the school, for example, in a student's home. Section 254(h)(2)(A)'s reference to ''classrooms'' is not prohibitive to the use of E-Rate support for off-premises use. The statute directs the Commission to establish rules to enhance access ''*for* all public and nonprofit elementary and secondary school classrooms . . . and libraries.'' Notably, the text does not say to enhance access to services ''at'' or ''in'' school classrooms (or libraries), as would more naturally indicate a tie to a physical location. As such, the statute permits funding of services that enhance access *for* school classrooms and libraries, even if such services are used off-premises. Accordingly, the Pilot can support the purchase of advanced firewall and cybersecurity services and equipment for use on school-owned devices for educational purposes, even if those devices may be used off-premises.

112. Lastly, the Commission finds that the Pilot Program is economically reasonable, and a prudent use of the limited universal service funds. The Commission has previously found expanding the types of cybersecurity services and equipment beyond basic firewall services to be cost-prohibitive to the E-Rate program. 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 cybersecurity threats and attacks by malicious actors who seek to exploit the schools' and libraries' networks and data. 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 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.'' 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.'' As a result, the Commission finds 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.

113. The Commission concludes 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 it has 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. 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, 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. Its determination that CIPA is applicable to the Pilot Program is consistent with past Commission decisions in the E-Rate program 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 services and components as category two internal connections services. Because the cybersecurity services and equipment it makes eligible under the Pilot Program serve functions equivalent to that of the basic firewall services currently supported by the E-Rate program, the Commission treats them similarly, either as standalone internal connections or as components of internet access. The Commission therefore concludes 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. As with the E-Rate and ECF programs, the Commission also concludes 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. Also, consistent with the ECF program, the Commission finds 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). 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.

114. In order to ease program administration, the Commission delegates 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 administrative tasks as may be necessary for the smooth implementation, administration, and operation of the Pilot Program. The Commission also delegates 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.

115. In addition, the Commission delegates 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. OMD performs this role with respect to USAC's administration of the Commission's universal service programs and it anticipates 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, it notes OMD is required to consult with the Bureau on any policy matters affecting the Pilot Program, consistent with § 0.91(a) of the Commission's rules.

116. The Commission directs 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, the Commission also directs 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.

117. The Commission recognizes 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. To promote maximum effectiveness and smooth administration of the Pilot Program, the Commission delegates to Bureau staff the authority to address and resolve such unforeseen administrative issues or problems, provided that doing so is consistent with the decisions it reached herein.

III. Procedural Matters

118. *Paperwork Reduction Act.* This document contains new information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, will

invite the general public to comment on the information collection requirements contained in the Order 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), the Commission previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees.

119. *Congressional Review Act.* The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, OMB, concurs, that this rule is ''non-major'' under the Congressional Review Act, 5 U.S.C. 804(2). The Commission will send a copy of the Order to Congress and the Government Accountability Office pursuant to 5 U.S.C. 801(a)(1)(A).

120. *Regulatory Flexibility Act.* As required by the Regulatory Flexibility Act of 1980, as amended (RFA), an Initial Regulatory Flexibility Analysis (IRFA) was incorporated in the *Cybersecurity NPRM,* released in November of 2023. 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.

121. 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 cybersecurity 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.

122. 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. 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.

123. In the Order, the Commission establishes a three-year Pilot Program (Pilot or Pilot Program) funded at $200 million, within the 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 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.

