LIBRARIES =

# Learning Without Limits

## Advanced Firewalls and Cybersecurity Safeguard Vulnerable Community Networks

**Frequently Asked Questions**

On The FCC's Order on the:

## Schools and Libraries Cybersecurity Pilot Program

(June 14, 2024 — Version 2.0)

## BACKGROUND

The security of library and school networks is essential to provide safe and reliable internet access to patrons, students, and staff, and to protect sensitive personal information and other data. Network security has become especially critical as more networks of all types are being subject to attack and compromise by criminal elements and other malicious actors. Considering this issue, over the past several years ALA and other library and education organizations have encouraged the Federal Communications Commission (FCC) to make comprehensive cybersecurity tools eligible for the E-rate program.[1] Partially to address this need, on June 11, 2024, the FCC released an Order creating a limited Cybersecurity Pilot Program.

The following FAQ summarizes key points in the Pilot Program Order and while it focuses on libraries, much of the information will also be relevant to schools. For more information, see the FCC Schools and Libraries Cybersecurity Pilot Program website.

## FAQ

### Q: Aren't comprehensive cybersecurity tools already E-rate eligible?

A: No. However, basic firewalls have been eligible for over twenty years. But at that time not much attention was given to more robust network security needs and there were far fewer incidents of networks being compromised.

### Q: What is the timeframe for this Pilot and when will it start?

A: The Pilot timeframe will be for three years. The FCC has announced that a Pilot Participant application window will open sometime in the fall 2024. ***Note:*** There are actions staff can undertake now in anticipation of filing a Pilot application when the window opens. See the question "What are the basics of the application process?" for more information.

### Q: Why did the FCC launch this Cybersecurity Pilot Program? Considering the critical need for network security tools, why hasn't the FCC simply added them to the E-rate's Eligible Services List (ESL)?

A: The FCC is primarily concerned about costs—or the unknown costs—of adding these tools to the E-rate program.[2] As the Commission states, it must "Be a mindful and prudent steward of the Commission's limited universal service funds [USF]." (Order, ¶ 4). Several times in past years (2010, 2014, 2019) the Commission addressed expanding the eligibility of basic firewalls but declined to do so citing cost concerns (¶ 10). Thus, a primary purpose of the Pilot Program is to collect cost information which will enable the FCC to make better informed "future decisions on how to best utilize the USF to support the connectivity and network security needs of K-12 schools and libraries." (¶ 2).

## Q: Who will administer the program?

A: The Universal Service Administrative Company (USAC) will administer the program. The FCC states that considering USAC's experience administering the E-Rate program, it is "uniquely situated to be the Administrator of the Pilot Program." (¶ 88).

## Q: Who can apply for the Cybersecurity Pilot?

A: The Pilot will be open to all libraries and schools that are eligible for the regular E-rate program, even if they do not currently participate in the program. Consortia of libraries and schools can also apply (¶ 32-35).

## Q: How much funding will the FCC allocate to the Pilot and what is the source of funding?

A: The Pilot will be funded at $200 million over its three-year timeframe using extra E-rate funds not expended in previous program years. (¶ 19-21).

## Q: How much funding can schools and libraries request? (¶ 25-29)

- **Annual funding for *schools and districts:***
  They can receive up to $13.60 per student with a minimum of $15,000 and a maximum of $1.5 million.
- **Annual funding for *libraries and library systems*:**
  They can receive $15,000 per library up to 11 sites (i.e., branches). Library systems with more than 11 sites will be eligible for up to $175,000.
- **Annual funding for *consortia*:**
  In a consortium of schools and libraries, both will be eligible for funds based on the amounts cited immediately above. Consortia solely comprised of schools are subject to a maximum of $1.5 million. Consortia solely comprised of libraries are subject to a $175,000 maximum for library systems.

The above amounts are pre-discount. Pilot participants will use the E-rate's Category 1 discount matrix to determine their discount. Per the matrix, a 90% discount will be the maximum participants can receive (¶ 29).

## Q: What advanced cybersecurity tools are eligible for discounts as part of the Pilot Program? (¶ 36-57)

A: The Order states that applicants have the "flexibility to determine which [cybersecurity] solutions best serve their needs" (¶ 37). In this regard, the FCC has developed a Pilot Eligible Services List (P-ESL), which is in Appendix B in the Order. The list specifies over seventy eligible cybersecurity tools and services divided into four categories: (1) Advanced/Next-Generation Firewalls, (2) Endpoint Protection, (3) Identity Protection, and (4) Authentication, Monitoring, Detection, and Response. Other eligible costs include maintenance, operation and support, and installation and activation charges. Like the regular E-rate program, equipment and services must be competitively bid (see question below). Since basic firewall services are currently eligible for E-rate discounts, they are not eligible for the Pilot Program.

