

**Before the  
Federal Communications Commission  
Washington, D.C. 20554**

In the Matter of	)	
	)	
Schools and Libraries Cybersecurity Pilot Program	)	WC Docket No. 23-234
	)	

**REPLY COMMENTS OF THE STATE E-RATE COORDINATORS’ ALLIANCE  
TO THE NOTICE OF PROPOSED RULEMAKING (FCC 23-92)**

---

**I. INTRODUCTION AND SUMMARY**

In releasing the Cybersecurity Pilot Notice of Proposed Rulemaking (“Pilot NPRM”) all five Commissioners of the Federal Communications Commission’s (“FCC” or “Commission”) unanimously acknowledge the vital threat that cybersecurity attacks pose to school and library broadband network services and equipment that are funded in part by the E-rate program. The Commission also seeks to develop a record to determine what services and equipment should be categorized under the cybersecurity definitional umbrella and the associated costs, over a three-year period. The State E-rate Coordinators’ Alliance (“SECA”) commends the FCC’s efforts.

SECA believes these efforts should be accompanied by another important timely actionable step within the Commission’s power and authority: allow E-rate to fund the cybersecurity features that are part of firewall devices. Firewall appliances are currently eligible for funding; however, the cybersecurity features that are integral to the equipment are not eligible. These features, known colloquially as “next generation” are excluded from eligibility and their costs must be deducted from E-rate funding requests. Through years of Eligible Services List Public Comments, and most recently the Wireline Competition Bureau’s Public Notice focused on this specific matter, as well as the initial comments filed

in this proceeding, and the Cybersecurity Pilot NPRM, the Commission already has developed the record which overwhelmingly supports the use of E-rate funding for these “next generation” firewall features that are critical tools for thwarting cyberattacks.

Related specifically to the cybersecurity pilot, SECA encourages the FCC to revise the parameters of the pilot to be more flexible and enable school and library applicants to use the funds to obtain vital professional expert services to evaluate and implement cybersecurity protections. Based on the NPRM and the proposed forms, we are concerned that pilot applicants must already possess a great deal of knowledge, and are well on their way to implementing their cybersecurity measures. The amount of information pilot applicants must submit on the Form 484 is arduous and may exclude applicants with less resources and less current knowledge of cybersecurity resources, yet desperately need access to cybersecurity funding. SECA asks the FCC to modify the proposed program format to enable all applicants, not just those with robust mitigation efforts already underway, to be able to meaningfully participate in the pilot.

In addition to offering our policy recommendations, we appreciate the opportunity to offer comments on the draft forms in advance of finalizing them. Our suggestions focus on identifying the most time intensive areas and suggesting efficiencies to alleviate the burden on applicants while balancing the FCC’s need and desire to collect information about each participant’s experience. We believe that the burden hours on the proposed forms are significantly understated because they do not adequately quantify all the time and effort required to prepare the data that the forms seek to collect.

In conclusion, SECA supports any and all efforts to facilitate access for schools and libraries to funding for cybersecurity mitigation efforts as quickly as possible. At the same time, SECA understands the need for a reasonable and realistic planning horizon that enables the Commission, the administrator, applicants and vendors to adequately prepare for and

implement the pilot, and encourages the Commission to consider a realistic timeline to revise the E-rate Eligible Services List definition of eligible firewalls to help address the vital threat of cyberattacks on schools and libraries.

## **II. THE PILOT PARAMETERS SHOULD ENABLE APPLICANTS OF ALL EXPERIENCE LEVELS TO PARTICIPATE IN THE PILOT PROGRAM.**

The five areas of information required to be provided in applications to participate in the pilot reflect an expectation of cybersecurity planning and execution that may foreclose many schools and libraries from being eligible to participate. SECA recommends, therefore, that the FCC reduce the amount of prerequisite planning to apply.

Specifically, item ii in paragraph 27 of the NPRM, and 47 C.F.R. §54.2004 (c) (ii) propose to require:

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.

Schools and libraries may lack the knowledge and expertise to prepare an advanced cybersecurity action plan to include in its pilot participation application. Unless a school or library has already invested considerable time and effort in developing a comprehensive cybersecurity strategy, they likely do not have a proposed cybersecurity action plan, let alone an advanced plan to submit with the pilot application. It is unclear what level of detail and information will be required. Item 31 of proposed Form 484 seeks to collect "Description of the applicant's plan for implementing and operating the proposed Schools and Libraries Cybersecurity Pilot Program project." Is this the proposed advanced cybersecurity action plan?

A similar concern arises with respect to item iv of paragraph 27, and §54.2004(b)(iv) which propose to require:

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.

