6712-01

This document is scheduled to be published in the Federal Register on 12/29/2023 and available online at **https://federalregister.gov/d/2023-27811**, and on **https://govinfo.gov**

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 54

[WC Docket No. 23-234; FCC 23-92; FRS ID 190276]

Schools and Libraries Cybersecurity Pilot Program

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) proposes a three-year pilot program within the Universal Service Fund (USF or Fund) to provide up to $200 million available to support cybersecurity and advanced firewall services for eligible schools and libraries.

DATES: Comments are due on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** and reply comments are due on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. Written comments on the Paperwork Reduction Act proposed information collection requirements must be submitted by the public, Office of Management and Budget (OMB), and other interested parties on or before **[INSERT DATE 60 DAYS OF AFTER PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Pursuant to §§ 1.415 and 1.419 of the Commission's rules, 47 CFR 1.415, 1.419, interested parties may file comments and reply comments. You may submit comments, identified by WC Docket No. 23-234, by any of the following methods:

- Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: https://www.fcc.gov/ecfs/.
- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing.

- Filings can be sent by commercial overnight courier or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.

- U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street, NE, Washington, DC 20554.

- Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings at its headquarters. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. *See* FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy, Public Notice, DA 20-304 (March 19, 2020), https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy.

- People with Disabilities: To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at (202) 418-0530 (voice), (202) 418-0432 (TTY).

- Availability of Documents: Comments, reply comments, and *ex parte* submissions will be publicly available online via ECFS.

FOR FURTHER INFORMATION CONTACT: Joseph Schlingbaum Joseph.Schlingbaum@fcc.gov in the Telecommunications Access Policy Division, Wireline Competition Bureau, 202-418-7400 or TTY: 202-418-0484. For information regarding the PRA information collection requirements contained in this PRA, contact Nicole Ongele, Office of Managing Director, at 202-418-2991 or Nicole.Ongele@fcc.gov. 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 summary of the Commission's Schools and Libraries Cybersecurity Pilot Program, Notice of Proposed Rulemaking (*NPRM*) in WC Docket No. 23-234; FCC 23-92, adopted November 8, 2023 and released November 13, 2023. The full text of this document is available at the following Internet address: https://www.fcc.gov/document/fcc-proposes-schools-libraries-cybersecurity-pilot-program-0.

Initial Paperwork Reduction Act of 1995 Analysis

This document contains proposed information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget (OMB) to comment on the information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. Public and agency comments are due **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. Comments should address: (a) whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information shall have practical utility; (b) the accuracy of the Commission's burden estimates; (c) ways to enhance the quality, utility, and clarity of the information collected; (d) ways to minimize the burden of the collection of information on the respondents, including the use of automated collection techniques or other forms of information technology; and (e) way to further reduce the information collection burden on small business concerns with fewer than 25 employees. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C. 3506(c)(4), the Commission seeks specific comment on how it might further reduce the information collection burden for small business concerns with fewer than 25 employees.

OMB Control Number: 3060-XXXX.

Title: Schools and Libraries Cybersecurity Pilot Program.

Form Numbers: FCC Forms 470, 471, 472, 474 – Cybersecurity, 484 and 488 - Cybersecurity.

Type of Review: New collection.

Respondents: State, local or tribal government institutions, and other not-for-profit institutions.

Number of Respondents and Responses: 23,000 respondents; 201,100 responses.

Estimated Time per Response: 4 hours for FCC Form 470 – Cybersecurity, 5 hours for FCC Form 471 – Cybersecurity, 1.75 hours for FCC Forms 472/474 – Cybersecurity, 15 hours for FCC Form 484, and 1 hour for FCC Form 488 - Cybersecurity.

Frequency of Response: On occasion and annual reporting requirements, and recordkeeping requirement.

Obligation to Respond: Required to obtain or retain benefits. Statutory authority for this collection of information is contained in sections 1-4, 201-202, 254, 303(r), and 403 of the Communications Act of 1934, as amended, 47 U.S.C. 151-154, 201-202, 254, 303(r), and 403.

Total Annual Burden: 743,900 hours.

Total Annual Cost: No Cost.

Needs and Uses: The information collected is designed to obtain information from applicants and service providers that will be used by the Commission and/or USAC to evaluate the applications and select participants to receive funding under the Cybersecurity Pilot Program, make funding determinations and disburse funding in compliance with applicable federal laws for payments made through the Pilot program. The Commission will begin accepting applications to participate in the Cybersecurity Pilot Program after publication of its Report and Order and notice of OMB approval of the Cybersecurity Pilot Program information collection in the Federal Register.

On November 8, 2023, the Commission adopted a *NPRM* in WC Docket No. 23-234, Schools and Libraries Cybersecurity Pilot Program. The Commission proposes a three-year pilot program within the Universal Service Fund to provide up to $200 million available to support cybersecurity and advanced firewall services for eligible schools and libraries. Accordingly, the Commission proposes to add subpart T to part 54 of its rules.

Synopsis

I. INTRODUCTION

1. Broadband connectivity and Internet access are increasingly important for K-12 students and adults alike. Whether for online learning, job searching, or connecting with peers and the community, high-speed broadband is critical to educational and personal success in the modern world. However, although broadband connectivity and Internet access can simplify and enhance the 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. Similarly, while advances in online technology benefit K-12 schools and libraries by expanding teaching and education beyond the physical confines of a school or library building, and permitting students and library patrons to complete online homework assignments, conduct online research, and learn the computer skills necessary to secure a job in the future, K-12 schools and libraries increasingly find themselves targets for attackers who would disrupt their ability to educate, illegally obtain sensitive student, school staff, and library patron data, and hold their broadband networks hostage to extract ransom payments. Given the growing importance of broadband connectivity and Internet access for K-12 schools and libraries, the Commission proposes a three-year pilot program within the Universal Service Fund (USF or Fund) to provide up to $200 million available to support cybersecurity and advanced firewall services for eligible schools and libraries.

2. Specifically, in the *NPRM*, the Commission proposes the creation of a Schools and Libraries Cybersecurity Pilot Program (Pilot or Pilot program) that would allow us to obtain valuable data concerning the cybersecurity and advanced firewall services that would best help K-12 schools and libraries address the growing cyber threats and attacks against their broadband networks and data, while also helping us to better understand the most effective way USF support could be used to help schools and libraries address these significant concerns while promoting the E-Rate program's longstanding goal of promoting basic connectivity. It is clear that the E-Rate program alone cannot fully address the K-12 schools' and libraries' cyber concerns and protect their broadband networks and data from cyber threats and attacks. As proposed, the Pilot seeks to learn more about which cybersecurity

and advanced firewall services will have the greatest impact in helping K-12 schools and libraries protect their broadband networks and data, while also ensuring that limited USF funds are being utilized in an effective manner. For example, the Commission expects that this Pilot will necessarily need to ensure that participating K-12 schools and libraries fully leverage the free and low-cost K-12 cybersecurity resources provided by our federal partners, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and the U.S. Department of Education (DOE), to complement the Pilot's work and make the most effective use of Pilot program funding.

3. As discussed further below, the Commission proposes that the program operate as a new Pilot within the USF, which would provide funding to eligible K-12 schools and libraries to defray the qualifying costs of receiving the cybersecurity and advanced firewall services needed to protect their E-Rate-funded broadband networks and data from the growing number of K-12 school- and library-focused cyber events. Additionally, the Commission seeks comment on the applicability of the Children's Internet Protection Act (CIPA) to the Pilot program and USF-funded cybersecurity and advanced firewall services for schools and libraries.

4. The Commission expects this Pilot program will benefit K-12 schools and libraries that are responding to a wide breadth of cyber threats and attacks that impact their ability to protect their broadband networks and data. Data gathered from the Pilot program will help us understand whether and how USF funds could be used to help address the K-12 school and library cybersecurity challenges, and the data and information collected through this Pilot program may also aid in the consideration of broader reforms across the government—including potential statutory changes—to help schools and libraries address the significant K-12 school and library cybersecurity concerns. In proposing this Pilot, the Commission is mindful of the E-Rate program's longstanding goal of promoting basic connectivity, its obligations to be a careful and prudent steward of the limited universal service funding, and the need to balance its actions in this proceeding against competing priorities, bearing in mind that this funding is obtained though assessments collected from telecommunications carriers that are typically passed on to and paid for by U.S. consumers.

II. DISCUSSION

5. Mindful of the need to protect universal service funding and aware that basic firewall services may be insufficient alone to protect E-Rate-funded broadband networks, the Commission proposes a three-year Pilot program to ascertain whether supporting cybersecurity and advanced firewall services with universal service support could advance the key universal service principles of providing quality Internet and broadband services to K-12 schools and libraries at just, reasonable, and affordable rates; and ensuring schools' and libraries' access to advanced telecommunications provided by Congress in the Telecommunications Act of 1996. To accomplish this, the Commission proposes a pilot structure similar to the one it used in the Connected Care Pilot Program. Specifically, interested K-12 schools and libraries would apply to be Pilot program participants by submitting an application containing information about how they would use the Pilot funds and providing information about their proposed cybersecurity and advanced firewall projects. If selected, the applicants would apply for funding for Pilot-eligible services and equipment. Pilot participants receiving a funding commitment would be eligible to begin receiving cybersecurity and advanced firewall services and equipment, and would submit invoices for reimbursement.

6. It is important that the Commission defines the goals of the proposed Pilot program, as well as establish criteria to measure progress towards those goals. This will help the Commission and other federal, state, and local stakeholders to determine whether, and how, to provide funding for cybersecurity and advanced firewall services after the Pilot ends. To that end, the Commission proposes three goals: (1) improving the security and protection of E-Rate-funded broadband networks and data; (2) measuring the costs associated with cybersecurity and advanced firewall services, and the amount of funding needed to adequately meet the demand for these services if extended to all E-Rate participants; and (3) evaluating how to leverage other federal K-12 cybersecurity tools and resources to help schools and libraries effectively address their cybersecurity needs.