124. In addition, the 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, annually, on a pre-discounted basis, to purchase eligible cybersecurity services and equipment, with a pre-discount annual funding floor of $15,000 and a pre-discount annual funding maximum of $1.5 million; (2) a pre-discount annual budget of $15,000 per library, with the provision that library systems with more than 11 sites will be eligible for support up to a pre-discount maximum of $175,000 annually; and (3) that consortia participants comprised of eligible schools and libraries are eligible to receive funding based on student count (using the annual pre-discount $13.60 per student multiplier) and the number of library sites (using the $15,000 per library pre-discount annual budget) subject to either the pre-discount $175,000 annual budget maximum for library systems or pre-discount $1.5 million annual budget maximum for schools depending on the consortium's constituency. While these budgets, including associated maximums and floors, are specified in terms of annualized dollar amounts, participants' expenses are capped based on the full three-year duration of the Pilot and not on an annual basis. Thus, Pilot participants may request reimbursement for expenses as they are incurred even if it means that the amount of funding disbursed to a participant in a given year of the program exceeds their annual budget, so long as the total amount disbursed to a participant over the three-year term does not exceed three times that annual budget. 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. The Commission also permits all eligible schools and libraries, including those that do not currently participate in the E-Rate program, to apply to participate in the Pilot.

125. The Commission also adopts a P–ESL in the 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, the Commission defines: (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 cybersecurity 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, the Commission confirms that a wide range of services and equipment that it had proposed for inclusion in the *Cybersecurity NPRM,* or that commenters had otherwise requested, are eligible. In the Order, the Commission describes 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.

126. In the Order, it explains that ineligible costs include, among other things, (i) any equipment, service, or other related cost that is eligible in the Commission's E-Rate program eligible services list in the corresponding E-Rate funding year for which Pilot reimbursement is sought, (ii) any equipment, service, or other related cost, or portion thereof, for which a participant has already received reimbursement in full or in part, or plans to apply for reimbursement in full or in part, through any other USF or Federal, state, or local program, and (iii) any equipment or services prohibited by the Secure and Trusted Communications Networks Act of 2019, Public Law 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 §§ 54.9 and 54.10 of the Commission's rules, that implement the Secure Networks Act.

127. The Commission designates USAC to be the Administrator for the Pilot. The Commission requires 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, the Commission anticipates 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, the Commission encourages participation in the Pilot by a broad range of service providers and do not discourage new companies from participating, nor does it 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.

128. In the Order, the Commission describes that it 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, the Commission 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, the Commission 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.

129. In the Order, the Commission directs the Bureau and the Universal Service Administration Company (USAC or the Administrator) to model the Pilot processes and forms on existing E-Rate and ECF programs' processes and forms to the extent possible for the Pilot Program. The Commission expects the Bureau and USAC to leverage the following 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).

130. To protect the integrity of the Pilot, and safeguard universal service funds, the Commission implements a number of program integrity protections. For example, it implements document retention requirements and a prohibition on gifts, and the Commission requires applicants provide certain certifications and be subject to auditing. The Commission has modeled these provisions after its E-Rate processes to protect the Pilot and ensure the limited program funding is used for its intended purposes. The Commission also applies its existing suspension are debarment rules to the Pilot. The Commission also delegates to Bureau 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 it reached in the Order. The Commission expects 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.

131. There were no comments filed that specifically address the proposed rules and policies presented in the IRFA.

132. 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. The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

133. 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. The RFA generally defines the term ''small entity'' as having the same meaning as the terms ''small business,'' ''small organization,'' and ''small governmental jurisdiction.'' In addition, the term ''small business'' has the same meaning as the term ''small business concern'' under the Small Business Act. 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).

134. *Small Businesses, Small Organizations, Small Governmental Jurisdictions.* The Commission's actions, over time, may affect small entities that are not easily categorized at present. The Commission therefore describes, at the outset, three broad groups of small entities that could be directly affected herein. 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. These types of small businesses represent 99.9% of all businesses in the United States, which translates to 33.2 million businesses.

135. 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.'' The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations. 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.

136. 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.'' U.S. Census Bureau data from the 2022 Census of Governments indicate there were 90,837 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States. Of this number, there were 36,845 general purpose governments (county, municipal, and town or township) with populations of less than 50,000 and 11,879 special purpose governments (independent school districts) with enrollment populations of less than 50,000. Accordingly, based on the 2022 U.S. Census of Governments data, the Commission estimates that at least 48,724 entities fall into the category of ''small governmental jurisdictions.''