This requirement indicates that the applicant must specify what equipment or services to request on its pilot Form 470, which presumably would have to be based on the eligibility list or criteria published in the Commission's report and order. But we are concerned that many applicants may not know what they need and therefore would be unable to complete the pilot application.

Detailed cost information that usually is not available until after the bidding process is completed is required in the Form 484. The estimated cost of the project including the estimated E-rate funding request and source of funds for paying the non-discounted share and ineligible costs are required. There is also an option to upload and submit documents in support of the pilot application. In other words, to become part of the pilot, the school or library already must know what cybersecurity protections they want to purchase, from the list of items that will presumably be announced in the report, the estimated costs (without first bidding the items) and the source of funds for the amounts not paid by E-rate. Typically, in the regular E-rate program, this information is collected in the Form 471 application *after* the bidding process has been completed. Essentially applicants must complete a request for information process to ask for price information and the service and equipment options from vendors to be able to complete the pilot application Form 484. Applicants must await the report and order to learn more about the equipment and services eligible for funding in the pilot before commencing to gather the required information and preparing the cybersecurity action plan.

This framework presupposes that applicants will be able to determine their needs for equipment and service before submitting their Form 484 pilot application. Indeed, Appendix B of the NPRM, the Initial Regulatory Flexibility Analysis, states in paragraph 33 that, “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.” Rather than requiring schools and libraries to incur additional costs for a mandatory assessment, the Commission should specify that completion or submission of an application for the free vulnerability assessment offered by CISA (<https://www.cisa.gov/cyber-hygiene-services>) is sufficient for meeting the assessment prerequisite as part of the Form 484 application process, and the ongoing evaluation and assessment expected of pilot participants is an eligible project cost that will be funded in part by E-rate.

Schools and libraries that lack sufficient and qualified staff to make these assessments should not be barred from the pilot. Nor should schools and libraries that have not yet availed themselves of free resources from CISA or other government organizations be barred. It may be reasonable to require selected pilot participants to utilize these resources as a condition of their participation to ensure all government resources are being leveraged. But mandating this condition as a prerequisite just raises the barriers to be able to participate in the pilot.

### **III. REVISIONS TO THE FORM 484 CAN COLLECT THE NEEDED INFORMATION IN LESS REQUIRED TIME FOR APPLICANTS.**

The NPRM also invited comments on the information collection requirements of the NPRM, and for which our comments will focus on the new proposed Form 484, Schools and Libraries Cybersecurity Pilot Program Application. The FCC estimated that fifteen (15) hours are required to complete the form. While fifteen (15) hours may be required or the data

entry of information in the online form, that estimate fails to consider the significant amount of time required to amass, organize and prepare the documentation required by the form.

The premise that each applicant must submit an encyclopedic amount of information to enable the evaluation and selection of the participants seems overly broad and burdensome. It is fair and accurate to predict that few, if any, applicants have on hand the information required by the form, and preparation and collection of that data will take considerable additional time for every applicant. SECA submits that the amount of information to be collected on the Form 484 should be limited to the critical information necessary for the evaluation and selection of participants and any other information should be collected only from the successful applicants that are chosen for the pilot.

There is an abundance of information that applicants must submit on the Form 484:

1. Background detailed information/assessment of current cybersecurity experience, actions, resources and challenges (Items 24 – 29, 41 - 44)
2. Narrative project plan that describes in detail the proposed approach including specific equipment and services, goals and objectives, including any cybersecurity requirements for vendors to provide free of charge (Items 30 – 36, 46, 50 – 51)
3. Financial aspects of the project including detailed cost estimates, sustainability plan, budget for non-eligible and non-discount cost amounts and source of funds (Items 52 – 58)
4. Evaluation and measurement of effectiveness including information to be collected from vendors (Items 37 – 40)
5. Other cybersecurity future plans outside of pilot (Items 47 – 49)

Each of these five aspects of the application requires research, information gathering, and generating documents and information that may not currently exist and will take substantial time. Preparing a budget will require the applicant to identify the services and/or equipment they want to buy with pilot funding and to obtain cost estimates for the equipment and services. A narrative description, budget, timeline, evaluation and description of past, current and future cybersecurity plans, including past incidents must all be available for the application.

SECA submits that the FCC should collect the background information in Item 1 above, and the projected project description in Item 2. The budget, evaluation plan and other future cybersecurity plans outside the pilot (Items 3 – 5 above) should be omitted from the Form 484 and collected at a later time from the pilot participants should the FCC feel the information is necessary.