7. *Improving the security and protection of E-Rate-funded broadband networks and data.* The Commission first proposes a goal for the proposed Pilot program of improving the security and

protection of E-Rate-funded broadband networks and data. As the Council of the Great City Schools stated, "schools and libraries desperately need assistance to acquire advanced . . . firewalls to protect the integrity of their broadband connections, networks and data." Funding made available by the proposed Pilot may be able to help participants acquire the cybersecurity and advanced firewall services and equipment needed to improve the security and protection of their broadband networks and data. The Commission seeks comment on how it can measure whether the Pilot is effective in protecting and securing E-Rate-funded broadband networks and data. The Commission also seeks comment on this proposed goal and related questions.

8. *Measuring the costs and effectiveness of Pilot-funded cybersecurity and advanced firewall services and equipment.* Next, the Commission proposes a goal of measuring the costs and effectiveness of cybersecurity and advanced firewall services and equipment. The Pilot can help the Commission and other federal, state, and local government agencies gather additional data on the types of new services and equipment that applicants will purchase to address network and data security concerns, and the associated cost and effectiveness of Pilot-funded services and equipment. Data provided in FCC Forms 470 and 471 (or their Pilot program equivalent) can aid the Commission in measuring the costs of cybersecurity and advanced firewall services and equipment. What data should be collected on the effectiveness of the funded equipment and services? For example, should Pilot participants be required to submit data on the number of intrusion attempts, number of successful attacks, mean time to detection and response, estimated cost of each attack, etc.? What other accepted metrics should the Commission requires Pilot participants to monitor and record? For example, should the Commission collect data on the number and percent of students and school and library staff using multi-factor identification, the frequency of school and library staff and, separately, student cyber training sessions, and participation rates? Should Pilot participants be required to assess awareness and readiness of school and library staff based on available guidance from CISA or other expert organizations? Should all or some of these potential requirements be standardized across Pilot participants to allow for comparative analysis of outcomes? The proposed intent of this Pilot is to also determine the most cost-effective use of universal service funding to help schools and libraries

proactively address K-12 cybersecurity issues. The Commission seeks comment on this proposed goal and related questions.

9. *Evaluating how to leverage other federal resources to address schools' and libraries' cybersecurity threats.* Third, the Commission proposes a goal of evaluating how to best leverage other federal resources to help schools and libraries proactively address K-12 cybersecurity issues. CISA, DOE, and NIST have made a wide array of free and low-cost K-12 cybersecurity tools and resources available to schools and libraries. Also, as discussed, more resources beyond funding are needed for schools and libraries to effectively protect their broadband networks and data from cyberattacks and other cyber threats. As part of this Pilot, the Commission intends to coordinate with its federal partners in identifying the most impactful tools and resources to help schools and libraries effectively protect themselves and address these cybersecurity issues. For example, DOE plans to establish a Government Coordinating Council (Council) to coordinate the activities of federal leaders in taking actions to help protect school networks. What role can the Pilot play to complement the efforts of other agencies that will participate in the Council? In addition, the CISA K-12 Cybersecurity Report contains three key recommendations for schools and libraries that would immediately improve their cybersecurity postures, the first of which recommends implementing a "small number of the highest priority steps", including implementing multi-factor authentication, fixing known cybersecurity flaws, performing and testing back-ups, minimizing exposure to common attacks, developing and exercising a cyber incident response plan, and creating a training and awareness campaign. Should the Pilot target funding to allow schools and libraries to implement some or all of the items contained in the list of highest priority steps from CISA's first recommendation to help them address K-12 cybersecurity issues (e.g., multi-factor authentication, correcting known security flaws, performing and testing system backups, etc.)? Should schools and libraries be required to implement a certain number of these free and low-cost tools to be eligible to receive Pilot funding for cybersecurity and advanced firewall services, and if so how should this requirement be enforced? Furthermore, DOE has made a number of recommendations in its K-12 Digital Infrastructure Briefs aimed at making K-12 networks safe, accessible, resilient, sustainable, and future-proof. How should the Pilot account for these recommendations? How can the Pilot funding

incentivize schools and libraries to take full advantage of other available free and low-cost K-12 cybersecurity tools and resources? How can the Pilot leverage USAC's established relationships with and processes for distribution of training to the schools and libraries to facilitate the efforts of CISA, DOE, and NIST in order to provide technical assistance or capacity building for Pilot participants? The Commission seeks comment on this proposed goal and how best to implement and measure success.

10. How can the Commission best measure progress towards these proposed performance goals, to ensure that the limited Pilot funds are used most impactfully and effectively to help schools and libraries protect their broadband networks and data? For example, by what objective criteria can the Commission determine whether the funding provided through the Pilot actually improved the protection and security of schools' and libraries' broadband networks and data? What information would the Commission need to collect to compare Pilot results against those criteria? Are there best practices and recommendations that the Commission can rely on from expert agencies or organizations that have undertaken similar or related cybersecurity pilots? What outcomes should the Commission measure? For example, in this Pilot should the Commission measure the reductions in the number of cyberattacks; average cost of an attack; time to detect and respond to a cyber threat; staff and user awareness/readiness; or some other measure(s)?

11. How should the Commission evaluate the Pilot? The Commission proposes 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 program. The Commission further proposes that these reports contain information on how the 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, and the number of cyber incidents that occurred each year of the Pilot program and whether the school or library was successful in defending its broadband network and data for each incident. The Commission seeks comment on these proposals. Are there any other cybersecurity assessments or evaluations that participants should conduct to determine whether the Pilot-funded cybersecurity and advanced firewall services and equipment bolstered the school's or library's

cybersecurity posture, even absent a breach or other cyber incident? What is the data or information that the Commission should be collecting in the proposed progress and final reports? What could the Commission do to allow comparability across pilots? Are there any public sources of information that the Commission can also use to determine the impact of the Pilot program in addressing K-12 cybersecurity issues, and if so, does this data impact what the Commission require participants to submit in their reports to the Commission?

12. Next, the Commission discusses the overall structure for the proposed Pilot program. Building on its experience administering the Connected Care Pilot Program, the Commission proposes a similar structure for the proposed Pilot program, and discuss in more detail below.

13. *Overall Structure.* The Commission proposes to structure the proposed Pilot program in a manner similar to the Connected Care Pilot Program. Under this proposal, interested schools and libraries would apply to be a Pilot participant. Those schools and libraries that are selected to participate will be provided an opportunity to apply for Pilot funding for eligible services and equipment. Participants will then receive a funding commitment, and can begin to receive equipment/services and submit invoices for reimbursement. Further, the Commission proposes that the Universal Service Administrative Company (USAC), the FCC's administrator for universal service programs, be appointed as the permanent administrator of the Pilot program. The Commission seeks comment on this general structure for the proposed Pilot program.

14. The Commission further proposes that interested participants will be required to submit an application describing their proposed use of Pilot funds, and provide information that will facilitate the selection of high-quality projects that will best further the goals of the proposed Pilot program. At a minimum, the Commission proposes that Pilot applications require the following information:

i. Name, address, and contact information for the interested school or library. For school district or library system applicants, the name and address of all schools/libraries within the district/system, and contact information for the district or library system.

ii. 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, and a description of its proposed advanced cybersecurity action plan should it be selected to participate in the Pilot program and receive funding.

iii. Description of any incident of unauthorized operational access to the Pilot participant's systems or equipment within a year of the date of its application; the date range of the incident; a description of the unauthorized access; 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.

iv. Description of the Pilot participant's proposed use of the funding to protect its broadband network and data and improve its ability to address K-12 cyber concerns. This description should include the types of services and equipment the participant plans to purchase and the plan for implementing and using the Pilot-funded equipment and services to protect its broadband network and data, and improve its ability to manage and address its cybersecurity risks.

v. Description of how the Pilot participant plans to collect and track its progress in implementing the Pilot-funded equipment and services into its cybersecurity action plan, and for providing the required Pilot data, including the impact the funding had on its initial cybersecurity action plan that pre-dated implementation of Pilot efforts.

The Commission seeks comment on these proposed requirements, and whether additional information should also be required. The Commission proposes that Pilot participants will submit these applications via an online platform, designed and operated by USAC, and seek comment on this proposal. Are there any confidentiality or security concerns with providing the above information, and if so, what protections should be implemented to protect potentially sensitive data regarding a prospective applicant's current cybersecurity posture? How can the Commission best leverage its experience receiving applications in USF programs, for example, E-Rate, Rural Health Care, and the Connected Care

Pilot Program, as well as in the appropriated programs, like COVID-19 Telehealth, Emergency Connectivity Fund (ECF), and the Affordable Connectivity Program (ACP) Outreach grants? Are there any lessons learned from the Connected Care Pilot Program and other FCC pilot programs that the Commission can benefit from when establishing the proposed Pilot program? The Commission further proposes that the Bureau review applications and select participants, in consultation with the Office of Economics and Analytics (OEA), the Public Safety and Homeland Security Bureau (PSHSB), and the Office of the Managing Director (OMD), as needed, and seek comment on this proposal. Lastly, to assist with program administration and ensure that the proposed Pilot program runs efficiently, the Commission proposes to delegate to the Bureau the authority to implement the proposed Pilot program and to direct USAC's administration of the Pilot program, consistent with the Commission's rules and orders, and seek comment on this proposal.

15. *Pilot Program Duration*. The Commission proposes that the Pilot program will make funding available to participants for a three-year term, and seek comment on this proposal. Does a three-year term provide sufficient data to the Commission to evaluate how effective the Pilot funding is in protecting K-12 schools and libraries, and their broadband networks and data, from cyberattacks and other cyber threats? The Commission acknowledges that there may be a tradeoff between learning more from the Pilot program and moving quickly to potentially expand support to protect all K-12 schools' and libraries' broadband networks and data from cyber threats. Are there ways to shorten the length of the Pilot, for example, by using a single application window that remains open until funds are exhausted, without compromising the amount or quality of the data the Pilot will generate? Should the Pilot program period include additional ramp-up time, to allow participants an opportunity to prepare for the Pilot? Should the Pilot program include additional time at the end of the three-year term for the Commission to evaluate results? The Commission seeks comment on the three-year term proposal and these related questions.

