Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of

Schools and Libraries Cybersecurity Pilot Program

WC Docket No. 23-234

COMMENTS RESPONDING TO THE COMMISSION'S PROPOSAL TO ESTABLISH A SCHOOLS AND LIBRARIES CYBERSECURITY PILOT PROGRAM

CONSORTIUM FOR SCHOOL NETWORKING
Keith Krueger, Chief Executive Officer

AMERICAN LIBRARY ASSOCIATION
Megan Janicki, Deputy Director, Public Policy and Advocacy

SCHOOLS, HEALTH & LIBRARIES BROADBAND COALITION
John Windhausen, Jr., Executive Director

NATIONAL ASSOCIATION OF STATE BOARDS OF EDUCATION
Paolo DeMaria, President and Chief Executive Officer

ALL4ED
Rebeca Shackleford, Director of Federal Government Relations

PACIFIC NORTHWEST GIGAPOP
Amy Philipson, Executive Director

STATE EDUCATIONAL TECHNOLOGY DIRECTORS ASSOCIATION
Julia Fallon, Executive Director

COUNCIL OF THE GREAT CITY SCHOOLS
Dr. Raymond C. Hart, Executive Director

NATIONAL SCHOOL BOARDS ASSOCIATION
Verjeana McCotter-Jacobs, Executive Director and Chief Executive Officer

COUNCIL OF CHIEF STATE SCHOOL OFFICERS
Peter Zamora, Director of Federal Relations and Policy Advocacy

LINK OREGON
Steve Corbató, Executive Director

COMMON SENSE
Amina Fazlullah, Head of Tech Policy Advocacy

SUMMARY

Schools and libraries face an urgent, complex cybersecurity crisis. Cybercriminals and other bad actors persistently target them for serious ransomware and other cyberattacks, seeking to acquire sensitive student and patron data and to steal public funds. Resulting network outages frequently disrupt learning and library services, imposing huge costs on individuals, institutions, and communities. The Commission's proposed cybersecurity pilot program represents an effective and pragmatic way to acquire data and other information to modernize E-rate and to inform other federal cybersecurity policies and programs. Our organizations welcome the Commission's decision to open this important proceeding and respectfully urge the agency to:

- Update the E-rate program's technologically outdated firewall definition to include advanced features like intrusion detection that are now standard components of firewalls. Designate firewalls with these advanced features as fully eligible for Category Two E-rate support. The Commission's recent firewall proceeding provides a comprehensive and nearly unanimous record to justify this change.

- Augment schools' and libraries' existing Category Two budgets by providing $200 million in supplemental Category Two funding for applicants to use in 2024 and 2025. This step will enable schools and libraries to access firewall cybersecurity protections without delay while the pilot produces data to information other policy improvements.

- Establish an 18-month cybersecurity pilot program providing no less than $200 million to participant schools and libraries. The pilot would fund purchases of cybersecurity services and equipment while gathering data about participants' implementation of best practices pre- and post-pilot. An 18-month pilot reflects real-world procurement cycles and the pressing need to implement other cybersecurity policy changes.

This recommended strategy will immediately help schools and libraries enhance protection of E-rate funded networks via modern firewalls, while collecting valuable data to shape future policymaking in this domain by the FCC and partner federal agencies. Consistent with E-rate principles, the pilot should be representative of a diverse range of applicants but prioritize the highest poverty schools and libraries. Evaluation should center on measuring cybersecurity maturity growth. The commenters stress that the firewall change and related funding increase should not await the pilot outcomes.

The Commission has clear legal authority for the proposed cybersecurity pilot. The Telecommunications Act makes clear that "Universal service is an evolving level of telecommunications services" and the services proposed by the pilot reflect ongoing advances in schools and libraries broadband networks and services consistent with this provision. Furthermore, cyberattacks throttle or completely thwart the ability of schools and libraries to use the "advanced telecommunications and information services" promised by the Act's universal service and other provisions.