This approach substantially reduces the burden on applicants to prepare their Form 483 applications and does not require all applicants to undertake such an arduous process just to apply to participate in the pilot. Should the FCC be concerned about limiting the allocation of funding to the \$200 million amount, they should instead allocate the pilot funding based on a prediscount budget amount similar to the administration of the E-rate Category two budgets.

By removing these requirements from the FCC Form 484, the burden on applicants will be alleviated significantly and the FCC can use other means such as the Form 471 application and/or the preparation of a post-commitment report or information collection from each selected pilot participant to obtain any required information.

#### **IV. REMOVING THE RESTRICTION AGAINST FULL ELIGIBILITY OF FIREWALLS SHOULD ALSO BE IMPLEMENTED PROMPTLY AND NOT AWAIT THE OUTCOME OF THE PILOT.**

SECA concurs with the numerous initial comments that urge the Commission to act promptly to remove the cost allocation requirement for advanced or next generation features of firewall equipment designed to defend against cyberattacks. The FCC has developed a substantial record to support this revision to the E-rate eligible services list. SECA recommends this restriction be lifted and implemented in a reasonable time frame that will enable all applicants to be informed of this change, and be able to meaningfully apply for E-rate funding.

Some commenters urge the Commission to swiftly act to implement this change for the upcoming funding year 2024 and to open a special filing window for this purpose, and to augment the existing Category 2 budget multipliers to reflect this added eligibility.

SECA is mindful that its recommendations in other proceedings may be at odds with these suggestions and therefore we do not offer an opinion on these recommendations. For example, in order to simplify the Category 2 budget process, SECA recommended to the FCC, and the FCC agreed, to set one budget multiplier amount for the full five years of the budget cycle, and not make annual inflation adjustments. This was recommended for simplicity and ease of administration. In the recent hot spot NPRM proceeding, SECA strongly encouraged the FCC to implement any new off-campus hotspot equipment and service eligibility effective for FY 2025 so as to provide sufficient advance notice to all stakeholders. We made these recommendations based on our experiences working with applicants that flourish more readily with consistent and dependable E-rate rules and deadlines.<sup>1</sup>

USAC's information technology resources likewise are a critical consideration in making these policy implementation decisions. A major change in the systems architecture to implement new FCC rules such as opening a special filing window and/or modifying the Category 2 budget tool requires considerable time and resources which are intensified when there is a compressed implementation deadline. These finite resources inevitably will be diverted from other IT projects that SECA and other stakeholders have requested, and that could streamline and improve the efficiency of the program – which are very important goals supported by applicants and the FCC and should continue to be balanced with new initiatives.

---

<sup>1</sup> Overall, the benefit of opening a special filing window for FY 2024 E-rate applications for advanced firewalls will only be realized if applicants remember to comply with the off-cycle form deadlines for filing FCC Form 486 and filing their Form 472 BEAR forms. If an applicant forgets to file FCC Form 486 or to file their BEAR form to recoup their E-rate discount funding, simply because the deadlines for each form were different from the usual program cycle timeline, they will have gone to great lengths to experience no added benefit from a special filing window.



Of course, should the FCC decide to modify the FY 2024 eligible services list to include advanced firewall features and/or to open a special filing form 471 filing window, SECA will assist applicants as we always strive to, and support their efforts to apply for advanced firewalls.

Should any firewall definitional changes be made to the ESL for FY 2024 we request that applicants be allowed to amend their FY 2024 firewall funding requests filed prior to the ESL change to add back costs for advanced features that may have been removed in the original application or during pre-commitment review. This should be allowed either through the RAL process in the case of pending applications or the appeal process in the case of funded applications.

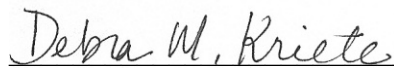
Should the budget multiplier for Category 2 be increased any time during the current budget cycle, the administrator should be required to update the category 2 budget tool to reflect any additional amounts of funding from an increase in the category 2 budget multiplier as soon as possible.

These measures will enable applicants to take maximum advantage of any changes in the eligibility of advanced firewall features as promptly as possible.

## V. CONCLUSION

The State E-rate Coordinators' Alliance respectfully requests the FCC to issue a Report and Order and to modify FCC Form 484 consistent with the recommendations set forth above.

Respectfully submitted,

A handwritten signature in cursive script that reads "Debra M. Kriete". The signature is written in dark ink and is positioned above a horizontal line.

Debra M. Kriete, Esq.  
State E-rate Coordinators' Alliance  
1300 Bent Creek Blvd, Ste 102  
Mechanicsburg, PA 17050  
717 232 0222  
dmkriete@comcast.net

February 27, 2024