16. *Pilot Budget*. The Commission proposes a budget of $200 million over the three-year duration of the proposed Pilot program, and seek comment on this proposal. Will a budget of $200

million be sufficient to obtain and receive meaningful data on how this funding helped to protect schools' and libraries' broadband networks and data and improved their ability to address K-12 cyber issues? Conversely, would a lower budget be sufficient for these purposes (e.g., $100 million) while also putting less pressure on the contribution factor? How should the total Pilot program budget be distributed over the three-year funding period? Should each selected project's funding commitment be divided evenly across the Pilot program duration? For example, if a selected project requests and receives a $9 million funding commitment and the funding period is three years, should the project receive $3 million for each year? Alternatively, are there reasons why a Pilot participant may need access to a greater amount of funding up front? If the Commission allows Pilot participants to access a greater amount earlier in the term, how can the Commission forecast a predictable budget over the three-year term? The Commission seeks comment on these questions.

17. As this proposed Pilot should not divert resources from the existing universal service support programs, the Commission proposes requiring USAC to separately collect on a quarterly basis the funds needed for the duration of the Pilot program. The Commission expects that funding the Pilot program in this manner would not significantly increase the contributions burden on consumers. This approach also would not impact the budgets or disbursements for the other universal service programs. The Commission seeks comment on this approach. Should the collection be based on the quarterly demand for the Pilot program? The Commission also proposes to have excess collected contributions for a particular quarter carried forward to the following quarter to reduce collections. Under this approach, the Commission also proposes to return to the Fund any funds that remain at the end of the Pilot program. Are there other approaches the Commission should consider for funding the Pilot program? Are there any tradeoffs between allocating funding to the proposed Pilot program as it relates to the size of the E-Rate program and the USF more generally? The Commission also seeks comment on whether the costs associated with the proposed Pilot program will impact other stakeholders' requests related to the use of universal service and E-Rate funding, such as allowing ECF-funded services to continue to be funded through the E-Rate program after the ECF program sunsets. Will the proposed $200 million budget help alleviate any concerns about the impact that this Pilot may

have on the USF? How can the Commission best balance the need to provide funding for cybersecurity and advanced firewall services with its responsibility as a careful and prudent steward of limited federal resources?

18. Should the Commission establish a maximum funding cap per Pilot participant? Should the Commission establish a per-student cap (and a corresponding cap on libraries based on their square footage), based on commercially available costs? Are there data sources for cost information that would be appropriate to use in setting such a cap? Or should the Commission allow selected Pilot participants to receive a different amount of funding that aligns with their application? Should the Commission adjust awards based on the Pilot participant's category two discount rate level? Should Pilot participants be required to contribute and be responsible for a portion of the costs in order to receive Pilot program funding? For example, the Commission proposes that Pilot participants will be subject to their current category two discount rate as the non-discounted share of costs for the Pilot program; should the Commission instead require participants to contribute a fixed percentage of the costs of the services and equipment purchased? How can the Commission ensure Pilot participants are making cost-effective purchases through this Pilot program?

19. Should the Commission disburse a smaller amount of funding to a larger number of Pilot participants to increase the total volume of cybersecurity data available? Or should the Commission disburse a larger amount of funding to fewer Pilot participants to obtain a more holistic look at how the support could best be used to protect E-Rate-funded broadband networks and data, as well as help K-12 schools and libraries address cybersecurity issues? Which approach would generate the best data to determine whether and how universal service support could most effectively be leveraged to help K-12 schools and libraries protect their E-Rate-funded broadband networks and data from targeted cyberattacks and other cyber threats?

20. Under its proposals, once selected, Pilot participants will be required to submit funding applications for the requested services and equipment. To ease administration of the Pilot, the Commission proposes that participants be permitted to seek funding for services and equipment to be

provided over the proposed three-year term in a single application and be supported by multi-year contract/agreement(s) for this term. The Commission seeks comment on these proposals and questions.

21. The Commission next discuss what types of entities should be eligible to participate in the proposed Pilot program. In doing so, the Commission notes that the number and type of schools and libraries that participate in the E-Rate program vary significantly. Who should be eligible to participate in the Pilot program and how should the Commission select Pilot participants? How can the Commission ensure that it identifies a wide cross-section of Pilot participants to allow it to evaluate the effectiveness of providing universal service support for K-12 schools' and libraries' cybersecurity needs, and do so in a fair and transparent manner? Should the Commission limit eligibility to schools and libraries currently participating in the E-Rate program or should it expand eligibility to include schools and libraries that do not currently participate in the E-Rate program? Should the Commission select Pilot participants based on specific objective factors like: E-Rate category two discount rate levels; location (e.g., urban vs. rural); and/or participant size (i.e., small schools, school districts, and libraries vs. large schools, school districts, and libraries)? How should the Commission define, or what sources should the Commission use to define, these factors to ensure they are applied objectively? Are any of these factors (i.e., discount rate level, urban vs. rural, large vs. small) more or less important than others from an eligibility perspective? If yes, why are particular factors more or less important than others? Are there other factors the Commission should consider when determining who should be eligible to participate in the Pilot and how participants should be selected? For example, would the Pilot benefit from including schools and libraries that have advanced expertise in cybersecurity as participants because they presumably would know how to best spend the Pilot funding? Or, should cybersecurity expertise not be a factor at all in the selection of Pilot participants? How can the Commission ensure that schools and libraries that lack funding, expertise, or are otherwise under-resourced can meaningfully participate in the Pilot? Is there a way to compare the cybersecurity performance of Pilot participants against non-participants (e.g., through the use of a survey or other data collection process) in a way that contrasts the current cybersecurity posture of Pilot participants with that of non-

participants? To be eligible for the Pilot program, should Pilot participants be required to demonstrate that they have started taking actions to improve their cybersecurity posture by, for example, starting to implement some of the DOE and CISA K-12 cybersecurity recommendations or potential forthcoming Council guidance or other similar actions? Or conversely, should a school or library 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? The Commission seeks comment on these preliminary participant eligibility questions.

22. In today's broadband-reliant environment, there are a plethora of evolving cyber threats and attacks. Should the Commission limit schools' and libraries' eligibility to participate in the Pilot program to those schools and libraries that have faced or are facing certain types of cyber threats or attacks? If so, which cyber threats or attacks should qualify a school or library for participation in the Pilot program? Are there certain types of cyber threats or attacks that schools and libraries most commonly face and are there any emerging cyber threats or attacks that have only recently arisen? What types of cyber threats or attacks are the most harmful or costly for schools or libraries to combat and/or recover from? What difficulties have schools and libraries faced when attempting to address cyber threats and attacks on their own? The Commission seeks comment on the types of cyber threats and attacks encountered by schools and libraries and how they should be evaluated, if at all, when selecting Pilot participants.

23. Past experience also indicates that there may be common cyber threats and attacks faced by K-12 schools, school districts, and libraries regardless of their particular characteristics (e.g., urban vs. rural, and large vs. small). However, the history of attacks also indicates that certain K-12 schools and libraries may be more likely than others to be targeted by malicious actors due to lack of information technology (IT) funding or constrained staff resources. When selecting Pilot participants, should the Commission consider an applicant's previous history regarding cyber threats or attacks? If yes, should the Commission select as Pilot participants schools and libraries with greater or fewer cyber incidents? How should the Commission define, or what sources should it use to define, a "greater"

versus "fewer" number of cyber incidents? Should the Commission assess "greater" or "fewer" in absolute terms or relative terms? For instance, should a school district with 100,000 students and school staff that faces 1,000 cyber incidents per year be viewed as having more incidents than a school district with 10,000 students and school staff that faces 900 incidents per year? Or, should the latter school district be seen as having more cyber incidents on a per-student and school staff member basis? Would the Pilot benefit from including both schools and libraries that have never experienced a cyber threat or attack, as well as those that have experienced at least one cyber threat or attack? In commenters' experience, are there certain types of schools or libraries that are more likely to face cyber threats or attacks? Are schools or libraries in certain geographic or socioeconomic settings more vulnerable than others to cyber threats or attacks? What role does lack of IT funding or constrained staffing resources play in the likelihood or frequency of cyber threats or attacks? When selecting Pilot participants, should cybersecurity risk, geographic or socioeconomic factors, staffing constraints or financial need, or technical challenges play a role in participant selection? The Commission seeks comment on the characteristics and circumstances that may result in a school or library being more or less likely to be targeted for a cyber threat or attack, and the role those characteristics should play in Pilot participant selection. Are there ways to ensure that under-resourced schools and libraries can meaningfully participate in the Pilot? For example, should the Commission direct USAC to provide assistance to schools and libraries that are under-resourced and may lack experience to assist them throughout the Pilot? The Commission also encourages commenters to share any first-hand knowledge they may have regarding factors that may increase or decrease the likelihood of a school or library being targeted for a cyber threat or attack, and discuss if or how that information should be considered in the Pilot participant selection process.

24. *Prerequisites*. There are a number of free and low-cost cybersecurity tools and resources available to K-12 schools and libraries. Should the Commission adopt any prerequisites for Pilot program participation? For example, should Pilot participants be required to take a more active role in improving/enhancing their cybersecurity posture? If so, how should this be monitored and enforced? For example, should Pilot participants be required to correct known security flaws and

conduct routine backups as part of this Pilot program? Should Pilot participants be required to participate in other federal efforts to share cybersecurity information and resources, such as the MS-ISAC or the K12 SIX? Should Pilot participants be required to implement, or demonstrate how they plan to implement, recommended best practices from organizations like the DOE, CISA, and NIST, as they are able? Should Pilot participants be required to take steps on their own to improve their cybersecurity posture by, for example, designating an officer or other senior-level staff member responsible for cybersecurity implementation, updates, and oversight, or implementing a cybersecurity training program for their staff and network users? The Commission seeks comment on these questions.

