Filling Out FCC Form 484 Application Information

The application window will open on Tuesday, September 17, 2024, at 8am EST, and close on Friday, November 1, 2024, at 11:59pm EST.

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

- Names, entity numbers, FCC registration numbers, employer identification numbers, addresses, and telephone numbers for all schools, libraries, and consortium members that will participate in the proposed Pilot project, including the identity of the consortium leader for any proposals involving consortia.

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

- Applicant number(s) and type(s) (e.g., school; school district; library; library system; consortia; Tribal school or library (and Tribal affiliation)), if applicable; and current E-Rate participation status and discount percentage, if applicable.

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

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

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

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

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

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

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

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

• Information about correcting known security flaws and conducting routine backups, developing and exercising a cyber incident response plan,301 and any cybersecurity changes or advancements the participant plans to make outside of the Pilot-funded services and equipment.

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

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

• Information about a participant's history of cybersecurity threats and attacks within a year of the date of its application; the date range of the incident; a description of the unauthorized access; a description of the impact to the K-12 school or library; a description of the vulnerabilities exploited and the techniques used to access the system; and identifying information for each actor responsible for the incident, if known.

- A description of the specific Education Department or CISA cybersecurity best practices recommendations that the participant has implemented or begun to implement.

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

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

Instructions for Filing Applications.

As previously discussed; in order to facilitate the application process, we plan to provide an application titled “Schools and Libraries Cybersecurity Pilot Program Application” (FCC Form 484) that applicants must use when submitting their project proposals to the Commission. Applicants will be required to complete each section of the first part of the application and make the required certifications. The applications for the Pilot Program must be submitted through the Pilot portal on USAC’s website during the announced FCC Form 484 application filing window.