Table of Contents

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of

Schools and Libraries Cybersecurity Pilot Program — WC Docket No. 23-234

COMMENTS RESPONDING TO THE COMMISSION'S PROPOSAL TO ESTABLISH A SCHOOLS AND LIBRARIES CYBERSECURITY PILOT PROGRAM

The Consortium for School Networking, the State Educational Technology Directors Association, the American Library Association, the Schools, Health & Libraries Broadband Coalition, the Council of the Great City Schools, the National Association of State Boards of Education, the Council of Chief State School Officers, the National School Boards Association, All4Ed, Common Sense, Pacific Northwest Gigapop, and Link Oregon respectfully submit these comments urging the Federal Communications Commission ("FCC" or "Commission"): (1) to immediately remove the required cost allocation of "advanced" features of firewalls, and designate advanced firewalls as fully eligible under E-rate Category Two; (2) provide at least $100 million per year in supplemental funding to E-rate Category Two for advanced firewalls for 2024 and 2025; and (3) establish a $200 million or more schools and libraries cybersecurity pilot program within the Universal Service Fund ("USF").[1] Modernizing the E-rate's firewall definition immediately, based on the extensive and favorable record gathered through the FCC

[1] 47 U.S.C. §254; 47 CFR Part 54.

Wireline Bureau's 2023 firewall proceeding[2], while also separately launching a pilot program to gather data about the school and library community's other cybersecurity needs and costs, will further the universal service goals and principles of the Telecommunications Act of 1996, including ensuring that schools and libraries have access to an evolving level of advanced telecommunications and information services.[3]

Our organizations represent a collection of school district, state education agency, library, broadband, privacy, and non-profit groups who are concerned about the pervasive and costly cyberattacks plaguing the nation's schools and libraries. Our members and partners in the field – the expert professionals responsible for establishing, managing, and securing broadband networks, internal connections, and data systems – often struggle independently to stay ahead of the domestic and international cyber criminals who use ransomware and other cyberattacks to acquire highly confidential student, library patron, and employee data, and steal public and private funds.[4] Writing about this problem in December 2023, the Cybersecurity and Infrastructure Security Agency ("CISA") said, "There is simply no way we can expect school districts, whose primary objective is to ensure the learning and safety of schoolchildren, to bear

[2] Wireline Competition Bureau Seeks Comment on Requests to Allow the Use of E-Rate Funds for Advanced or Next-Generation Firewalls and Other Network Security Services, Public Notice, 37 FCC Rcd 14633 (WCB 2023).
[3] 47 U.S.C. § 254(c)(1); Telecommunications Act of 1996, P.L. 104–104, Feb. 8, 1996, 110 Stat. 56
[4] 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).

the cybersecurity burden alone."[5] CISA said schools tend to be targeted for two primary reasons: they are "target rich and cyber poor."[6]

Secure high-capacity broadband access is essential to students' success. Given the immense challenge of solving the nation's K-12 school and library cybersecurity problem, our organizations welcome the Commission's invitation to comment on the value of using the proposed cybersecurity pilot program to help at least a limited group of schools and libraries mitigate risk and otherwise strengthen their cybersecurity in the near term, while also gathering additional data to inform future, farther reaching, cybersecurity policy decisions by the Commission and other federal agencies tasked with strengthening the nation's cybersecurity.[7] The other recommended actions described in these comments should be implemented in conjunction with the pilot, and not await the pilot's outcome.

1. THE CYBERTHREAT TO SCHOOLS AND LIBRARIES IS WIDESPREAD, COSTLY, AND UNDERMINES STUDENTS' AND PATRONS' PRIVACY AND ACCESS TO ADVANCED TELECOMMUNICATIONS AND INFORMATION SERVICES

Despite uneven cyberattack reporting by schools and libraries due to reputational concerns, potential liability, operational considerations, or other reasons, the cyberthreat to the their networks and sensitive data is well documented in the record gathered through the Wireline Competition Bureau's request for public input regarding proposed use of E-Rate funds for

---

[5] 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.

[6] U.S. K-12 Schools Are a Playground for Cyber Criminals." S&P Global, 24 Jan. 2024, https://www.spglobal.com/ratings/en/research/articles/231024-u-s-k-12-schools-are-a-playground-for-cyber-criminals-12892707. Accessed 24 Jan. 2024.

