Before the Federal Communications Commission

Washington DC 20554

In the Matter of	)	
	)	
Addressing the Homework Gap	)	WC Docket No. 23-234
Through the E-Rate Program	)	

Reply Comments of the national education organizations.

INTRODUCTION

On behalf of the 16 undersigned education associations, representing superintendents, principals, public and private schools, educators, rural educators, special educators, and more, these reply comments are submitted to the Wireline Competition Bureau's Public Notice (Notice) on the School and Libraries Cybersecurity Pilot Program. Many of the groups signing this letter have supported the E-Rate program since its enactment as part of the Telecommunications Act of 1996. Our groups are supportive of efforts to promote and improve the E-Rate to fulfill its mission of accelerating the deployment of advanced telecommunications and information services in schools and libraries, and have filed in many of the FCC's rulemakings related to the program. Our groups welcome the opportunity to provide feedback on this critically important proposal (hereinafter the "NPRM"), a pilot that will help schools and libraries bolster their cybersecurity in the short term while also generating the data and information necessary to inform future, broader cybersecurity decisions across the federal government, including the FCC, Congress, and other federal agencies.

We believe the critical need for schools and libraries to enhance cybersecurity for their respective networks is readily apparent from the countless and continuing media accounts of cyber-attacks on these institutions in every corner of the country A 2023 paper details school districts' ongoing struggles to stay ahead of the persistent cyber-attacks they face.[i] In essence, schools and libraries are operating in a world that is increasingly online, have become targets for cyber-attacks and lack the resources to deter or prevent them.

One significant driver of these cybersecurity issues is that school district efforts to ensure 1:1 student-to-device ratios —underway in many school districts before the COVID-19 pandemic—expanded exponentially as communities responded to the need for learners to participate in meaningful teaching and learning. Another is that school district administrative processes, including student health and disciplinary records, are being or already have been digitized and stored on school district servers or in the cloud.

This rapid shift to teaching, learning and district operations moving online has outpaced many school districts' existing cybersecurity infrastructure. The result? Sensitive student and personnel data remains vulnerable to cyber-attacks. The Commission's NPRM notes: "…K12 schools and libraries will continue to be prime targets for malicious actors, primarily because they are data-rich environments that tend to lag behind in terms of their available resources and cybersecurity program maturity." [ii]

Simply ignoring the problem is not a satisfactory response because cyber-attacks have real costs. The Government Accountability Office (GAO) quantified the impact of cyber attacks on schools in a 2021 report, detailing that 647,000 K-12 students were affected by ransomware attacks and that school district costs of downtime from such attacks were estimated to be $2.38 billion.[iii]

The comments below reflect our support for the proposed cybersecurity pilot; call on the FCC to move forward with establishing the proposed pilot in a timely manner; endorse FCC efforts to ensure representation among the participants, across myriad demographics; and support a flexible timeline within the three-year proposal.

KEY EDUCATION GROUP POSITIONS

1. Our groups support this proposed pilot because schools and libraries need additional financial support for cybersecurity technology as well as training solutions. Federal resources would be particularly helpful as state and local financial support has been limited. A 2024 report from the Consortium for School Networking (CoSN) detailed significant state policy interest in this issue but also highlighted the continued lack of funding from state governments: In 2023, state legislators introduced 307 cybersecurity bills with direct or indirect implications for schools, and states adopted 75 of these measures into law. The new laws feature valuable policy changes, but few provided cybersecurity financial assistance to schools.[iv] States are providing policy, but not funding, and that is a critical gap in successful implementation of cybersecurity strategies. CISA took issue with this same problem in December 2023, writing "There is simply no way we can expect school districts, whose primary objective is to ensure the learning and safety of schoolchildren, to bear the cybersecurity burden alone."v

2. Our groups support this proposed pilot because we believe it will serve as a critical component of what must be a coordinated federal response to cyber-attacks across multiple federal agencies. In addition to the Commission, numerous arms of the federal government, from the Department of Education to the Department of Commerce to the Department of Justice, all play significant policy or enforcement roles in this area, and each has produced assets which can assist school and library efforts to deter or prevent cyber-attacks. This pilot will provide critical data that will not only inform the Commission about the scope and variety of cyber-attacks affecting schools and libraries but also the costs of different solutions. It will also supply other federal agencies with useful information.

3. Our groups align with the majority of the feedback submitted by other national education, technology and learning companies replying to the proposed pilot, including K12Six, CoSN, and Council of Great City Schools, among others. At the same time, we stop short of their premature proposal to immediately add advanced firewalls to the E-Rate eligible services list. The very purpose of the pilot is to demonstrate the need for and costs of cybersecurity measures such as advanced firewalls, and to gauge how districts would respond to available federal funding. We have absolute faith the pilot will not only demonstrate demand for cybersecurity supports, but also generate data to inform a future, broader cyber response.

RESPONSES TO NPRM QUESTIONS

- **Authority**: We agree with the Commission's analysis that it has the legal authority to move forward with this pilot .The Telecommunications Act of 1996 , which authorizes E-Rate, is explicit: "Universal service is an evolving level of telecommunications services that the Commission shall establish periodically under this section, taking into account advances in telecommunications and information technologies and services."[vi]
- **Duration**: The Commission's NPRM proposes a three-year timeline for the pilot. We recommend the pilot move forward with the framing of a three-year pilot while allowing an expedited timeline for participants whose cyber plan can be carried out more quickly. Eligible participants should receive their funding in one lump sum and be able to spend down over an 18 to 36-month timeframe. The FCC could ask applicants to outline their proposed timeline in their application, though any such detail in the application would not be binding.