25. Should the Commission only include as Pilot participants those schools and libraries that have already implemented or are in the process of implementing CISA's K-12 cybersecurity recommendations, or have otherwise begun the process of implementing a cybersecurity framework or program? Are there any schools or libraries that have implemented or are in the process of implementing the DOE's or CISA's K-12 cybersecurity recommendations or another cybersecurity framework or program, to protect their E-Rate-funded networks and data? If so, what actions have been the most successful in establishing and implementing cybersecurity recommendations, or a cybersecurity framework or program? The Commission also asks schools and libraries that are already implementing or experimenting with CISA's K-12 cybersecurity recommendations, or another cybersecurity framework or program, to provide us with information about their cybersecurity projects and discuss how these actions should influence, if at all, the Pilot participant selection process. For schools and libraries that have not taken any preventative or mitigating actions, what are the key impediments to implementing a more robust cybersecurity posture? If cost is the reason that schools or libraries have been unable to implement and strengthen their cybersecurity posture, is there other federal, state, or local funding available that could be used in place of or in addition to universal service funding to help address cyber threats and attacks? If other sources of funding are available, should schools and libraries be required to seek or already have obtained cybersecurity funding commitments from other federal, state, or local sources to be eligible to participate in this proposed Pilot program?

The Commission seek comment on what prerequisites, if any, should be adopted to be a Pilot participant.

26. In the *December 2022 Public Notice*, the Commission sought comment on "the specific equipment and services that E-Rate should . . . fund as advanced or next-generation firewalls and services." Nearly all commenters who opined on this topic advocated for the eligibility of at least next-generation firewalls. Many of these commenters further advocated for the eligibility of a range of additional security measures, including some or all of: MFA, domain name system (DNS) security, distributed denial-of-service (DDoS) protection, and/or VPN. On the other hand, a small number of commenters urged the Commission to adopt general criteria for eligibility, rather than enumerate specific technologies (e.g., firewalls) as eligible, believing that this approach would provide E-Rate participants with appropriate flexibility in addressing their individualized security needs and ultimately better ensure the security of E-Rate-supported networks.

27. Commenters, however, were opining on security measures that would be appropriate for inclusion in the E-Rate program rather than on security measures that would be appropriate for inclusion in today's proposed Pilot. Therefore, to resolve any ambiguity and further develop the record specifically as to the proposed Pilot, the Commission seeks further comment on the security measures, including equipment and services, that should be made eligible to participants in the Pilot. The Commission also seeks comment on whether it should place restrictions on the manner or timing of a Pilot participant's purchase of security measures. For example, should Pilot funding be limited to a participant's one-time purchase of security measures or should the support 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 notes that an appropriate set of eligible measures and the timing for the security measures would balance its goal of using the Pilot to meaningfully assess the effectiveness of a wide range of different security approaches with the need to conserve and efficiently use the limited funding available for the Pilot to gain sufficient insight into each of those approaches. As a preliminary point, the Commission seeks comment on whether it should

specify eligibility in terms of general criteria rather than as a list of specific technologies. If so, what should the eligibility criteria be? For example, should the Commission adopts the Schools, Health & Libraries Broadband Coalition's (SHLB Coalition) proposed general criteria that would deem any security measure eligible as long as it "keep[s] the network from being shut down and . . . protect[s] the privacy of user data" or would some other general criteria be more appropriate? SHLB Coalition's views notwithstanding, the Commission believes that specifying an enumerated list of eligible security technologies/measures would provide more specific, and thus clearer, eligibility guidance to Pilot participants than would general eligibility criteria, ultimately leading to a more efficient use of the Pilot program's funds. A finite list of allowable cybersecurity options would also make comparisons of outcomes more tractable across Pilot participants. On the other hand, are there concerns that potential evolutions in security measures/technologies during the duration of the Pilot would render an enumerated Commission list of eligible technologies/measures outdated before the end of the Pilot? Are there concerns that limited Pilot funds could be used inefficiently, or misused, if the Commission adopts an approach based on generalized criteria? Should eligibility be limited to cybersecurity measures that are primarily or significantly used to facilitate connectivity? How does section 254 limit the kinds of cybersecurity solutions that can be purchased, and how they may be deployed, using pilot funds? The Commission seeks comment on these issues and more generally on the relative advantages and disadvantages of specifying eligibility in terms of an enumerated list of security measures/technologies as compared to general criteria.

28. If the Commission adopts a list of eligible measures/technologies, at what granularity should that list be specified? For example, should the Commission publish a specific list of security measures (similar to the Eligible Services List for the E-Rate program), to help participants understand which services and equipment are eligible for support through the proposed Pilot program? Should a list of resources from MS-ISAC be included in the application, so that applicants can easily select desired services from the list, thereby simplifying the application process? Moreover, what are the specific measures that should be included on that list? The Commission notes that a number of commenters opined that new security measures should be limited to advanced and next-generation firewalls, in the

context of discussing the E-Rate program. Are these the most important tools schools and libraries could adopt and how does the import of these cybersecurity tools compare to other tools identified in the record? For example, CISA and the DOE have identified things like MFA, regular software and hardware updates, and regular backups as important tools for combatting network threats. Do commenters continue to believe that focusing funding efforts primarily or exclusively on advanced and next-generation firewalls is appropriate in the context of today's proposed Pilot, which would utilize separate USF funding and aims to evaluate the effectiveness of a wide range of security approaches? If the list of eligible security measures should be more expansive than advanced firewalls in the context of today's Pilot, which other measures should be included? For example, should the Commission determine eligible measures based on the recommendations from the CISA K-12 Cybersecurity Report, the DOE K-12 Digital Infrastructure Briefs, and/or other federal partner resources and guides. If so, how?

29. Moreover, the Commission notes that while nearly all commenters advocated for the eligibility of at least advanced or next-generation firewalls and services, commenters generally disagree on which features an "advanced firewall" service includes. For example, commenters variously opined that advanced firewalls should include some or all of: intrusion detection and prevention, application-level inspection, anti-malware and anti-virus protection, VPN, DNS security, DDoS protection, and content filtering. If the Commission were to make advanced firewall services eligible, how should "advanced firewall" be defined for the purposes of the proposed Pilot program? Alternatively, given the lack of consensus around the scope of these terms, and the import of this technology, should the Commission simply make "firewalls" eligible for the Pilot without regard to whether they are "basic" or "advanced/next-generation" as has been suggested to the Commission? If the Commission were to adopt a single, updated "firewalls" definition for purposes of the Pilot that includes advanced or next-generation firewalls, should the definition encompass intrusion detection and prevention, application-level inspection, anti-malware and anti-virus protection, VPN, DNS security, DDoS protection, and content filtering and/or other measures/technologies? Given the limited amount of funding available,

which of these measures/technologies should the Commission prioritize for inclusion within a broader definition of "firewall" and for what reasons?

30. The Commission further proposes to limit Pilot 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. To be eligible for the Pilot, the Commission further proposes that the equipment or services be 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 notes that this proposed eligibility criteria would apply regardless of whether the equipment or services are located within a school's or library's classroom or other physical premises. The Commission believes that this eligibility criteria, which is not restricted to physical premises, would provide schools and libraries with the flexibility to cost-effectively procure remotely-located equipment and services obviating a potentially costly need to install, maintain, and troubleshoot solutions on-site. The Commission also believes that this approach is consistent with the way that many modern security services are increasingly offered, i.e., as a remotely-located or cloud-based, centralized resource accessible via the Internet. The Commission further believes that limiting eligible services to end-user devices owned or leased by a school or library strikes a reasonable balance between protecting those entities' networks with the need to limit the scope of protections given the limited Pilot funding available. The Commission believes that its approach also reflects the reality that schools and libraries often already restrict the permissions available to third-party-owned devices that connect to their networks. The Commission seeks comment on this proposed scope of eligibility or any further restrictions, or relaxation of this proposal, that would best protect school and library broadband networks at a reasonable cost.

31. As noted, the DOE and CISA K-12 cybersecurity recommendations describe a broad range of steps that K-12 entities may utilize to address cybersecurity risks, and many of these steps go beyond the types of specific firewall and technical technologies/measures that the Commission has

traditionally deemed eligible for reimbursement within the context of the E-Rate program. For example, the DOE and CISA recommend that entities develop a mature cybersecurity plan, leverage existing free or low-cost cybersecurity services, negotiate for the inclusion of certain services with their technology providers, and engage in strategic collaboration, information-sharing, and relationship-building with other entities. CISA's CPGs similarly recommend a broad range of cybersecurity practices, including practices related to asset management, organizational cybersecurity leadership structure, and reporting processes, that entities may use to reduce their cyber risk and help them develop the cybersecurity plan needed to implement the NIST Cybersecurity Framework (CSF). These recommendations again involve actions that go beyond the traditional measures that the Commission has found to be eligible for reimbursement in the E-Rate program.

32. The Commission thus seeks comment on whether it should allow participants to use Pilot funds to meet any of the DOE or CISA K-12 cybersecurity recommendations or CISA CPGs, or otherwise improve/enhance their cybersecurity posture and, if so, what the appropriate restrictions or limitations on the eligibility of such measures should be. Does the Commission have legal authority to allow spending on these broader DOE and CISA recommendations and CISA CPGs? If so, based on which statutory provisions and other sources of authority? Alternatively, should Pilot funding be limited to equipment and services that can directly protect the E-Rate-funded broadband networks and data, as has traditionally been the case within the E-Rate program?

33. Similarly, does the Commission have legal authority to fund broader steps that entities may take to address cybersecurity risks, such as through staff or user cybersecurity training, that are necessary parts of a K-12 school's or library's cybersecurity plan/framework as part of this proposed Pilot program? Or should staff and user cybersecurity training be treated similarly as the necessary resources needed to be able to participate in the Pilot program, similar to the necessary resources rule for the E-Rate program? As discussed earlier, CISA has provided a number of free and low-cost K-12 cybersecurity tools and resources, including staff and user cybersecurity training in Appendix 1 to its K-

12 Cybersecurity Report. The Commission seeks comment on these questions and what services and equipment should be eligible for support in the Pilot program.

34. The Commission proposes that Pilot participants comply with the new proposed rules, that largely reflect and mirror its existing E-Rate rules, including by requiring competitive bidding, prohibiting gifts, and requiring that a participant pay its non-discounted portion of the costs of the supported services. The Commission believes that this approach is appropriate given the structural similarities of E-Rate and the Pilot, which is designed to study the expansion of equipment and services supported by E-Rate program. The Commission believes that the Pilot rules are likely to be effective for the same reason that the E-Rate rules, which have been developed and refined by it over many years, have proven to be effective. The Commission further believes that by modeling today's proposed rules on the existing E-Rate rules, it would ease compliance burdens for Pilot participants who are likely already familiar with, and have appropriate compliance measures in place to address, existing E-Rate program requirements. The Commission seeks comment on today's proposed rules and these preliminary conclusions.