[7] Schools and Libraries Cybersecurity Pilot Program, Notice of Proposed Rulemaking, 88 Fed. Reg. 90141 (proposed Dec. 29, 2023) (to be codified at 47 CFR Pt. 54) ("Cybersecurity Pilot NPRM").

advanced or next-generation firewalls and other network security services.[8] Other government agencies and offices have reported on the problem. The Government Accountability Office ("GAO") reported that, in 2021, 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.[9] The study cited by the GAO shows that cyberattack costs are also very high at the school district level. For example, "Buffalo Public Schools saw recovery costs of around $10 million after its March 2021 attack, Baltimore County Public Schools reported recovery costs of around $8.1 million after its November 2020 attack…"[10] CISA aptly summarized the scale and seriousness of the cybersecurity challenge when it wrote, in 2023, that "Malicious cyber actors are targeting K–12 education organizations across the country, with potentially catastrophic impacts on students, their families, teachers, and administrators."[11] The topic has captured the attention of state policymakers. 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 direct cybersecurity financial assistance to schools.[12]

---

[8] Wireline Competition Bureau Seeks Comment on Requests to Allow the Use of E-Rate Funds for Advanced or Next-Generation Firewalls and Other Network Security Services, Public Notice, 37 FCC Rcd 14633 (WCB 2023)("Firewall Public Notice").

[9] 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.

[10] Paul Bischoff, Ransomware Attacks on US Schools and Colleges Cost $9.45bn in 2022, Comparitech (Aug. 31, 2021), https://www.comparitech.com/blog/information-security/school-ransomware-attacks/.

[11] Cybersecurity and Infrastructure Sec. Agency, Protecting Our Future: Partnering To Safeguard K-12 Organizations From Cybersecurity Threats (2023), https://www.cisa.gov/sites/default/files/2023-01/K-12report_FINAL_V2_508c_0.pdf.

[12] CoSN, 2023 Education Cybersecurity Policy Developments, (Jan, 2024), https://www.cosn.org/cybersecurity-2023legislation/

Like schools, libraries also routinely face cyberattacks capable of compromising their E-rate supported broadband networks and the sensitive private patron, personnel, and other data they contain. The May 2023 shutdown of Ohio's Akron-Summit County Library and its 18 countywide branches spotlights the challenge. A debilitating ransomware attack locked the library's network, preventing staff and the public from accessing their computers. With phones unusable and borrowing records blocked, all automated library operations were ground to a halt.[13] Even very large library systems are vulnerable to cyberattacks and need sustained assistance. Meeting with the Commission in July 2023, Mr. David Leonard of the Boston Public Library said despite having robust infrastructure, good protocols and knowledgeable staff, the Boston Public Library was a victim of a major ransomware attack in 2021. He added that without proper cybersecurity investments, attacks will continue to disrupt broadband services that E-rate supports for Boston's library patrons.[14] Boston's central library and twenty-five neighborhood branches serve nearly 4 million visitors per year and millions more online, so service disruptions caused by cyberattacks are significant.[15]

We agree with the Commission's analysis and finding that it has the legal authority for the proposed pilot. The Telecommunications Act makes clear that "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

---

[13] April Helms & Alan Ashworth, Akron-Summit County Library: Ransomware Behind Cyberattack, Hopes Website Fixed by Monday, Akron Beacon J. (May 31, 2023), https://www.beaconjournal.com/story/news/local/2023/05/31/outage-akron-summit-county-public-libraries-branches-are-open/70273296007/.

[14] Schools, Health & Libraries Broadband (SHLB) Coal., Letter to Marlene H. Dortch, Sec'y, FCC, WC Docket No. 13-184 (filed July 27, 2023), https://www.fcc.gov/ecfs/document/10703289476252/1.

[15] "About the BPL." *Boston Public Library*, www.bpl.org/about-the-bpl/. Accessed January 23, 2024.

technologies and services."[16] The proposed new services reflect ongoing advances in schools and libraries broadband networks and services consistent with this provision. The Commission also correctly notes, as demonstrated by the extensive firewall proceeding record and other evidence, that cyberattacks throttle or completely thwart the ability of schools and libraries to use the "advanced telecommunications and information services" promised by the Act.[17] For these and the other reasons described in the notice of proposed rulemaking, we agree that the Commission is well within its legal authority to establish the pilot.

2. THE COMMISSION SHOULD IMMEDIATELY ADD ADVANCED FIREWALLS TO THE E-RATE ELIGIBLE SERVICES LIST AND SUPPLEMENT APPLICANTS' CATEGORY 2 FUNDING ALLOCATIONS FOR 2024 AND 2025

On December 14, 2022, the Wireline Competition Bureau ("Bureau") requested public comment regarding a 2020 petition for rulemaking and other formal requests for the Commission's permission to use E-Rate funds for advanced or next-generation firewalls and other network security services.[18] The Bureau's firewall proceeding produced an extensive record, including over 150 comments and reply comments filed by school districts, state education agencies, library leaders, privacy advocates, and an array of representative national education and other professional associations. The proceeding record reflects near unanimous agreement that the Commission should modernize the E-rate program's technologically out-of-date firewall definition and provide program applicants an opportunity to use their E-rate Category Two funding for advanced or next generation-firewalls.[19] To be clear, the language