137. Small entities potentially affected by the rules herein are Schools, Libraries, Telecommunications Resellers, Local Resellers, Wired Telecommunications Carriers, All Other Telecommunications, Wireless Telecommunications Carriers (except Satellite), Wireless Carriers and Service Providers, Wired Broadband internet Access Service Providers (Wired ISPs), Wireless Broadband internet Access Service Providers (Wireless ISPs or WISPs), internet Service Providers (Non-Broadband), Vendors of Infrastructure Development or Network Buildout, Telephone Apparatus Manufacturing, Custom Computer Programming Services, Other Computer Related Services (Except Information Technology Value Added Resellers), Information Technology Value Added Resellers, Software Publishers.

138. While the Commission sought to minimize compliance burdens on small entities where practicable, the rules adopted in the 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.

139. *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, the Commission requires 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 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 cybersecurity threats and attacks within a year of the date of its application. Moreover, the Commission requires applications to be submitted through an online Pilot portal on USAC's website and 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.

140. *Competitive Bidding, Requests for Services, and Invoicing and Reimbursement Processes.* The Commission requires 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).

141. *Reporting Requirements.* The Commission requires 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.

142. *Document Retention Requirements.* The Commission 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 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. This rule requires that Pilot participants must retain documents regarding participation in the Pilot, including asset and inventory records, accumulated during the Pilot, for a period of 10 years. The Commission also requires 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.

143. *Pilot Program Certifications.* As noted, the Commission requires participants to provide several certifications as part of their FCC Form 484 application, competitive bidding requirements, requests for services, and invoicing processes. Similarly, the Commission requires their selected service providers to provide certifications related to invoicing processes. The Commission also requires 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.

144. *Other Delegations.* As part of the Order, the Commission also delegates to Bureau 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 it reached in the Order.

145. The record does not include a detailed cost/benefit analysis that would allow the Commission 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 the Commission expects that Pilot participants will carefully weigh the benefits, costs, and burdens of participation to ensure that the benefits outweigh their costs. The Commission expects 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.

146. 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.''

147. In the Order, the Commission takes multiple steps that minimize economic impact on small entities related to the final rules it adopted. The Commission has 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 its decision about whether to approve the entity as a participant in the Pilot), the Commission minimizes 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 it could have required that the entire form be completed with the initial application.

148. The Commission has 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. The Commission expects this action will meaningfully reduce any economic impact on small entities associated with completing information requested via these forms. First, the Commission expects 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, the Commission expects that even those small entities that may not be involved 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, the Commission expects that these forms will generally be easy to use and efficient to complete based on its observation, made over many years, that forms with similar substance have proven effective in the Commission's E-Rate and ECF programs. The Commission thus expect its actions will significantly minimize any economic impact on small entities compared to an alternative approach where it developed Pilot processes and forms that were not related to those already developed in the Commission's E-Rate and ECF programs.

149. The Commission has also designed its reporting requirements to minimize the economic impact on small entities while ensuring that it gathers 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 it 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 the Commission has also directed the Bureau to consider the development of a standardized reporting form for use by Pilot participants.

150. Additionally, the Commission has also delegated authority to the Bureau to address and resolve a number of matters, including unforeseen administrative issues or problems, provided that doing so is consistent with the decisions it reached in the Order. The Commission expects 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.

151. The Commission 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, the Commission adopts its 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.

152. The Commission 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, the Commission modifies 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, the Commission thinks the change is appropriate for the Pilot Program because it will allow for faster decisions in a program that has a limited duration.

153. The Commission will send a copy of the Order, including this FRFA, in a report to Congress pursuant to the Congressional Review Act. In addition, the Commission will send a copy of the Order, including the FRFA, to the Chief Counsel for Advocacy of the SBA. A copy of the Order and FRFA (or summaries thereof) will also be published in the **Federal Register**.

