PUBLIC NOTICE

Federal Communications Commission
45 L Street NE
Washington, DC 20554

News Media Information 202 / 418-0500
Internet: https://www.fcc.gov

DA 24-887
Released: September 4, 2024

WIRELINE COMPETITION BUREAU ANNOUNCES APPLICATION FILING WINDOW FOR CYBERSECURITY PILOT PROGRAM AND PROVIDES GUIDANCE FOR SUBMITTING APPLICATIONS

Applications may be filed from September 17 to November 1, 2024

WC Docket No. 23-234

By this Public Notice, the Wireline Competition Bureau (Bureau) announces that the FCC Form 484 application filing window for the Schools and Libraries Cybersecurity Pilot Program (Pilot Program or Pilot)[1] will open on Tuesday, September 17, 2024 at 8 a.m. E.T., and close on Friday, November 1, 2024 at 11:59 p.m. E.T.[2] During the application filing window, eligible schools, libraries, and consortia comprised of eligible schools and libraries, can apply to participate in the three-year, $200 million Pilot Program by completing Part 1 of the FCC Form 484, available through the Universal Service Administrative Company's (USAC's) E-Rate Productivity Center (EPC) system via its website.[3] Applicants selected to participate in the Pilot Program can request and receive support to defray the costs of eligible cybersecurity services and equipment.

Prospective applicants interested in participating in the Pilot Program must file Part 1 of the FCC Form 484, to provide basic information about their cybersecurity needs, experience, and plans to use the cybersecurity funding if selected to participate in the Pilot.[4] To facilitate the inclusion of a diverse set of Pilot projects and target Pilot funds to the populations most in need of cybersecurity support, the Bureau will award support to a combination of large and small and urban and rural schools, libraries, and consortia, with an emphasis on funding proposed Pilot projects that include low-income and Tribal

[1] *Schools and Libraries Cybersecurity Pilot Program*, WC Docket No. 23-234, Report and Order, FCC 24-63, 2024 WL 3010578 (WCB June 11, 2024) (*Cybersecurity Pilot Program Report and Order*).

[2] On August 29, 2024, the Commission's rules for the Schools and Libraries Cybersecurity Pilot Program became effective with the exception of sections 54.2004 – 54.2006 and 54.2008. *See* Federal Communications Commission, Schools and Libraries, Final Rule, 89 Fed. Reg. 61282 (Jul. 30, 2024), https://www.govinfo.gov/content/pkg/FR-2024-07-30/pdf/2024-15866.pdf. Thus, applicants can save drafts of their Part 1 of the FCC Form 484 application but will not be able to certify their application until the Commission receives approval from the Office of Management and Budget (OMB). The Commission will publish a notice announcing OMB action and the effective dates of sections 54.2004 – 54.2006, and 54.2008 of the Commission's rules in the Federal Register. In the event there is a delay in OMB action, the closing date of the FCC Form 484 application filing window may be modified accordingly.

[3] USAC is the designated administrator of the Cybersecurity Pilot Program. *See Cybersecurity Pilot Program Report and Order, 2024 WL* 3010578 at *40, para. 88. EPC is USAC's online account and management system for the E-Rate, Emergency Connectivity Fund (ECF), and the Schools and Libraries Cybersecurity Pilot Programs.

[4] *Cybersecurity Pilot Program Report and Order,* 2024 WL 3010578 at *26, para. 63.

applicants.[5] Applicants selected to participate in the Pilot Program will be announced by the Bureau in a Public Notice.

Selected participants in the Pilot Program will be required to provide more detailed cybersecurity information in Part 2 of the FCC Form 484, which may be submitted at the same time the Cybersecurity Pilot Program FCC Form 471 is filed in an upcoming FCC Form 471 application filing window.[6] Selected participants will also be able to seek competitive bids, request eligible services and equipment, and seek reimbursement for eligible services and equipment. All Pilot Program participants and service providers will be subject to the Pilot Program integrity protection safeguards, including document retention and production, gift, certification, audit, and suspension and debarment rules, as well as all other FCC rules and requirements for the Pilot.