[16] 47 U.S.C. §254(c)(1).
[17] 47 U.S.C. §254(h)(2).
[18] Firewall Public Notice.
[19] See, Reply Comments of the Los Angeles Unified School District and State and Regional Education Agencies, WC Docket No. 23-234 (filed Mar. 29, 2023); Comments of the Massachusetts Educational Technology Administrators Association, WC Docket No. 23-234

"advanced" or "next generation" refers to any feature that is not considered to be part of a basic firewall as defined at least as far back as 2014.[20]

Given the overwhelmingly positive record in the firewall proceeding, the ongoing, serious cyber threat facing schools and libraries, and the shortage of sustained K-12 cybersecurity funding, the Commission should add the intrusion detection and network security features that are now standard components of firewalls – defined by the Commission as "advanced or next-generation" firewalls to the Eligible Services List for the E-rate's 2025 program year and open a special window in 2024 for applicants to seek Category Two funds for acquiring advance firewalls in 2024. Eighty-one percent (81%) of K-12 respondents to the 2022 Nationwide Cybersecurity Review reported the "lack of sufficient funding" as their top security concerns.[21]

In taking this step to protect the integrity of E-rate supported broadband networks, the Commission should adopt a broad and technologically neutral firewall definition. Individual schools and library applicants should be permitted to select from an array of firewall options for protecting their network. Adopting a more inclusive firewall definition will provide applicants with the community level flexibility required to maximize E-rate's potential positive impact on schools' and libraries' cybersecurity. The existing E-rate cost-effectiveness safeguards such as the Category Two budget, the requirements to conduct a competitive bid and to pay the non-

(filed Mar. 19, 2023); Reply Comments of the Texas Education Technology Leaders, WC Docket No. 23-234 (filed Mar. 27, 2023).

[20] Cybersecurity Pilot NPRM, n.1; Firewall Public Notice, n.17.

[21] K-12 Report CIS MS-ISAC Cybersecurity Assessment of the 2022–2023 School Year, https://learn.cisecurity.org/2023-k-12-report-media, Accessed 23 January 2024

discounted share, will serve as protections to ensure reasonable and efficient use of E-rate funding for firewall cybersecurity protection.

Currently, these advanced features must be cost-allocated or deducted from the E-rate eligible pre-discount amount of the firewall, and applicants must pay for those critical protections without being able to leverage E-rate. By removing this requirement, the Commission will be updating the definition of the E-rate eligible firewall to include these vital network security features.

In addition to modernizing the outdated firewall definition, we urge the Commission to supplement program participants' Category Two budgets to enable applicants to benefit from this definitional update immediately. Otherwise, applicants with exhausted or insufficient Category Two budgets for the FY 2021-2025 cycle will be unable to leverage E-rate funding to buy this essential component to protect their networks until the next E-rate Category Two budget cycle is set for FY 2026 – FY 2030. Specifically, we ask the Commission to add $200 million to the Category Two budgets for FY 2024 and FY 2025 and adjust the formula for the school and library budget multipliers accordingly. This increase, above and beyond the proposed pilot funding, will enable a meaningful number of eligible schools and libraries to acquire firewalls.[22] This capped amount, administered through the existing Category Two formula, provides budget certainty for the program and aligns with the ranges provided through the recent expert analysis and recommendations made by the E-rate consulting firm Funds for Learning.[23] It is also relatively small, in light of the billions of dollars in cyberattack costs that experts estimate are

[22] See, Reply Comments of New York State E-rate Applicants (WC Docket 13-184), ("Firewall Public Notice").
[23] Funds for Learning, Letter to Marlene H. Dortch, Secretary, FCC, WC Docket No. 13-184, (filed Nov. 21, 2022).

imposed on schools and libraries and the broader economy.[24] Given that the 2024 E-rate application window will close before the Commission is able to take action, we urge the agency to open a special filing window in summer or fall 2024 to enable applicants to apply for firewall equipment using their Category Two budgets as adjusted by the $200 million of additional Category Two firewall funding provided for this year.[25]

3. THE COMMISSION SHOULD ESTABLISH A SHORTENED SCHOOLS AND LIBRARIES CYBERSECURITY PILOT PROGRAM WITHIN THE UNIVERSAL SERVICE FUND TO INFORM THE NEXT FIVE-YEAR BUDGET CYCLE FOR E-RATE CATEGORY TWO AND OTHER RELATED DECISION MAKING.