35. While today's proposed rules would mirror in most respects the Commission's E-Rate rules, it proposes some deviations from those rules. For example, the Commission proposes to adopt several rules from the ECF program that are not included in the E-Rate rules. First, the Commission proposes to use the shorter timeframe for appealing a decision by USAC or requesting a waiver of the Commission's rules. Second, the Commission proposes that invoices must also be submitted along with the request for reimbursement, as required in the ECF program. The Commission believes that these two deviations from the E-Rate rules will work better for the Pilot program as it is a short-term program, similar to the ECF program. The Commission seeks comment on these proposals. The Commission also seeks comment on whether any of today's proposed rules should not be adopted, or adopted in a different form than proposed for logical, policy, administrative, or other reasons. For example, should the Commission allow Pilot participants to select the invoicing mode, as is required in the E-Rate rules? Or should the service provider be required to affirmatively agree to invoice on behalf of the Pilot

participant as required in the ECF rules? The Commission tentatively concludes that it should allow Pilot participants to determine which invoicing mode will be used and the Commission seeks comment on these questions and tentative conclusion. In providing comments, the Commission requests that commenters provide specific cites to relevant provisions of the proposed rules and, if instructive, the E-Rate rules. The Commission also requests that commenters describe any proposed rule modifications in detail. The Commission also seeks comment on whether it should promulgate any additional new rules, specific to the Pilot program. For example, what rules might the Commission adopt to ensure the collection of data that will aid it in evaluating the effectiveness of various cybersecurity approaches via the Pilot and an application filing window for the selection of Pilot participants?

36. The Commission also proposes to create a standardized set of forms for the Pilot as it believes this will both increase administrative efficiency and reduce burdens for the Pilot participants. The Commission's proposals is informed by its significant experience creating and employing standardized forms in a number of USF programs, including E-Rate, ECF, and the Connected Care Pilot Program. The Commission seeks comment on whether its objectives of administrative efficiency and minimizing Pilot participant burdens would best be met if the Commission leverages the forms used in its other USF programs as a starting point for creating forms for the Pilot. Based on its experience with E-Rate and ECF, in particular, the Commission proposes to create new forms for the Pilot participants that mirror the E-Rate FCC Form 470: Description of Services Requested and Certification Form; E-Rate/ECF FCC Form 471: Description of Services Ordered and Certification Form; E-Rate/ECF FCC Form 472: Billed Entity Applicant Reimbursement (BEAR) Form; and the E-Rate/ECF FCC Form 474: Service Provider Invoice (SPI) Form. The new Pilot forms would thus allow participants to: (i) request Pilot-eligible services and equipment and open the competitive bidding process among vendors of these services and equipment; (ii) describe services and equipment the participant ordered after competitive bidding and request applicable discounts on the services and equipment; (iii) request reimbursement from USAC for the discounted costs of eligible services and equipment that have been approved by USAC and for which the applicant has received and paid for in full (i.e., BEAR invoicing); and (iv) request reimbursement from USAC for the discounted costs of eligible services and equipment that have been

approved by USAC for which the applicant has received and paid the non-discounted portion to the service provider (i.e., SPI invoicing), respectively. The Commission seeks comment on its proposals to use these forms for the Pilot. The Commission further proposes to create a new Pilot participant application form (Form 484) that will collect the data proposed in paragraph 27 of the *NPRM*. The Commission will still leverage the data available in the E-Rate Productivity Center (EPC) and the ECF Portal to streamline the application process by auto-populating with Pilot applicant data that is already available through the E-Rate and ECF online systems. The Commission seeks comment on this proposal.

37. The Commission also seeks comment on whether any other new forms, processes, and software systems are needed or would be beneficial for the Pilot and on how these should be structured. For example, can the Commission leverage existing E-Rate or ECF forms, processes, and software systems for the disbursement of funding in the Pilot program? Additionally, can the Pilot incorporate the existing E-Rate or ECF processes and software systems for seeking bids, requesting funding, and requesting disbursements/invoicing? What challenges or obstacles to using existing E-Rate or ECF forms, processes, and software systems exist, if any, and how can the Commission address them in the Pilot? Can the Pilot leverage existing E-Rate or ECF invoicing procedures, including the program's associated deadlines for submitting invoices, and what modifications, if any, should be made to these deadlines to better reflect the structure of today's Pilot program as compared to the E-Rate or ECF programs? For example, how should the Commission define and implement a service delivery date for the Pilot program given its limited three-year duration? The Commission seeks detailed comment on these questions.

38. The Commission also seeks comment on steps the Commission can take to protect the program integrity of the Pilot and its limited USF funds. Should the Commission apply the E-Rate and/or ECF program integrity rules to the Pilot and, if so, what modifications, if any, should the Commission make to those rules? The Commission proposes similar program integrity protections, for example, document retention requirements, audits, site visits, and other methods of review in the Pilot program. The Commission seeks comment on these proposals and questions. To further protect program

integrity, the Commission also proposes that that it apply its existing USF suspension and debarment rules to the Pilot. The Commission additionally notes that it is considering whether to update its suspension and debarment rules to provide it with broader and more flexible authority to promptly remove bad actors from participating in USF and other programs in a separate, pending proceeding. To the extent that this proceeding is resolved and results in final rules prior to or during the duration of the Pilot program, the Commission proposes to apply the updated rules to the Pilot program. The Commission believes that the steps outlined here would strike an appropriate balance between encouraging active participation in the Pilot by various schools and libraries and protecting the program integrity of the Pilot and its limited funds. The Commission seeks comment on its proposals, including the sufficiency of its legal authority to take its proposed actions, and any additional or alternative steps the Commission should take to safeguard the integrity of the proposed Pilot.

39. These proposals would create a Pilot that allows participants to receive universal service support for cybersecurity and advanced firewall services, an expansion of the basic firewall services currently allowed in the E-Rate program. In the *December 2022 Public Notice*, the Commission sought comment on whether it had sufficient legal authority for funding advanced firewall services, including pursuant to sections 254(c)(1), (c)(3), (h)(1)(B), and (h)(2) of the Communications Act, and any other legal issues or concerns it should consider based on the proposals. All commenters who opined agreed that the Commission had sufficient legal authority to fund advanced firewall equipment and services. The record thus indicates that it has sufficient legal authority for today's proposed Pilot. The Commission seeks comment on this view and on the other aspects of legal authority raised below.

40. As a preliminary matter, the record to date supports commenters' views that today's Pilot, which would use USF funding to support the provision of cybersecurity and advanced firewall services to participating schools and libraries, is consistent with Congress's view that the USF represents an evolving level of service. The Commission finds it likely that the results of the Pilot would inform potential future actions that it takes to further its obligation to "establish periodically" universal service rules that "tak[e] into account advances in telecommunications and information technologies and

services." The utility and necessity of the proposed new services, including cybersecurity and advanced firewall services, reflects ongoing advances in networks and the associated threats that schools' and libraries' broadband networks face today compared to in years past. The Commission seeks comments on these views.

41. The record supports commenters' view that the Commission has legal basis for today's proposed Pilot pursuant to section 254(h)(2)(A) of the Communications Act "to enhance, to the extent technically feasible and economically reasonable, access to advanced telecommunications and information services for all public and nonprofit elementary and secondary school classrooms . . . and libraries . . ." based on two distinct views. First, the proposed Pilot could make a number of new services, including, for example, advanced and next-generation firewalls, VPNs, intrusion detection and prevention protection, DNS security, and/or DDoS protection, directly available to participants. Each of these services is itself an "advanced telecommunications" and/or "information service" as each filters the information permitted to influence and affect participants' telecommunications networks. Second, the proposed new services would remediate many common types of cyber threats that would otherwise dimmish the ability of schools and libraries to use their existing "advanced telecommunications and information services" (e.g., the Internet), thereby meaningfully "enhanc[ing]" their access to the existing services. The Commission seeks comment on these two views. For example, according to the first view, to what extent are the services included in today's pilot proposal themselves "advanced telecommunications and information services" within the meaning of section 254(h)(2) of the Communications Act?

42. In addition, the Commission believes that by taking steps to deter harm to a school or library network when it is accessed remotely on end-user devices that are owned or leased by the school or library, it is necessarily also ensuring that the same network would remain functional when accessed from within a traditional school classroom or a library's physical premises. This reflects the fact that students can access school networks before or after school hours to complete homework and other assignments, which often occurs from the home or another location outside of the school

premises. The Commission seeks comment on these views, generally on its legal authority for today's proposals and on the physical spaces that qualify for eligible equipment and services, whether based on legal authority considerations or other practical concerns.

43. The Commission further believes that today's Pilot is "technically feasible and economically reasonable" as required by section 254(h)(2)(A) of the Communications Act. While the Commission has previously expressed a view, as recently as 2019, that any expansion of cybersecurity services beyond basic firewall services may be cost-prohibitive to the E-Rate program, the Commission seeks comment on whether changed circumstances in the years since that determination (and earlier Commission determinations) warrant today's proposed Pilot. As discussed, the COVID-19 pandemic changed the extent to which K-12 schools and libraries utilize their networks to deliver quality education and learning materials off-premises to students and patrons. Moreover, since 2021, Congress, CISA, GAO, and other federal agencies have effectuated legislation or taken other actions to study how the number and variety of cyberthreats facing K-12 schools and libraries continues to evolve. The Commission believes that today's Pilot reflects these actions by seeking to better understand the nature of current cyber threats faced by K-12 schools and libraries participating in the E-Rate program. Moreover, the Commission has designed the Pilot to limit USF expenditures until the nature of any significant threats are understood based on the Pilot's results in several ways. One, the costs of today's proposals would fall entirely within a time-limited, three-year USF-supported Pilot program, and not would not draw from the budget for the E-Rate program. Two, the costs would be mitigated because the Commission proposes that the participants be required to leverage other free and low-cost K-12 cybersecurity tools and services as part of their cybersecurity action plans. The Commission expects to obtain results from the Pilot that will enable us to make informed long-term decisions on whether any of the equipment and services studied in the program would be cost-effective to include in E-Rate, should it address that matter through subsequent Commission action. The Commission expects these steps will lead to lower USF costs as the burden for K-12 cybersecurity protection will not be borne solely by the E-Rate program or other universal service program funding. The Commission seeks comment on these views.

