



- Funding Status for E-Rate and ECF
 - E-Rate for FY 2023
 - ECF for 2021-2023
 - E-Rate for FY 2024
- Draft of the Cybersecurity Pilot Application Form 484
- Updates and Reminders
 - Upcoming Dates
- USAC E-Rate News Brief Dated January 25 – Form 471 Guidance
 - School Bus Wi-Fi Filing Instructions
 - Treatment of New 25% CEP Threshold

Funding Status for E-Rate and ECF

E-Rate for FY 2023:

USAC issued Wave 40 for FY 2023 on Thursday, January 25th, for \$11.2 million, none for North Carolina. Total funding is now \$2.56 billion including \$84.3 million for North Carolina. At this point, USAC has funded 97.4% of the originally submitted applications representing 91.1% of the dollars requested.

ECF for 2021-2023:

Total commitments for all three ECF windows are \$6.45 billion including \$192 million for North Carolina.

E-Rate for FY 2024:

The Form 471 filing window for FY 2024 opened January 17th and will close on Wednesday, March 27th, at 11:59 p.m. EDT. We are already seeing some applications being marked as “Wave Ready” with a strong probability of being included in the first funding wave expected in late April.

Draft of the Cybersecurity Pilot Application Form 484

Field descriptions of the forms that USAC will use for the FCC’s proposed cybersecurity pilot program (see [FCC 23-92](#) and our [newsletter of November 20th](#)) are posted on the OMB website for review. In large part, the pilot program will use near-identical versions of familiar E-rate forms. A new and important form, however, to be used to apply for entry into the pilot program itself, will be the “Schools and Libraries Cybersecurity Pilot Program Application (FCC Form 484).” Field descriptions for the [draft Form 484](#) are available for download on the OMB site.

The Form 484 will begin and end with familiar fields for entity information and certifications. Most interesting, for those applicants planning to apply for the pilot, are the 38 following “Project Information” fields:

Item #	Field Description	Category	Purpose/Instructions
22	Executive Summary of Project	Project Information	Provide a summary of the proposed Pilot project for which Schools and Libraries Cybersecurity Pilot Program funding is being requested, including, but not limited to, information about the cybersecurity issues the applicant faces and the proposed cybersecurity action plan for the applicant and any other sites that included as part of the project.
23	Description of How Project Funding Will be Used	Project Information	Describe how the proposed Pilot project would use Schools and Libraries Cybersecurity Pilot Program funding to protect the applicant's broadband network and data, and address cybersecurity concerns, including, but not limited to, a discussion of the types of equipment and services the applicant plans to purchase and how it plans to use the equipment and services to protect its broadband network and data and manage and address its cybersecurity risks.
24	Previous Cybersecurity Experience	Project Information	Information on whether the applicant has previous experience implementing cybersecurity protections or has or is implementing a cybersecurity framework or program, including the length of the applicant's cybersecurity experience.
25	Current Cybersecurity Posture and Resources	Project Information	Information on the applicant's current cybersecurity posture and resources, including, but not limited to, how current cybersecurity risks are being managed and addressed and the cybersecurity equipment and services the applicant already has in place.
26	History of Cyber Threats and Attacks	Project Information	Information on whether the applicant has experienced a cybersecurity threat or attack, including, but not limited to, the timing and length of the threat or attack, information about the malicious cybersecurity actor(s), if known, the time it took to detect and respond to the threat or attack, the estimated cost of the threat or attack, and whether/how the cybersecurity threat or attack impacted the applicant's/participant's operations, network, or data.
27	Implementation of DOE or CISA Cybersecurity Recommendations	Project Information	Information on whether the applicant has implemented, or begun implementing, any of the U.S. Department of Education (DOE) or Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) recommended cybersecurity protections and which protections it will or has implemented.
28	Participation in Cybersecurity Collaboration and/or Information Sharing Groups	Project Information	Information on whether the applicant is a member of, or plans to join, any cybersecurity collaboration and information-sharing groups and a list of the applicable cybersecurity groups it has joined or plans to join.
29	Other Sources of Funding	Project Information	Information on whether the applicant has received, or expects to receive, cybersecurity funding from any other federal universal service program, or another federal, state, local, Tribal, or other program or source, including information about the source of the other funding, what the other funding will be used for, and whether funding from the Schools and Libraries Cybersecurity Pilot Program would be duplicative of the other funding received.
30	Cybersecurity Risks Proposed Pilot Project will Prevent or Address	Project Information	Information on the cybersecurity risks the proposed Schools and Libraries Cybersecurity Pilot Program project will prevent or address.
31	Pilot Project Implementation and Operation	Project Information	Description of the applicant's plan for implementing and operating the proposed Schools and Libraries Cybersecurity Pilot Program project.
32	Goals and Objectives	Project Information	Applicant's goals and objectives for the proposed Schools and Libraries Cybersecurity Pilot Program project.
33	Correction of Known Security Flaws and Routine Backups	Project Information	Information on whether the applicant plans to correct known security flaws and/or conduct routine backups as part of the proposed Schools and Libraries Cybersecurity Pilot Program project.