A. Shorten the Proposed Pilot Timeline

The proposed 3-year pilot timeline should compress to 18 months reflecting real-world procurement cycles and the need to move more quickly to adjust broader Commission policies and practices. This approach would enable, depending on the pilot start date, the agency to use the pilot program data and related evaluation to inform the next fixed Category Two five-year budget cycle, which begins with program year 2026.[26] 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."[27] A shorter pilot period is justified by the urgent need to help more of the nation's schools and libraries bolster their cybersecurity.

---

[24] The technology research company, Comparitech, notes that "since 2018, ransomware attacks on the education sector have cost the world economy over $53 billion in downtime alone. Comparitech Website (Sep. 2023), https://www.comparitech.com/blog/vpn-privacy/school-ransomware-attacks-worldwide/.

[25] The Joint Commenters believe that cybersecurity protection is such a paramount concern to schools and libraries that a special filing window for FY 2024 is warranted, limited to applications for firewalls based on the updated ESL that allows for funding of the network.

[26] Modernizing the E-Rate Program for Schools and Libraries, Report and Order, 34 FCC Rcd 11967 (2019).

[27] Schools and Libraries Cybersecurity Pilot Program NPRM, Paragraph 6.

We support the Commission's plan to model the cybersecurity pilot after the successful Connected Care Pilot. The cybersecurity threats facing schools and libraries, however, justify a faster process. An 18-month pilot schedule better reflects the real-world procurement cycles of school districts and library systems seeking cybersecurity solutions. It also provides expanded cybersecurity protections at a critical juncture when threats to schools and libraries are rapidly evolving. Select schools and libraries have confirmed that they can complete needs assessments, bidding, purchases, and deployment on this briefer timeline without shortchanging quality or rigor, if the Universal Service Administrative Company is equipped to manage a timely application approval process. This approach provides sufficient data to inform future policy while recognizing the need for nimble, timely security in a shifting threat landscape.

B. Expand the Pilot's Proposed Budget

The Commission's first proposed goal is to "impro[ve] the security and protection of E-Rate-funded broadband networks and data." Considering this goal and given the urgent need to help as many of the nation's schools and libraries strengthen the cybersecurity of their E-rate funded networks, we urge the Commission to allocate more than $200 million for the pilot program. According to the National Center for Education Statistics, as of 2020, there are over 98,000 public schools and over 30,000 private schools in the United States.[28] The American Library Association estimates that there are over 123,000 libraries of all kinds in the United States today.[29] Given this huge pool of schools and libraries, and based on the significant number of

[28] National Center for Education Statistics (2020). Fast Facts Tools, Ed.gov. https://nces.ed.gov/fastfacts/display.asp?id=84.

[29] American Library Association, Library Statistics and Figures: Number of Libraries in the United States, https://libguides.ala.org/c.php?g=751692&p=9132142.

cyberattacks on schools and libraries, more than $200 million is needed to help more schools and libraries in the near term, and to ensure the pilot program produces a comprehensive evaluation of the investment's impact on schools and libraries access to sufficient cybersecurity. The pilot budget should increase within the USF budget, particularly given that E-rate funding has been well below the program's annual cap for recent program years.[30]

C. Develop a Pilot Sample Representative of E-rate Applicants.

In choosing the schools and libraries to participate in the pilot, 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, prioritize 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 with the greatest financial need. A higher proportion or percentage of the most impoverished applicants that request to participate in the pilot should be selected. Additionally, the Commission should seek to ensure the group of pilot participants reflect diverse characteristics, such as being located throughout the country, in rural and urban areas, and range in size from small to large organizations.

D. Adopt a Cybersecurity Maturity Model to Evaluate the Pilot

[30] Wireline Competition Bureau. (2023, May). Wireline competition bureau directs USAC to fully fund eligible Category One and Category Two E-rate requests (Public Notice No. CC Docket 02-6). Federal Communications Commission.

The pilot program's effectiveness should be measured by its impact on expanding schools' and libraries' access to and adoption of cybersecurity. Such an evaluation could be accomplished in more than one way, but we recommend that the Commission adopt or develop a cybersecurity maturity model for pilot participants that uses a rubric that assesses critical security controls and preparedness. Using this approach, pilot schools and libraries would complete an assessment when applying to the pilot and at the end to measure improvement. The Commission also could consider evaluating pilot participants' implementation of CISA and U.S. Department of Education priorities and National Institute of Standards and Technology (NIST) best practices.[31] With this evaluation data, the Commission would aim to catalog the degree of best practice implementation beforehand and measure adoption increases enabled by pilot funding and support.