44. The record also supports commenters' view that the Commission has an additional legal basis for structuring the Pilot program as proposed today pursuant to section 254(c)(3) of the Communications Act. This section grants the Commission authority to "designate additional services for [USF] support . . . for schools [and] libraries." The Commission's proposed Pilot is consistent with this authority, the record indicates, as the Pilot would allow for the designation of additional services that may be used by participating schools and libraries based on USF funding. Moreover, the results of the proposed Pilot program could be used by the Commission to inform potential further actions to facilitate the availability of these services to schools and libraries based on the USF. The Commission seeks comment on these preliminary conclusions.

45. *Other Legal Bases and Considerations*. The Commission seeks comment on the extent to which the cybersecurity and advanced firewall services made available through its proposed Pilot fulfill its mandate to make "[q]uality services" available at just, reasonable, and affordable rates. Does ensuring that E-Rate-funded networks are able to implement strong and up-to-date cybersecurity measures, through the services funded through this Pilot program, further this statutory goal and, if so, how does ensuring the protection and privacy of school and library networks contribute to the provision of "[q]uality services"?

46. The record to date indicates that the statutory bases identified, taken collectively or individually, provide sufficient authority for the Commission's proposals. The Commission seeks comment on this view. The Commission also seeks comment on any other sources of legal authority, or constraints on such authority, that could bear on or otherwise impact today's proposals. For example, does the Commission have bases for its proposals based on its authority to set discounted rates for certain services provided to schools and libraries pursuant to section 254(h)(1)(B) of the Communications Act? Relatedly, do the services made eligible in today's Pilot fall within the scope of services that telecommunications carriers can be required to provide pursuant to this statute?

47. *Limits and Restrictions*. The Commission further seeks comment on any other limits and restrictions that it should place on recipients of Pilot funds to remain within the statutory authority

identified and on any other legal requirements that apply to its implementation of the proposed Pilot program. For example, should recipients of Pilot funds be barred from selling, reselling, or otherwise transferring the services that they receive using funds provided for by the Pilot program? The Commission proposes to apply the Secure and Trusted Communications Networks Act of 2021 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 equipment or services on the Commission's Covered List or to maintain any of the equipment or services on the Covered List that was previously purchased, rented, leased, or otherwise obtained. The Commission seeks comment on this proposal and on whether there are any other restrictions or requirements that it should place on recipients of Pilot funds based on the Secure Networks Act and/or other related concerns related to supply chain security. Should Pilot participants be required to refund the USF any unused money, including if they withdraw from the Pilot program?

48. *The Children's Internet Protection Act.* The Commission also seeks comment on the applicability of the Children's Internet Protection Act (CIPA) to the Pilot program and USF-funded cybersecurity and advanced firewall services for schools and libraries. Congress enacted CIPA to protect children from exposure to harmful material while accessing the Internet from a school or library. In enacting CIPA, Congress was particularly concerned with protecting children from exposure to material that was obscene, child pornography, or otherwise inappropriate for minors (i.e., harmful content). CIPA prohibits certain schools and libraries from receiving funding under section 254(h)(1)(B) of the Communications Act for Internet access, Internet service, or internal connections, unless they comply with specific Internet safety requirements. Specifically, CIPA applies to schools and libraries "having computers with Internet access," and requires each such school or library to certify that it is enforcing a policy of Internet safety that includes the operation of a technology protection measure "with respect to any of its computers with Internet access." Schools, but not libraries, must also monitor the online activities of minors and provide education about appropriate online behavior, including warnings against cyberbullying.

49. In the *Emergency Connectivity Fund Report and Order,* 86 FR 29136, May 28, 2021, the Commission found that receipt of ECF- or E-Rate-funds for recurring Internet access, Internet services, or internal connections (if any) triggers CIPA compliance when used with any school- or library-owned computer, even if used off-premises. On the other hand, the Commission determined that CIPA does not apply to the use of any third-party-owned device, even if that device is connecting to a school's or library's E-Rate- or ECF-funded Internet access or Internet service. The Commission seeks comment on what impact its interpretation of CIPA in the *Emergency Connectivity Fund Report and Order* has on the Pilot or USF-funded cybersecurity and advanced firewall services.

50. At the time of CIPA's enactment, schools and libraries primarily owned one or two stationary computer terminals that were used solely on-premises. Today, it is commonplace for students, school staff, and library patrons to carry Internet-enabled devices onto school or library premises and for schools and libraries to allow third-party-owned devices access to their Internet and broadband networks. The Commission invites comment on the scope of its authority to impose CIPA requirements on third-party devices that may connect with school- or library-owned broadband networks as part of this Pilot program or school- and library-owned broadband networks funded with USF support, and whether the imposition of such requirements would be appropriate. Similarly, the Commission invites comment on whether the requirements of CIPA should apply to USF-funded cybersecurity and advanced firewall services (e.g., cybersecurity software) if placed on third-party owned devices that connect to a school- or library-owned broadband network.

51. Finally, the Commission acknowledges there are privacy concerns related to certain CIPA requirements, particularly as it relates to students' and library patrons' data that is often subject to various federal and/or state privacy laws. The Commission seeks comment on these privacy issues and any privacy concerns commenters may have about the application of CIPA to this Pilot program or USF-funded cybersecurity and advanced firewall services for schools and libraries.

52. The Commission, as part of its continuing effort to advance digital equity for all, including people of color, persons with disabilities, persons who live in rural or Tribal areas, and others

who are or have been historically underserved, marginalized, or adversely affected by persistent poverty or inequality, invites comment on any equity-related considerations and benefits (if any) that may be associated with the proposals and issues discussed herein. Specifically, the Commission seeks comment on how its proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility, as well the scope of its relevant legal authority.

III. PROCEDURAL MATTERS

53. *Regulatory Flexibility Act.* As required by the Regulatory Flexibility Act of 1980, as amended (RFA), the Commission has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities by the policies and rules proposed in the *Schools and Libraries Cybersecurity Pilot Program, Notice of Proposed Rulemaking* (*NPRM*). Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments in the *NPRM.* The Commission will send a copy of the *NPRM*, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).

54. In the *NPRM*, the Commission proposes a Schools and Libraries Cybersecurity Pilot Program (Pilot) that will assist us in obtaining valuable data to satisfy the requirements to support cybersecurity and advanced firewall services for eligible schools and libraries. The Commission seeks comment on what role the federal Universal Service Fund (USF) could play in helping K-12 schools and libraries protect their E-Rate-funded broadband networks and data, and improve their ability to defend against the cyber threats and attacks that have increasingly been targeting K-12 schools and libraries, and their students' and patrons' data. The Commission expects that the data gathered from the Pilot will help us understand whether and how USF funds could best be leveraged to help address the K-12 cybersecurity challenges, and the data and information collected through this Pilot may also aid in the consideration of broader reforms—whether statutory changes or updates to rules—that could support helping schools and libraries address the significant K-12 cybersecurity concerns that impact them.

55. First, the Commission proposes three goals for the proposed Pilot and that the Pilot be for a three-year term with a budget of $200 million. These include: (1) improving the security and protection of E-Rate-funded broadband networks and user data; (2) measuring the costs associated with cybersecurity and advanced firewall services, and the amount of funding needed to adequately meet the demand for these services if extended to all E-Rate participants; and (3) evaluating how to leverage other federal K-12 cybersecurity tools and resources to help schools and libraries effectively address their cybersecurity-related needs. Second, the Commission proposes that interested K-12 schools and libraries apply to be Pilot participants by submitting an application containing information about how they would use the Pilot funds and providing information about their proposed cybersecurity and advanced firewall projects. The Commission also seeks comment on the application process and the objective criteria for selecting participants among the applications it receives for the Pilot. In addition, the Commission proposes that Pilot participants be permitted to seek funding for services and equipment to be provided over the proposed three-year term. The Commission further proposes that Pilot participants submit a single application with their funding requests that will be relied on for the proposed three-year term of the Pilot and be supported by multi-year contract(s)/agreement(s) for this term. The Commission also seeks comment on the extent to which E-Rate or ECF program processes, rules, and forms could be leveraged and adopted to apply to the proposed Pilot, including, for example, competitive bidding, funding disbursement, invoicing, document retention, and auditing processes, rules, and forms. Finally, the Commission seeks comment on its legal authority to establish the proposed Pilot and the applicability of the Children's Internet Protection Act (CIPA) to the proposed Pilot. The Commissions believe that, through the Pilot, it will be able to fund a range of diverse cybersecurity projects for K-12 schools and libraries throughout the country.

56. The proposed actions are authorized pursuant to 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 through 154, 201 through 202, 254, 303(r), and 403.

57. 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 proposed rules, if adopted. 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).

58. *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.

59. 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 2020, there were approximately 447,689 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.

60. 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 2017 Census of Governments indicate there were 90,075 local governmental jurisdictions consisting of general

purpose governments and special purpose governments in the United States. Of this number, there were 36,931 general purpose governments (county, municipal, and town or township) with populations of less than 50,000 and 12,040 special purpose governments—independent school districts with enrollment populations of less than 50,000. Accordingly, based on the 2017 U.S. Census of Governments data, the Commission estimates that at least 48,971 entities fall into the category of "small governmental jurisdictions."

61. Small entities potentially affected by the rules herein include 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.

62. In the *NPRM*, the Commission seeks comment on a proposed Pilot with a $200 million budget and three-year duration, that would provide support for cybersecurity and advanced firewall services for eligible K-12 schools and libraries.

63. To participate in the Pilot, the *NPRM* proposes that interested K-12 schools and libraries apply by submitting an application containing information about how they would use the Pilot funds and providing information about their proposed cybersecurity and advanced firewall projects. All eligible schools and libraries that choose to participate may be required to collect and submit data as part of the application process, at regular intervals during the Pilot program and at the end of the Pilot, to the Universal Service Administrative Company (USAC) and the Commission. The collection of this information, which may go beyond that provided in FCC Forms 470 and 471, is necessary to evaluate the impact of the Pilot, including whether the Pilot achieves its goals. This includes the proposed evaluation

process, with annual and final progress reports detailing use of funds and effectiveness of the program. It is expected that the benefits of collecting this information will outweigh any potential costs.