Eligible Pilot Participants

Schools, libraries, and consortia of schools and libraries (e.g., regional or statewide groups of schools or libraries that jointly apply for the Pilot) that meet the E-Rate Program's eligibility requirements may apply to participate in the Pilot Program.[7] An applicant need not be a current or former E-Rate Program participant to be able to apply for the Pilot.[8] Given the limited funding for the Pilot Program and the Commission's objective to select as many participants as possible, a school or library may only submit one application to participate in the Pilot Program, either individually or as part of a consortium.[9]

Applicants that are not currently participating in the E-Rate Program, or have not done so in the past, are encouraged to review the statutory requirements and rules relating to Pilot Program participation[10] and to submit their applications earlier in the window. New Pilot applicants must provide information to USAC to calculate and verify their discount rate percentages that will be used to prioritize applications should demand exceed the available budget.

While entities (such as governmental agencies and not-for-profit entities) that are not a school or library as defined under section 54.2000 of the Commission's rules are ineligible to apply for the Pilot Program, they may serve as a consortium leader, provided they pass through the benefits, discounts, and support received from the Pilot Program to their eligible school and library consortium members.[11]

Budget

Schools and school districts will be eligible to receive up to $13.60 per student, annually, on a pre-discount basis, to purchase eligible cybersecurity services and equipment over the three-year Pilot duration.[12] There is a $15,000 pre-discount annual funding floor and a maximum, annual pre-discount

[5] *Id.*

[6] Additional information will be made available in the future about how to complete Part 2 of the FCC Form 484 application, as well as the processes for conducting competitive bidding, seeking reimbursement for eligible cybersecurity services and equipment, complying with the Pilot's periodic reporting requirements, and other processes.

[7] *Id.* at *14, para. 34.

[8] *Id.*

[9] *Id.* at *15, para. 35.

[10] *Id.* at *78-81, Appendix B.

[11] *Id.*

[12] *Id.* at *10, para. 24. The annual pre-discount budget of $13.60 per student equates to a pre-discount budget of $40.80 per student over the three-year term of the Pilot Program.

budget of $1.5 million for schools and school districts.[13] Libraries will be eligible to receive a pre-discount annual budget of $15,000 per library up to 11 libraries/sites.[14] Library systems with more than 11 libraries/sites will be eligible for a total pre-discount annual support amount of up to $175,000.[15]

Consortia that are solely comprised of schools will be subject to the pre-discount annual $1.5 million budget maximum applicable to schools.[16] Consortia that are solely comprised of libraries will be subject to the pre-discount $175,000 annual budget maximum for library systems. Consortia comprised of eligible schools and libraries will be eligible to receive funding based on student count (using the annual pre-discount $13.60 per student multiplier and $1.5 million, pre-discount, annual cap) and number of library sites (using the pre-discount $15,000 per library annual budget up to 11 libraries/sites and the $175,000, pre-discount, annual cap.[17] Consortia comprised of both eligible schools and libraries will be subject to the pre-discount annual $1.5 million budget maximum applicable to schools.[18]

Each Pilot participant will be required to contribute a portion of the costs of the eligible cybersecurity services and equipment they seek to purchase with Pilot Program support, similar to the share that E-Rate applicants are required to contribute towards the cost of E-Rate eligible services and equipment.[19] That portion will be calculated using the participant's category one discount rate, which will range from 20 percent to 90 percent of the pre-discount price of eligible services and equipment.[20] Because some participants may incur greater costs up front, Pilot participants will have the ability to request any amount of funding they wish in a given Pilot Program year, as long as the total amount of funding they seek does not exceed their three-year budget.