  The proposed pilot calls for a representative sample of participants, which presumably would include schools and libraries occupying different levels of cybersecurity sophistication -- some on the cutting edge of cyber response, those just beginning the work of building their cyber defenses, and everyone in between. It makes sense, then, that while some participants would welcome a three-year pilot to allow them time to plan, implement, and evaluate, others would see the pilot as an opportunity to build out their current cyber response or otherwise update an existing "cyberstructure". If and when pilot participants demonstrate an ability to access and invest their funds in an abbreviated timeline, we support such flexibility. We think there is room for the pilot to accommodate an 18-month timeline or a three-year timeline, both of which are aligned to real-world procurement cycles. Echoing a sentiment submitted by CoSN et al in their comments , "A less lengthy pilot would also more swiftly help answer the question posed by the Commission's proposed third goal for the pilot, "How to leverage other federal K–12 cybersecurity tools and resources to help schools and libraries effectively address their cybersecurity

needs. A shorter pilot period is justified by the urgent need to help more of the nation's schools and libraries bolster their cybersecurity."[vii]

- **Leveraging Other Federal Resources &Training**: Our groups recognize that technology is not the sole solution to cyber-threats; training is a critical component that cannot be ignored. We also recognize that elements of the federal government —including the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and the U.S. Education Department, among others— have created high-quality, free or low-cost resources and tools that will help schools and libraries provide training to their personnel, students, and library patrons on avoiding cyber-attacks. That said, we do not believe that schools and libraries should be required to make use of these federal government tools and resources, as suggested by the NPRM, because many schools and libraries have implemented their own cybersecurity strategies already. Instead, we recommend that the Commission require that school and library participants in the pilot engage in some form of training (either courses, materials, or both) as a condition of receiving pilot funding, but not mandate using federal resources as the only acceptable way of fulfilling that condition.
- **Size of Fund**: The NPRM proposes an initial $200 million investment in the pilot. This is obviously far short of what is needed for a pressing reality that will be exponentially more expensive. More concisely, the available funding is not even a drop in the bucket in terms of what it will take to help schools and libraries come online with basic cybersecurity. That said, we commend the commission for finding the money it did and marking it for such a critical issue. We also note that the pilot includes a very modest goal of improving the security of E-Rate funded networks and data, not ensuring their complete protection. We take this goal to mean that the pilot represents but a downpayment on what will be an enduring, expensive need in an increasingly online and digitized K12 and library experience. We look forward to continuing the conversation on the role of USF in supporting cyber response and working to expand available funding.
- **Participants**: We commend the Commission for their continued focus on representation within the pilot. In response to the Commission's question about how to choose the schools and libraries who participate in the pilot, we align with the comments filed by CoSN et.al, who wrote: "…the Commission should balance the need to choose a diversity of schools and libraries with the need to prioritize the highest-need schools and libraries, per E-rate principles." We agree with the NPRM that the Commission should strive to include a wide range of school and library participants in the pilot program to develop the best possible body of evidence for future decisions about the E-rate program and other government cybersecurity investments. The pilot sample should include a pool of schools and libraries representative of small and large, rural, and urban, and other characteristics. The Commission must, however, seek to prioritize (over sample) the inclusion of the highest need schools and libraries, consistent with the E-rate's

longstanding emphasis on providing the most assistance to the applicants demonstrating the greatest financial need. This strategy could take the form of oversampling high financial need schools and libraries within each target demographics (rural and urban, small, and large, etc.) sought to ensure the pilot evaluation provides the data required for later decision making." [viii]

CONCLUSION

We appreciate the opportunity to weigh-in on the particulars of the Commission's cybersecurity pilot proposal and look forward to working with the FCC as this matter proceeds.

Signing Groups

AASA, The School Superintendents Association
American Federation of School Administrators
American Federation of Teachers
Association of Educational Service Agencies
Association of Latino Administrators and Superintendents
Association of School Business Officials International
Council of Administrators of Special Education
National Alliance of Black School Educators
National Association of Independent Schools
National Association for Pupil Transportation
National Association of Federally Impacted Schools
National Association of Elementary School Principals
National Association of Secondary School Principals
National Catholic Education Association
National Education Association
National Rural Education Association

---

[i] Michele Kielty & A. Renee Staton, Leading K-12 Community Responsiveness to Cyber Threats via Education of School Community, 2024 J. Cybersecurity Educ. Res. & Prac. 28 (2023).
[ii] *Cybersecurity Pilot NPRM* at para. 6
[iii] U.S. Gov't Accountability Office, GAO-23-105480, Critical Infrastructure Protection: Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity 15-17 (2022), https://www.gao.gov/assets/gao-23-105480.pdf.
[iv] CoSN, 2023 Education Cybersecurity Policy Developments, (Jan, 2024), https://www.cosn.org/cybersecurity-2023legislation/
[v] Cybersecurity and Infrastructure Security Agency, Findings and Updates from CISA's Ongoing Collaboration with Education Technology Vendors to Address K-12 Cybersecurity Challenges (Dec. 12, 2023), https://www.cisa.gov/news-events/news/findings-and-updates-cisas-ongoing-collaboration-education-technology-vendors-address-k-12
[vi] 47 U.S.C. §254(c)(1)
[vii] CoSN, SEDTA, CGCS, SHLB, NSBA, NASBE, CCSSO ECFS Filing (https://shorturl.at/aeklu) (Accessed February 1, 2024)
[viii] ibid.