64. Application requirements will necessitate that small entities make an assessment of their cybersecurity posture and services needed to address risks, which may require additional staff and/or staff with related expertise. The proposal to incorporate the existing E-Rate forms, processes, and software systems for seeking bids, requesting funding, and requesting disbursement/invoicing into the proposed Pilot may decrease the burden on small entities that are already familiar with these requirements. This may result in proposals from small entities that lessen the economic impact of the Pilot and increase their participation. In contrast, additional protections proposed in the *NPRM*, such as, document retention requirements, audits, site visits, and other methods of review in the Pilot, may require small entities to incur additional operational costs.

65. The *NPRM* also proposes that participants be permitted to seek funding for services and equipment to be provided over the proposed three-year term and be supported by multi-year contract(s)/agreement(s) for this term. The *NPRM* also considers whether to adopt prerequisites for Pilot participants, some of which may require small entities to acquire additional software, equipment, or staffing. For example, the *NPRM* seeks comment on whether Pilot participants should be limited to those schools and libraries that have already implemented or are in the process of implementing CISA's K-12 cybersecurity or other cybersecurity recommendations.

66. In assessing the cost of compliance for small entities, at this time the Commission cannot quantify the cost of compliance with any of the proposals that may be adopted. Further, the Commission is not in a position to determine whether, if adopted, the proposals and matters upon which the *NPRM* seeks comment will require small entities to hire professionals to comply. However, consistent with its objectives to leverage and adopt existing E-Rate processes and procedures, the Commission does not anticipate that small entities will be required to hire professionals to comply with any proposals the Commission adopt. The Commission expects the information it receives in comments, including, where requested, cost information, will help it and evaluate relevant compliance matters for

small entities, including compliance costs and other burdens that may result from potential changes discussed in the *NPRM*.

67. The RFA requires an agency to describe any significant, specifically small business, alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities."

68. The *NPRM* considers a number of alternatives which the Commission expects may have a beneficial impact on small entities. For example, allowing additional ramp-up time so that participants may prepare for the Pilot could benefit small entities that would need more time to implement cybersecurity measures. The funding proposals, including whether to distribute evenly over the three-year period and establishing funding caps, may impact the resources of small entities that would require flexibility to implement the Pilot program. Small entities may benefit from the *NPRM's* proposal to certify they do not have the resources to implement CISA's K-12 cybersecurity recommendations, as opposed to demonstrating that they have implemented those or similar actions. The *NPRM* proposes an application process that would encourage a wide variety of eligible schools and libraries to participate, including small entities. The Commission seeks to strike a balance between requiring applicants to submit enough information that would allow us to select high-quality, cost-effective projects that would best further the goals of the Pilot program, but also minimize the administrative burdens on small entities that seek to apply and participate in the Pilot.

69. The Commission does not expect the requirements for the proposed Pilot to have a significant economic impact on eligible K-12 schools and libraries for several reasons. The Commission expects to leverage and adopt existing E-Rate processes and procedures and also note that schools and libraries have the choice of whether to participate in the Pilot. The Bureau will also consider whether

the proposed projects will promote entrepreneurs and other small businesses in the provision and ownership of telecommunications and information services, consistent with section 257 of the Communications Act, including those that may be socially and economically disadvantaged businesses.

70. The Commission expects the information received in the comments to allow it to more fully consider ways to minimize the economic impact on small entities and explore additional alternatives to improve and simplify opportunities for small entities to participate in the Pilot.

71. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules. None.

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

73. *Ex Parte Rules – Permit but Disclose*. Pursuant to section 1.1200(a) of the Commission's rules, the *NPRM* shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules. Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda, or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings

(specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (e.g.,.doc,.xml,.ppt, searchable.pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

74. *Providing Accountability Through Transparency Act*. Consistent with the Providing Accountability Through Transparency Act, Public Law 118-9, a summary of this document will be available on https://www.fcc.gov/proposed-rulemakings.

IV. ORDERING CLAUSES

75. Accordingly, IT IS ORDERED that, pursuant to the authority found 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 through 154, 201 through 202, 254, 303(r), and 403, this Notice of Proposed Rulemaking IS ADOPTED.

76. IT IS FURTHER ORDERED that the Commission’s Office of the Secretary, Reference Information Center, SHALL SEND a copy of this Notice of Proposed Rulemaking, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

List of Subjects in 47 CFR Part 54

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

FEDERAL COMMUNICATIONS COMMISSION

Marlene Dortch,

Secretary.

Proposed Rules

For the reasons discussed in the preamble, the Federal Communications Commission proposes to amend 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 part 54 to read as follows:

Subpart T -- Schools and Libraries Cybersecurity Pilot Program

Secs.

§ 54.2000 Terms and Definitions.

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

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

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

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

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

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

Cyber threat. A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) 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 integrity.

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

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

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

Library. A "library includes:

(1) A public library;

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

(3) A Tribal library;

(4) An academic library;

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

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

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

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

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

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

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 Budget and Duration.

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

(b) *Duration*. The Schools and Libraries Cybersecurity Pilot Program shall make funding available to applicants selected to participate (in accordance with § 54.2004 of this

subpart) for three years, to begin when selected applicants are first eligible to receive eligible services and equipment.

§ 54.2002 Eligible Recipients.

(a) *Schools.*

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

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

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

(b) *Libraries*.

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

(2) Except as provided in paragraph (b)(4) of this section, a library's eligibility for universal service funding 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) For consortia, discounts under this subpart shall apply only to the portion of eligible services and equipment used by eligible schools and libraries.

(2) 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 listed in the Schools and Libraries Cybersecurity Pilot Program Eligible Services List, as updated in accordance with paragraph (b) of this section. 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 the universal service support mechanisms.

(b) *Schools and Libraries Cybersecurity Pilot Program Eligible Services List Process*. The Wireline Competition Bureau will release a list of services and equipment eligible for support prior to the opening of the Pilot Participant Selection Application Window, in accordance with § 54.2004. The Wireline Competition Bureau may, as needed, amend

the list of services and equipment eligible for support prior to the termination of the Schools and Libraries Cybersecurity Pilot Program, in accordance with § 54.2001.

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

§ 54.2004 Application for Selection in the Pilot Program.

(a) The Wireline Competition Bureau will announce the opening of the Pilot Participant Selection Application Window. Eligible recipients shall have no less than sixty (60) days to submit a Pilot Participant Selection Application, following the opening of the window.

(b) The Wireline Competition Bureau shall announce those eligible applicants that have been selected to participate in the Schools and Libraries Cybersecurity Pilot Program no more than ninety (90) days following the close of the Pilot Participant Selection Application Window.

(c) *Filing the FCC Form 484*.

(1) Schools, libraries, or consortia of eligible schools and libraries to participate in the Schools and Libraries Cybersecurity Pilot Program shall submit a completed FCC Form 484 to the Administrator. The FCC Form 484 shall include, at a minimum, the following information:

(i) Name, address, and contact information for the interested school or library. For school district or library system applicants, the name and

address of all schools/libraries within the district/system, and contact information for the district or library system.

(ii) 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, and a description of its proposed advanced cybersecurity action plan should it be selected to participate in the Pilot program and receive funding.

(iii) Description of any incident of unauthorized operational access to the Pilot participant's systems or equipment within a year of the date of its application; the date range of the incident; a description of the unauthorized access; 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.

(iv) Description of the Pilot participant's proposed use of the funding to protect its broadband network and data and improve its ability to address K-12 cyber concerns. This description should include the types of services and equipment the participant plans to purchase and the plan for implementing and using the Pilot-funded equipment and services to protect its broadband network and data, and improve its ability to manage and address its cybersecurity risks.

(v) Description of how the Pilot participant plans to collect and track its progress in implementing the Pilot-funded equipment and services into its cybersecurity action plan, and for providing the required Pilot data,

including the impact the funding had on its initial cybersecurity action plan that pre-dated implementation of Pilot efforts.

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

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

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

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

Cybersecurity Pilot Program could result in civil or criminal prosecution by law enforcement authorities."

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

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

(E) I certify and acknowledge, under penalty of perjury, that if selected, the schools, libraries, and consortia in the application will comply with all applicable Schools and Libraries Cybersecurity Pilot Program rules, requirements, and procedures, including the competitive bidding rules and the

requirement to pay the required share of the costs for the supported items from eligible sources.

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

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

§ 54.2005 Competitive Bidding Requirements.

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

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

(c) *Posting of FCC Form 470.*

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

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

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

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

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

(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. 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, sections 3729–3730 and 3801–3812)."

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

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

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

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

(x) I will retain required documents for a period of at least 10 years (or whatever retention period is required by the rules in effect at the time of this certification) after the later of the last day of the applicable funding year or the service delivery deadline for the associated funding request. I also certify that I will retain all documents necessary to demonstrate compliance with the statute 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 applicant 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(c). 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 applicant will comply with all applicable requirements.

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

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

(d) *Gift Restrictions*.

(1) Subject to paragraphs (d)(3) and (4) of this section, an applicant selected to participate in the Schools and Libraries Cybersecurity Pilot Program may not directly or indirectly solicit or accept any gift, gratuity, favor, entertainment, loan, or any other thing of value from a service provider participating in or seeking to participate in the Schools and Libraries Cybersecurity Pilot Program. No such service provider shall offer or provide any such gift, gratuity, favor, entertainment, loan, or other thing of value except as otherwise provided herein. Modest refreshments not offered as part of a meal, items with little intrinsic value intended solely for presentation, and items worth $20 or less, including meals, may be offered or provided, and accepted by any individuals or entities subject to this rule, if the value of these items received by any individual does not exceed $50 from any one service provider per year. The $50 amount for any service provider shall be calculated as the aggregate value of all gifts provided during a year by the individuals specified in paragraph (d)(2)(ii) of this section.