154. *OPEN Government Data Act.* The OPEN Government Data Act, 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. This requirement is to be implemented ''in accordance with guidance by the Director'' of OMB. 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)].'' A ''data asset'' is ''a collection of data elements or data sets that may be grouped together,'' and ''data'' is ''recorded information, regardless of form or the media on which the data is recorded.'' The Commission delegates authority, including the authority to adopt rules, to the 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, the Bureau 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.

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

IV. Ordering Clauses

156. *Accordingly, it is 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, the Report and Order *is adopted* effective August 29, 2024.

157. *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,* and such rule amendments shall be effective August 29, 2024, except for §§ 54.2004, 54.2005, 54.2006, and 54.2008, which are delayed indefinitely. The Commission will publish a document in the **Federal Register** announcing the effective date for those sections after approved by the Office of Management and Budget as required by the Paperwork Reduction Act.

List of Subjects in 47 CFR Part 54

Communications common carriers, Cybersecurity, Internet, Libraries, Reporting and recordkeeping requirements, Schools, Telecommunications, Telephone.

Federal Communications Commission.

Katura Jackson,

Federal Register Liaison Officer.

Final Rules

For the reasons discussed in the preamble, the Federal Communications Commission amends part 54 of title 47 of the Code of Federal Regulations as follows:

PART 54—UNIVERSAL SERVICE

■ 1. The authority citation 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, unless otherwise noted.

■ 2. Add subpart T to read as follows:

Subpart T—Schools and Libraries Cybersecurity Pilot Program

Sec.

§ 54.2000 Terms and definitions.

Administrator. 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 (FCC).

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 subpart 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 this subpart, 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 (OMB) 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 OMB 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. Budgets are specified in terms of annualized dollar amounts, but participants' expenses are capped based on the full three-year duration of the Pilot and participants may seek reimbursement for more than the annual budget for any given Pilot Program year, so long as the total amount disbursed over the three-year term does not exceed three times the applicable annual budget.

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

(2) *Libraries.* Each eligible library will receive a pre-discount budget of $15,000

annually up to 11 libraries/sites. For library systems with more than 11 libraries/sites, the budget will be up to $175,000 pre-discount annually.

(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 $1.5 million pre-discount funding caps, and the number of library sites, using the pre-discount $15,000 annual per-library budget and $175,000 pre-discount funding caps. Consortia solely comprised of eligible schools or comprised of both eligible schools and libraries are subject to the pre-discount annual $1.5 million budget maximum for schools and school districts. Consortia solely comprised of eligible libraries will be subject to the pre-discount annual $175,000 budget maximum for library systems.

(c) *Duration.* The Schools and Libraries Cybersecurity Pilot Program shall make funding available to applicants selected to participate in the Pilot for three years, to begin when the applicants selected to participate in the Pilot 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 (NSLP). 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 definition of ''elementary school'' or ''secondary school'', as defined in § 54.2000, and not excluded under paragraph (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 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 (see § 54.502(a)), available on the FCC's website at *https://www.fcc.gov/cybersecurity-pilot/cybersecurity-pilot-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.

§§ 54.2004–54.2006 [Reserved]

§ 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 (NSLP) or a federally-approved alternative mechanism. School districts shall divide the total number of students eligible for the NSLP 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 NSLP 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 NSLP 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.

TABLE 1 TO PARAGRAPH (C)

% of students eligible for national school lunch program	Discount level	
	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 subpart, 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 [Reserved]

§ 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 in this chapter 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 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 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 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 a *de novo* review of requests for review of decisions issued by the Administrator.

(2) The Commission shall conduct a *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 a *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) *Certifications required.* 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) *CIPA certifications.* (1) A Schools and Libraries Cybersecurity Pilot Program participant need not complete additional Children's internet Protection Act (CIPA) (47 U.S.C. 254(h) and (l)) compliance certifications if the participant has already certified its 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.,* 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 47 U.S.C. 254(h) and (l);

(ii) That they are undertaking the actions necessary to comply with CIPA requirements under 47 U.S.C. 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 47 U.S.C. 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 within one year from the date the waiver was granted.