Item #	Field Description	Category	Purpose/Instructions
34	Recommended Cybersecurity Best Practices	Project Information	Information on whether the applicant plans to implement recommended best practices from highly-regarded cybersecurity organizations (e.g., the DOE, CISA, the National Institute of Standards and Technology (NIST), etc.) as part of the proposed Schools and Libraries Cybersecurity Pilot Program project.
35	Designated Cybersecurity Officer	Project Information	Information on the applicant's officer or other senior-level staff member that will be the designated cybersecurity officer and the tasks for which the officer will be responsible for.
36	Estimated Timeline for Ramping Up Proposed Pilot Project	Project Information	Estimated timeline for ramping up the proposed Schools and Libraries Cybersecurity Pilot program project.
37	Data and Metrics Collected by Applicant	Project Information	Description of the data the applicant will collect and the metrics it will use to assess the outcomes of the proposed Schools and Libraries Cybersecurity Pilot Program project, including, but not limited to, a description of how the project, will collect, track, and store such information.
38	Cost-Effectiveness Data and Metrics Collected by Service Provider	Project Information	Information on data the applicant will require its selected service providers to collect, track, and measure to determine the cost-effectiveness of Schools and Libraries Cybersecurity Pilot program-funded cybersecurity equipment and services.
39	Awareness and Readiness Data and Metrics Collected by Service Provider	Project Information	Information on the data the applicant will require its selected service providers to collect, track, and measure to determine the impact/effect on the applicant's current cybersecurity awareness and readiness.
40	Non-monetary Challenges	Project Information	Information on the non-monetary cybersecurity challenges faced by the applicant and if/how the Pilot project will address them.
41	Current Cybersecurity Measures	Project Information	Information on the current cybersecurity measures that are utilized by the applicant.
42	Cybersecurity Training	Project Information	Information about the applicant's cybersecurity training efforts, including, but not limited to the number/percentage of students, school and library staff, and/or library patrons who receive cybersecurity training, and training participation rates.
43	Free and Low-Cost Cybersecurity Resources	Project Information	Information on whether the applicant is utilizing or plans to utilize any of the free or low-cost cybersecurity resources identified/offered by the DOE or CISA, and which resources it is utilizing/plans to utilize. If an applicant has not started to utilize the available free and low-cost cybersecurity resources, they should explain what are the impediments that are preventing them from doing so.
44	Impediments to Developing a More Robust Cybersecurity Posture	Project Information	If applicable, information on why an applicant has not been able to take any preventative or mitigating actions to protect against cybersecurity threats and attacks and implement a more robust cybersecurity posture.
45	Ability of Proposed Pilot Project to be Self-sustaining	Project Information	Information on whether/how the applicant plans for the Schools and Libraries Cybersecurity Pilot Program project to be self-sustaining once established and after the Pilot program ends.
46	Network Equipment, Hardware and Software Services	Project Information	Information on any network equipment, hardware or software services the applicant plans to request as part of its Schools and Libraries Cybersecurity Pilot project, including, but not limited to, any cloud services or third-party managed cybersecurity services.
47	Cybersecurity Protections for Broadband Networks and Data Outside of the Pilot Program	Project Information	Information on whether the applicant plans to obtain or upgrade any of its cybersecurity protections for its broadband networks and data outside of the Schools and Libraries Cybersecurity Pilot program.
48	Implementation of Cybersecurity Recommendations or Framework Outside of Pilot Program	Project Information	If not selected to participate in the Schools and Libraries Cybersecurity Pilot Program, information on whether the applicant/participant has resources to begin implementation of the DOE's and/or CISA's cybersecurity recommendations and/or a cybersecurity program or framework.
49	Funding for Non-cybersecurity Equipment and Services That Support Cybersecurity Equipment and Services	Project Information	Information on whether the proposed Schools and Libraries Cybersecurity Pilot project has funding for any non-cybersecurity equipment or services that the applicant/participant will use to support cybersecurity equipment or services and protect against cybersecurity threats and attacks, including, but not limited to, whether the equipment/services facilitate capturing, transmitting, or storing data about cybersecurity threats, attacks, and/or incidents.