(2) For purposes of this paragraph:

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

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

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

(i) Are motivated solely by a personal relationship,

(ii) Are not rooted in any service provider business activities or any other business relationship with any such applicant selected to participate 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 an applicant selected to participate in the Schools and Libraries Cybersecurity Pilot Program in the support of its programs as long as such contributions are not directly or indirectly related to Schools and Libraries Cybersecurity Pilot Program procurement activities or decisions and are not given by service providers to circumvent competitive bidding and other Schools and Libraries Cybersecurity Pilot Program rules.

(e) *Selecting a provider of eligible services*. In selecting a provider of eligible services and equipment, applicants selected to participate in the Schools and Libraries Cybersecurity Pilot Program shall carefully consider all bids submitted and must select the most cost-effective service offering. In determining which service offering is the most cost-effective, entities may consider relevant factors other than the pre-discount prices submitted by providers, but price should be the primary factor considered.

§ 54.2006 Requests for Funding.

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

(1) An applicant selected to participate in the Schools and Libraries Cybersecurity Pilot Program shall, upon entering into a signed contract or other legally binding agreement for eligible services and 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 applicant selected to participate 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 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 application has been examined and is true, accurate, and complete. I acknowledge that any false statement on this application or on other documents submitted by this 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 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, sections 1001, 286–287 and 1341 and Title 31, sections 3729–3730 and 3801–3812)."

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

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

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

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

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

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

(x) The school, library, or consortia is not seeking Schools and Libraries Cybersecurity Pilot Program support or reimbursement for eligible services and/or equipment that have been purchased and reimbursed in full with other federal funding, targeted state funding, other external sources of targeted funding or targeted gifts, 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(c).

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

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

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

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

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

(b) *Service or Equipment Substitution.*

(1) A request by a Schools and Libraries Cybersecurity Pilot Program applicant to substitute service or equipment for one identified in its FCC Form 471 must be in writing and certified under 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*. If the service or equipment includes both ineligible and eligible components, the applicant selected to participate in the Schools and Libraries Cybersecurity Pilot Program must remove the cost of the ineligible components of the service or equipment from the request for funding submitted to the Administrator.

§ 54.2007 Discounts.

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

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

(2) For libraries and library consortia, the level of poverty shall be based on the percentage of the student enrollment that is eligible for a free or reduced price lunch under the National School Lunch Program or a federally-approved alternative mechanism in the public school district in which they are located and should use that school district's level of poverty to determine their discount rate when applying as a library system or as an individual library outlet within that

system. When a library system has branches or outlets in more than one public school district, that library system and all library outlets within that system should use the address of the central outlet or main administrative office to determine which school district the library system is in, and should use that school district's level of poverty to determine its discount rate when applying as a library system or as one or more library outlets. If the library is not in a school district, then its level of poverty shall be based on an average of the percentage of students eligible for the National School Lunch Program in each of the school districts that children living in the library's location attend.

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

(4) Applicants selected to participate 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*. Except as provided in paragraph (d) of this section, the Administrator shall use the following matrix to set the discount rate to be applied to eligible services purchased by applicants selected to participate in the Schools and Libraries Cybersecurity Pilot Program based on the applicant's level of poverty and location in an "urban" or "rural" area.

	Discount Level	
% of students eligible for National School Lunch Program	Urban Discount	Rural Discount
< 1	20	25
1-19	40	50
20-34	50	60
35-49	60	70
50-74	80	80
75-100	85	85

(d) Tribal Library Discount Level. For the costs of eligible cybersecurity equipment and services, Tribal libraries at the highest discount level shall receive a 90 percent discount.

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

unrelated to the supported service or equipment constitutes a rebate of the non-discount portion of the costs for the supported services and equipment.

§ 54.2008 Requests for Reimbursement.

(a) *Submission of request for reimbursement (FCC Form 472 or FCC Form 474)*. Reimbursement for the costs associated with eligible services and equipment shall be provided directly to an applicant selected to participate, or service provider, 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, sections 3729–3730 and 3801–3812)."

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

reimbursement were determined to be eligible and approved by the Administrator.

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

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

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

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

(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 applicant from anyone in connection with the Schools and Libraries Cybersecurity Pilot Program or the schools and libraries universal service support mechanism.

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

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

(xiii) No federal subsidy made available through a program administered by the Commission that provides funds to be used for the capital

expenditures necessary for the provision of advanced communications services has been or will be used to purchase, rent, lease, or otherwise obtain, any covered communications equipment or service, or maintain, any covered communications equipment or service, or maintain any covered communications equipment or service previously purchased, rented, leased, or otherwise obtained, as required by § 54.10.

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

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

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

comply with the rules and orders governing the Schools and Libraries Cybersecurity Pilot Program could result in civil or criminal prosecution by law enforcement authorities."

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

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

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

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

supported equipment or services constitutes a rebate of the non-discount portion of the costs as stated in § 54.2007(e).

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

(viii) The Service Provider certifies that it is compliant with the Commission's rules and orders regarding gifts and this Service Provider has not directly or indirectly offered or provided any gifts, gratuities, favors, entertainment, loans, or any other thing of value to any eligible school, library, or consortium, except as provided for at § 54.2005(d).

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

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

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

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

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

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

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

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

(e) *Invoice deadline extensions*. In advance of the deadline calculated pursuant to paragraph (c) 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.

§ 54.2009 Audits, Inspections, and Investigations.

(a) *Audits*. Schools and Libraries Cybersecurity Pilot Program participants shall be subject to audits and other investigations to evaluate their compliance with the statutory and regulatory requirements for 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 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 shall retain all documents related to their participation in the program sufficient to demonstrate compliance with all program rules for at least 10 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 10 years after purchase.

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

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

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

(b) The Administrator shall be responsible for reviewing applications for funding, recommending funding commitments, issuing funding commitment decision letters, reviewing invoices and recommending payment of funds, as well as other administration related duties.

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

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

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

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

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

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

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

(j) The Administrator shall make available to whomever the Commission directs, free of charge, any and all intellectual property, including, but not limited to, all records and information generated by or resulting from its role in administering the support mechanisms, if its participation in administering the Schools and Libraries Cybersecurity Pilot Program ends. If its participation in administering the Schools and Libraries Cybersecurity Pilot Program ends, the Administrator shall be subject to close-out audits at the end of its term.

§ 54.2012 Appeal and waiver requests.

(a) *Parties permitted to seek review of Administrator decision*.

(1) Any party aggrieved by an action taken by the Administrator must first seek review from the Administrator.

(2) Any party aggrieved by an action taken by the Administrator under paragraph (a)(1) of this section may seek review from the Federal Communications Commission as set forth in paragraph (b) of this section.

(3) Parties seeking waivers of the Commission's rules in this subpart shall seek relief directly from the Commission and need not first file an action for review from the Administrator under paragraph (a)(1) of this section.

(b) *Filing deadlines*.

(1) An affected party requesting review of a decision by the Administrator pursuant to paragraph (a)(1) of this section shall file such a request within thirty (30) days from the date the Administrator issues a decision.

(2) An affected party requesting review by the Commission pursuant to paragraph (a)(2) of this section of a decision by the Administrator under paragraph (a)(1) of this section shall file such a request with the Commission within thirty (30) days from the date of the Administrator's decision. Further, any party seeking a waiver of the Commission's rules under paragraph (a)(3) of this section shall file a request for such waiver within thirty (30) days from the date of the Administrator's initial decision, or, if an appeal is filed under paragraph (a)(1) of this section, within thirty days from the date of the Administrator's decision resolving such an appeal.

(3) Parties shall adhere to the time periods for filing oppositions and replies set forth in § 1.45 of this chapter.

(c) *General filing requirements*.

(1) Except as otherwise provided in this section, a request for review of an Administrator decision by the Commission shall be filed with the Commission's Office of the Secretary in accordance with the general requirements set forth in part 1 of this chapter. The request for review shall be captioned “In the Matter of Request for Review by (name of party seeking review) of Decision of Universal Service Administrator” and shall reference the applicable docket numbers.

(2) A request for review pursuant to paragraphs (a)(1) through (3) of this section shall contain:

(i) A statement setting forth the party's interest in the matter presented for review;

(ii) A full statement of relevant, material facts with supporting affidavits and documentation;

(iii) The question presented for review, with reference, where appropriate, to the relevant Commission rule, Commission order, or statutory provision; and;

(iv) A statement of the relief sought and the relevant statutory or regulatory provision pursuant to which such relief is sought.

(3) A copy of a request for review that is submitted to the Commission shall be served on the Administrator consistent with the requirement for service of documents set forth in § 1.47 of this chapter.

(4) If a request for review filed pursuant to paragraphs (a)(1) through (3) of this section alleges prohibitive conduct on the part of a third party, such request for review shall be served on the third party consistent with the requirement for service of documents set forth in § 1.47 of this chapter. The third party may file

a response to the request for review. Any response filed by the third party shall adhere to the time period for filing replies set forth in § 1.45 of this chapter and the requirement for service of documents set forth in § 1.47 of this chapter.

(d) *Review by the Wireline Competition Bureau or the Commission*.

(1) Requests for review of Administrator decisions that are submitted to the Federal Communications Commission shall be considered and acted upon by the Wireline Competition Bureau; provided, however, that requests for review that raise novel questions of fact, law, or policy shall be considered by the full Commission.

(2) An affected party may seek review of a decision issued under delegated authority by the Wireline Competition Bureau pursuant to the rules set forth in part 1 of this chapter.

(e) *Standard of review*.

(1) The Wireline Competition Bureau shall conduct de novo review of requests for review of decisions issued by the Administrator.

(2) The Commission shall conduct de novo review of requests for review of decisions by the Administrator that involve novel questions of fact, law, or policy; provided, however, that the Commission shall not conduct de novo review of decisions issued by the Wireline Competition Bureau under delegated authority.

(f) Schools and Libraries Cybersecurity Pilot Program disbursements during pendency of a request for review and Administrator decision. When a party has sought review of an Administrator decision under paragraphs (a)(1) through (3) of this section, the Commission shall not process a request for the reimbursement of eligible equipment and/or services until a final decision has been issued either by the

Administrator or by the Commission; provided, however, that the Commission may authorize disbursement of funds for any amount of support that is not the subject of an appeal.

[FR Doc. 2023-27811 Filed: 12/28/2023 8:45 am; Publication Date: 12/29/2023]