Eligible Services and Equipment

Applicants selected to participate in the Pilot Program will be able to request funding and reimbursement for a wide variety of cybersecurity services and equipment, subject to per-student/per-library budgets, with minimum funding floors and overall funding caps described above. Eligible services and equipment include the following features, substantially similar features, or their equivalents:

- **Advanced/Next Generation Firewalls:** Equipment and services that implement advanced/next-generation firewalls, including software-defined firewalls and Firewall-as-a-Service, are eligible.[21] Specifically, equipment, services, or a combination of equipment and services that limit access between networks, excluding basic firewalls that are funded through the Commission's E-Rate Program, are eligible.[22]
- **Endpoint Protection:** Equipment and services that implement endpoint protection are eligible.[23] Specifically, equipment, services, or a combination of equipment and services that implement

[13] *Id.* at *11, para. 26.

[14] *Id.* at *12, para. 27.

[15] *Id.*

[16] *Id.* at *12, para. 28.

[17] *Id.*

[18] *Id.*

[19] *Id.* at *12, para. 29.

[20] *Id.*

[21] Advanced/Next generation firewalls "enable Pilot participants to protect their networks from outside cyber attackers by blocking malicious or unnecessary network traffic." *Id.* at *17, para. 41.

[22] *Id.* at *17-19, paras. 41-45.

[23] Endpoint protection ensures "participants can protect their networks from potential vulnerabilities introduced by desktops, laptops, mobile devices, and other end-user devices that connect to their networks." *Id.* at *20, para. 46.

safeguards to protect school- and library-owned end-user devices, including desktops, laptops, and mobile devices, against cyber threats and attacks are eligible.[24]

- **Identity Protection and Authentication:** Equipment and services that implement identity protection and authentication are eligible.[25] Specifically, equipment, services, or a combination of equipment and services that implement safeguards to protect a user's network identity from theft or misuse and/or provide assurance about the network identity of an entity interacting with a system are eligible.[26]
- **Monitoring, Detection, and Response:** Equipment and services that implement monitoring, detection and response are eligible.[27] Specifically, equipment, services, or a combination of equipment and services that monitor and/or detect threats to a network and that take responsive action to remediate or otherwise address those threats are eligible.[28]

Training. Training is eligible as part of installation of the equipment and services only if it is basic instruction on the use of eligible equipment and services, directly associated with installation, and is part of the contract or agreement for the equipment and services.[29] Training must occur coincidentally or within a reasonable time after installation.[30]

Ineligible Pilot Program Expenditures. While a broad range of services and equipment are eligible for funding through the Pilot Program, some are not. Ineligible items include all services and equipment that are eligible for funding through the E-Rate Program;[31] and those that have already been fully reimbursed (or will be fully reimbursed) through a different funding source.[32] Additionally, consistent with limitations established in the E-Rate Program, staff salaries and labor costs, as well as beneficiary and consulting services that are not related to the installation and configuration of eligible equipment and services, are ineligible for Pilot funding.[33] Costs for training beyond basic instruction, as described above, is ineligible. Finally, insurance costs and costs associated with responding to specific ransom demands are ineligible for Pilot support.[34]

The Pilot Eligible Services List provides more detailed information about the types of equipment and services that are eligible/ineligible for support through the Pilot Program.

[24] *Id.* at *20, paras. 46-47.

[25] Identity Protection and Authentication ensures "participants can prevent malicious actors from accessing and compromising their networks under the guise of being legitimate users." *Id.* at *20, para. 48.

[26] *Id.* at *20-21, paras. 48-49.

[27] Monitoring, detection, and response ensures "participants can promptly and reliably detect and neutralize malicious activities that would otherwise compromise their networks." *Id.* at *21, para. 50.

[28] *Id.* at *21, paras. 50-51.

[29] *Id.* at *81, Appendix B.

[30] *Id.*

[31] *Id*. at *21, para. 52.

[32] *Id.* Applicants selected to participate in the Pilot may use funding to pay for Pilot-eligible services and equipment that they were previously paying for themselves, subject to our competitive bidding rules. *Id.*

[33] *Id.* at *23, para. 55.

[34] *Id.*

Application Requirements

To be considered for the Pilot Program, applicants must complete certain pre-application requirements and provide basic information about their cybersecurity needs, experience, and plans to use the funding if selected to participate.