Item #	Field Description	Category	Purpose/Instructions
50	Will Service Provider be Required to Include any No Cost Cybersecurity Equipment and/or Services	Project Information	Information on whether the applicant will require its selected service provider(s) to provide any cybersecurity equipment and/or services at no cost to the applicant, including a description of the applicable equipment and services.
51	Required Free and Low Cost Cybersecurity Resources	Project Information	Information on any mandatory free and/or low cost cybersecurity resources the applicant expects the its selected service providers to implement and utilize.
52	Estimated Costs of Pilot-Eligible Services and Equipment	Project Information	Estimated cost information for the services and equipment that the applicant will seek funding through the Schools and Libraries Cybersecurity Pilot Program.
53	Total Estimated Funding Request	Project Information	Total estimated funding the applicant anticipates requesting from the Schools and Libraries Cybersecurity Pilot Program for eligible cybersecurity equipment and services.
54	Estimated Applicant/Participant Share of Cost for Eligible Items	Project Information	Applicant's estimated share of the costs for eligible equipment and services for which it requests funding under the Schools and Libraries Cybersecurity Pilot Program.
55	Estimated Applicant/Participant Cost for Ineligible Items	Project Information	Cost that the applicant expects to pay for equipment and services that ineligible for funding under the Schools and Libraries Cybersecurity Pilot Program.
56	Total Estimated Pilot Project Cost	Project Information	Total cost that the applicant estimates it will incur for participating in the Schools and Libraries Cybersecurity Pilot Program.
57	Sources of Support for Applicant's/Participant's Share of Cost for Eligible Items	Project Information	Information on the sources of financial support the applicant will use to pay its share of the cost for equipment and services that are eligible for funding under the Schools and Libraries Cybersecurity Pilot Program.
58	Plan to Cover Cost of Ineligible Items	Project Information	Information on the applicant's plan to pay the cost of equipment and services that are ineligible for funding under the Schools and Libraries Cybersecurity Pilot Program.
59	Supporting Documentation	Project Information	Provides an option for the user to upload and submit documents to support their proposed Pilot Program project.

By all indications, applying for entry into the cybersecurity pilot program will not be a trivial exercise. The Form 484 questions indicate that USAC and the FCC will be seeking applicants with a pre-determined plan to conduct a rigorous cybersecurity exercise leading to measurable outcomes.

Updates and Reminders

Upcoming Dates:

January 29 Due date for reply comments on the FCC's hotspot eligibility NPRM (FCC 23-91). [E-Rate Central's reply comments proposing a funding allocation mechanism which, if adopted, would assure hotspot funding for all interested applicants, were filed January 25th.](#)

January 29 Due date for comments on the FCC's cybersecurity pilot NPRM (FCC 23-92). Reply comments are due February 27th.

January 29 Invoice (or invoice deadline extension request) deadline for FY 2022 non-recurring service FRNs.

February 2 Form 486 deadline for FY 2023 Wave 24. More generally, the Form 486 deadline is 120 days from the FCDL date or from the service start date (typically July 1st), whichever is later. Upcoming Form 486 deadlines are:

Wave 25	02/09/2024
Wave 26	02/16/2024
Wave 27	02/23/2024

Applicants missing their Form 486 deadlines should, within a week, receive Urgent Reminder Letters from USAC providing a 15-day grace period.