E. Pilot Data Access

Consistent with the Universal Service Administrative Company's ("USAC") open data model for the E-rate and other universal service programs, we urge the Commission to adopt an open data model for the cybersecurity pilot that is designed to enable the public, researchers, program participants, and other stakeholders to independently analyze and use aggregate/anonymized data to support informed decision-making.[32] By making the pilot data open and usable, the Commission will promote transparency, accountability, public engagement and data-driven decision-making. The approach aligns with the Commission's data practices,

[31] U.S. Dep't of Educ. & Cybersecurity and Infrastructure Sec. Agency, Defensible & Resilient K-12 Digital Infrastructure Brief (2023), https://tech.ed.gov/files/2023/08/DOEd-Report_20230804_-508c.pdf.; Consortium for Sch. Networking (CoSN), NIST Cybersecurity Framework Resource Alignment for K-12 (2023), https://www.cosn.org/tools-and-resources/resource/cosns-nist-cybersecurity-framework-resource-alignment-for-k-12/.

[32] Universal Serv. Administrative Co., Open Data Tools, https://opendata.usac.org/ (last visited Jan. 22, 2024)..

and related federal requirements such as the Foundations for Evidence-Based Policymaking Act of 2018 and Federal Data Strategy.[33] We remind the Commission, however, that this transparency should not extend to technical or other information collected through the pilot that might compromise school and library participants' cybersecurity. Affirmative steps must be taken to protect the confidentiality of sensitive security data submitted by applicants. We encourage the Commission to adopt a layered data management strategy that allows the wider analysis of non-sensitive data while safeguarding sensitive details. Such a strategy could include removing all personally identifiable information from applicant's cybersecurity posture data, aggregating data across applicants to publish general statistics and trends rather than applicant-specific information and storing sensitive data in encrypted formats in access-controlled databases.[34]

CONCLUSION

Our organizations respectfully urge the Commission to swiftly modernize the E-rate program's firewall definition, increase the Category Two budget beginning with fiscal year 2024 and quickly establish the cybersecurity pilot program consistent with the above recommendations. Adopting this multi-part strategy will help more schools and libraries improve the security and protection of their E-Rate-funded broadband networks and data, while also producing the data required to shape the longer-term cybersecurity strategies of the Commission

[33] Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435, 132 Stat. 5529; Exec. Office of the Pres., Office of Mgmt. & Budget, Federal Data Strategy (2019).
[34] See, e.g., Nat'l Acads. of Scis., Eng'g, & Med., Principles and Practices for a Federal Statistical Agency: Seventh Edition (2021); Sci. & Tech. Policy Inst., Building Data Capability: A Guide for Legal Departments (2021)

and other federal agencies responsible for helping schools and libraries mitigate the risk of ransomware and other cyberattacks.

Respectfully submitted,

CONSORTIUM FOR SCHOOL NETWORKING
Keith Krueger, Chief Executive Officer

AMERICAN LIBRARY ASSOCIATION
Megan Janicki, Deputy Director, Public Policy and Advocacy

SCHOOLS, HEALTH & LIBRARIES BROADBAND COALITION
John Windhausen, Jr., Executive Director

ALL4ED
Rebeca Shackleford, Director of Federal Government Relations

NATIONAL ASSOCIATION OF STATE BOARDS OF EDUCATION
Paolo DeMaria, President and Chief Executive Officer

PACIFIC NORTHWEST GIGAPOP
Amy Philipson, Executive Director

STATE EDUCATIONAL TECHNOLOGY DIRECTORS ASSOCIATION
Julia Fallon, Executive Director

COUNCIL OF THE GREAT CITY SCHOOLS
Dr. Raymond C. Hart, Executive Director

NATIONAL SCHOOL BOARDS ASSOCIATION
Verjeana McCotter-Jacobs, Executive Director and Chief Executive Officer

COUNCIL OF CHIEF STATE SCHOOL OFFICERS
Peter Zamora, Director of Federal Relations and Policy Advocacy

LINK OREGON
Steve Corbató, Executive Director

COMMON SENSE
Amina Fazlullah, Head of Tech Policy Advocacy