Pre-Application Requirements. Prospective applicants must be in good financial standing with the FCC and the federal government and complete several steps before they can apply for, and receive, Pilot Program support. Prospective applicants are strongly encouraged to complete these steps now, to ensure that they are ready when the application filing window opens on September 17, 2024.

Prospective applicants must have an FCC Registration Number (FCCFRN) to participate in the Pilot Program. Prospective applicants may obtain an FCCFRN by visiting the FCC's Commission Registration System (CORES) and completing the registration process.[35] Prospective applicants must also obtain a Billed Entity Number (BEN). Prospective applicants that are already registered in EPC already have a BEN and will get access to the Pilot Program application using their existing credentials. New applicants will need to contact USAC's E-Rate Customer Service Center at (888) 203-8100 to set up a BEN and EPC account. Once a new applicant's BEN is set up, the USAC Customer Service Center will provide the new applicant with access to its EPC account. Prospective applicants should create, review, and update their EPC user profile as necessary to ensure that the information in their profile is accurate. EPC will be used to manage program processes, set-up access rights, receive notifications, and contact the USAC Customer Service Center. Prospective applicants will also need to set-up their credentials in One Portal, USAC's single sign-on dashboard that allows applicants to access their online application(s). To set up credentials in One Portal, prospective applicants should click the blue Sign In button at the top of any USAC web page and follow the instructions. If a prospective applicant is already an EPC user, USAC will set-up the applicant's One Portal account using the applicant's EPC contact email address as the username. Be aware that the first time you sign into any USAC system, such as One Portal, the system will prompt you to set up multi-factor authentication for your account.

Prospective applicants must also verify that they are not currently in red light status at the FCC or on the U.S. Treasury's do not pay list. These mechanisms verify whether an entity seeking federal funding has an outstanding debt or delinquency with the federal government. Prospective applicants will not be eligible to participate in the Pilot Program if any debts or other delinquencies are not resolved prior to the FCC Form 484 filing window close date.

Prospective applicants should also register with the System for Award Management at SAM.gov. Prospective applicants that already have a SAM.gov registration should ensure that it is active, as it must be renewed annually. Although an active SAM.gov registration is not required to apply for Pilot Program support, it is required to receive funds and disbursements through the Program. Prospective applicants should also be aware that the SAM.gov registration process may take a few weeks to complete.

Part 1 of FCC Form 484 Application Requirements. Applicants will use the Part 1 of the FCC Form 484 to provide general cybersecurity information and answer questions about their proposed Pilot projects, including the eligible services and equipment they intend to seek funding for if selected for the Pilot Program. Applicants will be required to provide the following information:

- Names, entity numbers, FCC registration numbers, employer identification numbers, addresses, and telephone numbers for all schools, libraries, and consortium members that will participate in the proposed Pilot project, including the identity of the consortium leader for any proposals involving consortia.
- Contact information for the individual(s) who will be responsible for the management and

[35] If a prospective applicant is already registered with the FCC, it does not need a new FCCFRN to apply for or receive support through the Pilot Program.

operation of the proposed Pilot project (name, title or position, telephone number, mailing address, and email address).