## Q: How will libraries and schools initially apply for the Pilot Program? (58-77)

A: The first step applicants will take in applying for the Cybersecurity Pilot Program will be completion of a new form, the 484. This form will be completed via USAC's online application portal. There are two parts to the new form.

**PART ONE**

The information submitted in Part One is important because *it will be a key factor used by the FCC and USAC to select Pilot Program participants.* This part asks applicants for basic information, like name, address, contact information, etc. But it also asks for more detailed information including: A description of the applicant's proposed Pilot project, the cybersecurity risks the project will address, the cybersecurity equipment and services the applicant plans to request and an estimate of their costs. ***Note:*** While the application window is not yet open, *staff can act now by reviewing the information requested in Part One and developing tentative answers.* By doing this, applicants will be in a good position to complete the first part of the 484 form when the window opens this fall.

**PART TWO**

Only applicants selected to participate in the Pilot Program will complete Part Two. This part asks for detailed cybersecurity information including current network vulnerabilities, describing any unauthorized network access, developing a cyber incident response plan, etc.

## Q: How will libraries and schools be selected to participate in the Pilot Program?

A: The Commission and USAC staff will use a variety of factors to select Pilot participants. As referenced above, an especially crucial factor is the applicant's information submitted as Part One on Form 484. Other factors that will be considered include applications with Tribal schools or libraries and applications that come from low-income communities. The selection process will also consider the need to have a variety of Pilot participants representing schools and libraries of all sizes and with a wide geographic distribution (¶ 70-72). In addition, the FCC and USAC will be looking for applicants with a wide variety of cybersecurity experience, including those who are "resource-challenged" (¶ 72).[3] If the total funding requested from all applications exceeds the $200 million allocation, priority will be given to applicants in the 90% discount band.

## Q: What happens after the Pilot Program applicants are selected?

A: Once applicants are selected, then many rules and processes similar to the regular E-rate program will come into play. The FCC states that "Modeling the Pilot processes and forms on existing E-Rate…processes and forms" will save Pilot participants time and reduce administrative costs (¶ 78). For example, a Pilot version of Form 470 must be filed seeking competitive bids on what cybersecurity equipment and services the applicant wants. Like the E-rate, this form must be open for a minimum of 28 days. Once bids are evaluated the applicant will select the most cost-effective bid with price being the primary factor. Then a version of Form 471 is filed listing the services and equipment selected, their costs and the service provider. One significant difference from the current E-rate program is that the Pilot Form 471 will cover the applicant's full Pilot project costs for all three years (¶ 84). The Pilot invoicing process using versions of Form 472 (BEAR) or Form 474 (SPAC) will be similar to current E-rate processes. Other Pilot Program rules will mirror the current E-rate program rules. Examples include a 10-year document retention requirement (¶ 91-92), participants being subject to audits, and the need to comply with the Children's Internet Protection Act (CIPA) (¶ 122).

## Q: Will USAC provide information on the program and conduct outreach on how to apply?

A: Yes. The FCC has directed USAC to develop a communications strategy that includes training and other outreach. The FCC acknowledges that providing this type of service to prospective applicants and ultimately Pilot participants "Will be an important tool in ensuring the Pilot Program is successful and meets its goals" (¶ 125).

## Q: How will the FCC measure the effectiveness of the Pilot Program?

A: The FCC has established three Performance Goals that include: (1) Improving the security and protection of E-rate-funded networks and data; (2) Measuring the costs of cybersecurity services and equipment, and the total funding needed if cybersecurity tools would be made a permanent part of the E-rate program; and (3) Evaluating how to leverage other federal cybersecurity tools and resources to help schools and libraries with their cybersecurity needs (¶ 101-106). To measure the Pilot's success the FCC has adopted initial, annual, and final reporting requirements for each goal. The initial reporting will be done to establish a baseline. If the information provided by participants in these reports contains sensitive business information, the FCC will withhold it from public access (¶ 111).

For questions on this FAQ, please contact:

**Robert Bocher,** *Senior Fellow*
ALA Public Policy and Advocacy
@ robert.bocher@gmail.com

[1] For example, see the E-rate comments ALA filed with the FCC on September 3, 2019. "Considering how essential robust network security is to our libraries (and schools), we strongly encourage the Commission to broaden the definition of E-rate eligibility to include all segments of network security" (https://www.fcc.gov/ecfs/document/10903401633871).

[2] In 2021 the Coalition on School Networking and Funds For Learning estimated that providing comprehensive cybersecurity tools to all E-rate participants could cost $2.389 billion annually, pre-discount. (See footnote 36 in the Order.)

[3] Regarding the challenges of smaller and "resourced-challenged" applicants, ALA filed Pilot Program comments with the FCC in January 2024 where it stated that "Assistance from USAC must start early in the application process, well before the actual application filing deadline." The FCC's Order acknowledges ALA's suggestion (footnote 273) and directs USAC to provide "Outreach, education, and engagement with Pilot Program applicants…" (¶ 125).