- February 27 Extended invoice deadline for FY 2022 recurring service FRNs.
- February 28 Last day to file a Form 470 for FY 2024 so as to allow its posting for at least 28 days before the close of the Form 471 application window.
- Please note that any applicant waiting until February 28th to file a Form 470 would have to review all bids, select vendors, sign contracts, and upload them into EPC, create and file their Form 471, all on March 27th when the EPC is likely to be at its busiest. This is **NOT** a recommended course of action!
- March 27 Close of the Form 471 application window for FY 2024. To be considered as having been filed “in window,” Form 471s must be filed and certified by 11:59 p.m. EDT.

USAC E-Rate News Brief Dated January 25 – Form 471 Guidance

[USAC’s E-Rate News Brief dated January 25, 2024](#), provides tips related to the now open FY 2024 application window including the two important areas discussed below.

School Bus Wi-Fi Filing Instructions:

USAC suggests the following steps when filing a Form 471 for school bus Wi-Fi:

- Submit a separate FCC Form 471 for Wireless School Bus Services.
- Submit a separate funding request number (FRN) for each contract or vendor for these services.
- Use “School Bus Wi-Fi” or similar name as the FCC Form 471 nickname.
- List all schools as recipients of service that will be served by the buses.
- At the FRN level:
 - Include “School Bus Wi-Fi” again in the FRN nickname.
 - In the FRN Narrative, include “Applicant seeks support for wireless school bus service, and, if applicable, associated equipment to make the service functional” along with make and model information, the number of buses serviced.”
 - For FRN Purpose, select “Internet access service that includes a connection from any applicant site directly to the Internet Service Provider.”
 - In the Function text box, enter “Wireless School Bus Service.”
 - For Type of Connection, enter “Wireless data service,” “Equipment,” “Installation,” etc., as applicable. Note that the “Wireless data service,” when used will ask you to enter “Number of Buses Being Serviced.”

Treatment of New 25% CEP Threshold:

Last October, the U.S. Department of Agriculture (“USDA”) finalized new rules reducing the school eligibility threshold for participation in the Community Eligibility Provision (“CEP”)

program from an Identified Student Percentage (“ISP”) of 40% to 25%. (See our [newsletter of October 2nd](#)). Although the new threshold was to apply for CEP applications for the 2024-2025 school year, USDA accepted and approved waivers for use in the second half of this year. For E-rate purposes, this will mean that new CEP schools will be able to use an NSLP percentage calculated as 1.6 times their new lower ISP percentage.

EPC, however, does not yet accept any ISP percentage below the original 40%. Applicants trying to enter a lower percentage during the administrative window could not do so. Thus FY 2024 Form 471s being submitted for these applicants now will have to use current EPC discount rates.

Last week’s News Brief explains this problem and advises: “If you want to report a CEP percentage less than 40%, you must enter your regular NSLP numbers (without CEP multiplier calculations) and **use the FCC Form 471 narrative field to communicate your request for the PIA reviewer to enter the proper CEP percentage.**”

Newsletter information and disclaimer: This newsletter may contain unofficial information on prospective E-rate developments and/or may reflect E-Rate Central’s own interpretations of E-rate practices and regulations. Such information is provided for planning and guidance purposes only. It is not meant, in any way, to supplant official announcements and instructions provided by USAC, the FCC, or NCDPI.

Additional North Carolina specific E-rate information is available through our Web site — <http://www.e-ratecentral.com/us/stateInformation.asp?state=NC>. Note that this site provides easy access to formatted North Carolina applicant E-rate histories via the Billed Entity Number (“BEN”) search mechanism in the upper left-hand corner. Detailed information can be obtained by “drilling down” using the links for specific funding years and individual FRNs.

If you have received this newsletter from a colleague and you would like to receive your own copy of the North Carolina E-Rate Forum, send an email to join-ncerate@lists.dpi.state.nc.us. Please include your name, organization, telephone, and e-mail address.

In compliance with federal law, the NC Department of Public Instruction administers all state-operated educational programs, employment activities and admissions without discrimination because of race, religion, national or ethnic origin, color, age, military service, disability, or gender, except where exemption is appropriate and allowed by law.