- Applicant number(s) and type(s) (e.g., school; school district; library; library system; consortia; Tribal school or library (and Tribal affiliation)), if applicable; and current E-Rate participation status and discount percentage, if applicable.[36]
- A broad description of the proposed Pilot project, including, but not limited to, a description of the applicant's goals and objectives for the proposed Pilot project, a description of how Pilot funding will be used for the proposed project, and the cybersecurity risks the proposed Pilot project will prevent or address.
- The cybersecurity equipment and services the applicant plans to request as part of its proposed project, the ability of the project to be self-sustaining once established, and whether the applicant has a cybersecurity officer or other senior-level staff member designated to be the cybersecurity officer for its Pilot project.
- Whether the applicant has previous experience implementing cybersecurity protections or measures (answered on a yes/no basis), how many years of prior experience the applicant has (answered by choosing from a preset menu of time ranges (e.g., 1 to 3 years)), whether the applicant has experienced a cybersecurity incident within a year of the date of its application (answered on a yes/no basis), and information about the applicant's participation or planned participation in cybersecurity collaboration and/or information-sharing groups.
- Whether the applicant has implemented, or begun implementing, any Education Department or Cybersecurity and Infrastructure Security Agency (CISA) best practices recommendations (answered on a yes/no basis), a description of any Education Department or CISA free or low-cost cybersecurity resources that an applicant currently utilizes or plans to utilize, or an explanation of what is preventing an applicant from utilizing these available resources.
- An estimate of the total costs for the proposed Pilot project, information about how the applicant will cover the non-discount share of costs for the Pilot-eligible services, and information about other cybersecurity funding the applicant receives, or expects to receive, from other federal, state, local, or Tribal programs or sources.
- Whether any of the ineligible services and equipment the applicant will purchase with its own resources to support the eligible cybersecurity equipment and services it plans to purchase with Pilot funding will have any ancillary capabilities that will allow it to capture data on cybersecurity threats and attacks, any free or low-cost cybersecurity resources that the applicant will require service providers to include in their bids, and whether the applicant will require its selected service provider(s) to capture and measure cost-effectiveness and cyber awareness/readiness data.
- A description of the applicant's proposed metrics for the Pilot project, how they align with the applicant's cybersecurity goals, how those metrics will be collected, and whether the applicant is prepared to share and report its cybersecurity metrics as part of the Pilot Program.

To minimize burden, much of the information on Part 1 of the FCC Form 484 will be pre-populated using information from the applicant's EPC profile. In addition, most of the application questions will be answered using "yes/no" or pre-defined responses (i.e., multi-select questions with pre-defined answers). Applicants are expected to provide a clear strategy for addressing their cybersecurity needs on the application form and should clearly articulate how their proposed projects will accomplish

[36] Note that there is no need for an applicant to indicate its urban or rural status, as that information will be auto-populated by the system based on 2020 U.S. Census Bureau data that is also used in the E-Rate program for this determination.

their cybersecurity objectives. Applications should be tailored to the unique circumstances of each applicant. Applicants should be aware that they may be disqualified from consideration for the Pilot if their applications provide a bare minimum of information or are generic or template in nature.[37]

All applicants, but especially those that have not participated in the E-Rate Program, are encouraged to submit Part 1 of the FCC Form 484 early to allow additional time for USAC to verify their eligibility for the Pilot and to calculate their discount rate percentage. An applicant's discount rate percentage will be used as part of the Pilot selection process if the number of FCC Form 484 applications received exceeds the number of projects that can be funded.[38] Applicants with higher discount rates generally will be funded before applicants in the lower discount bands.[39]

Additional Information and Resources

In preparation for the opening of the application filing window, interested prospective applicants may start by reviewing the references and guides below to learn more about the Pilot. Additionally, prospective applicants may start collecting the information discussed above and outlined in the references and guides that applicants generally will be required to submit as part of their Part 1 of the FCC Form 484 applications. Note that the actual wording on Part 1 of the FCC Form 484 application and the order in which the information appears on the final form may vary from the wording and the order of the items discussed in this Public Notice.

- Cybersecurity Pilot Program Overview
- Cybersecurity Pilot FAQs
- Getting Ready Guide
- Cybersecurity Pilot Program Application Guide
- USAC Cybersecurity Pilot Program Website
- USAC Applicant Process Guide
- Upcoming USAC Webinars and Trainings

For further information regarding this Public Notice, email CyberPilot@fcc.gov. Visit https://www.fcc.gov/cybersecurity-pilot-program to learn more about the Schools and Libraries Cybersecurity Pilot Program or click here to sign up for USAC's Schools and Libraries Cybersecurity Pilot Program Email List.

- FCC -

[37] *Cybersecurity Pilot Program Report and Order*, 2024 WL 3010578 at *26, para. 62.

[38] *Id*. at *32, para. 73.

[39] *Id.*