■ 3. Delayed indefinitely, add §§ 54.2004 through 54.2006 to read as follows:

§ 54.2004 Application for Pilot Program selection and reporting of information.

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

(b) *Participant announcement.* 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(s) 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 (Education Department) or Cybersecurity and Infrastructure Security Agency (CISA) best practices recommendations, 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.

(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 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.

(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. The 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 also certify under oath that:

(i) ''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 any 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).''

(ii) ''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.''

(iii) ''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).''

(iv) 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.

(v) ''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.''

(vi) ''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.''

(vii) ''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 cybersecurity 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 best practices 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. The 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 also certify under oath 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 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, 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 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.

(v) ''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.''

(vi) ''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.''

(vii) ''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) *Fair and open competitive bidding process.* 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.

Note to Paragraph (a): The following is an illustrative list of activities or behaviors that would not result in a fair and open competitive bidding process: the participant seeking supported services has a relationship with a service provider that would unfairly influence the outcome of a competition or would furnish the service provider with inside information; someone other than the participant or an authorized representative of the participant prepares, signs, and submits the FCC Form 470 and certification; a service provider representative is listed as the FCC Form 470 contact person and the participant allows that service provider to participate in the competitive bidding process; the service provider prepares the participant's FCC Form 470 or participates in the bid evaluation or vendor selection process in any way; the participant turns over to a service provider the responsibility for ensuring a fair and open competitive bidding process; a participant employee with a role in the service provider selection process also has an ownership interest in the service provider seeking to participate in the competitive bidding process; and the participant's FCC Form 470 does not describe the supported services with sufficient specificity to enable interested service providers to submit responsive bids.

(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, except as provided in paragraph (f) of this section. 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; and

(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 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 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 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 $50,000,000.

(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 Pilot Program 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 CFR 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 website designated for this purpose.

(4) After posting on the Administrator's website 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 28 days from the date on which its description of services and/or equipment is posted on the Administrator's website before making any 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 in this paragraph (d). 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 subpart, 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 (d):

(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 (d) 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 in this subpart.

(e) *Selecting a provider of eligible services and/or equipment.* 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 and equipment offerings. In determining which service and equipment offering is the most cost-effective, entities may consider relevant factors other than the pre-discount prices submitted by providers, but price must be the primary factor considered.

(f) *Exemption to competitive bidding requirements.* Participants in the Schools and Libraries Cybersecurity Pilot Program are not required to file an FCC Form 470 when seeking support for services and equipment purchased from Master Service Agreements negotiated by Federal, state, Tribal, or local governmental entities on behalf of such Pilot participants, if such Master Service Agreements were awarded pursuant to the E-Rate program FCC Form 470 process, as well as applicable Federal, state, Tribal, or local competitive bidding requirements.

§ 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 any 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 definition of ''elementary school'' or ''secondary school'', as defined in § 54.2000, does not operate as a for-profit business, and does not have endowments exceeding $50,000,000.

(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 a for-profit business 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 for services and equipment 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 the portion of eligible services and/or equipment that have been purchased and reimbursed in full or in part 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 in this chapter 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, including, but not limited to, their employees, officers, representatives, agents, independent contractors, consultants, family members, and individuals who are on the governing boards, 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 in this chapter 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.

■ 4. Delayed indefinitely, add § 54.2008 to read as follows:

§ 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 in full 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 the portion of eligible services and/or equipment that have been purchased and reimbursed in full or in part 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 and received along with the submission of its request for reimbursement as required by paragraph (b) of this section.

(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, including, but not limited to, their employees, officers, representatives, agents, independent contractors, consultants, family members, and individuals who are on the governing boards, 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 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 the Service Provider 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 and provided to the school, library, or consortium, along with the submission of its request for reimbursement as required by paragraph (b) of this section.

(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 in this subpart.

(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 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 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 and received 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(c).

(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.

[FR Doc. 2024–15866 Filed 7–29–24; 8:45 am]

BILLING CODE 6712–01–P