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

In the matter of Allowing the Use of E-Rate Funds for Advanced or Next-Generation Firewalls and Other Network Security Services	WC Docket No. 13-184

COMMENTS RESPONDING TO THE WIRELINE BUREAU'S PUBLIC NOTICE REGARDING ALLOWING THE USE OF E-RATE FUNDS FOR ADVANCED OR NEXT-GENERATION FIREWALLS AND OTHER NETWORK SECURITY SERVICES

CONSORTIUM FOR SCHOOL NETWORKING
Keith Krueger, Chief Executive Officer

COUNCIL OF CHIEF STATE SCHOOL OFFICERS
Carissa Moffat Miller, Chief Executive Officer

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

STATE E-RATE COORDINATORS' ALLIANCE
Debra M. Kriete, Chair

NATIONAL ASSOCIATION OF STATE BOARDS OF EDUCATION
Paolo DeMaria, President and CEO

ALL4ED
Rebeca Shackleford, Director of Federal Government Relations

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
John Heim, Executive Director and CEO

CENTER FOR DEMOCRACY AND TECHNOLOGY
Cody Venzke, Senior Counsel Equity in Civic Technology

BENTON INSTITUTE FOR BROADBAND & SOCIETY
Adrianne Furniss, Executive Director

February 13, 2023

SUMMARY

Far too many of America's schools and libraries fall on the wrong side of the cybersecurity poverty line. All schools and libraries are at significant risk, but the community anchor institutions in the nation's most vulnerable communities often lack sufficient cyber protections. Successful cyberattacks cause lost instructional time, halt library services, and compromise sensitive personally identifiable information. Such disruptions disproportionately harm the populations that depend most on schools and libraries. Given this immense digital equity challenge, the above organizations respectfully urge the Wireline Bureau to: (1) make advanced or next generation firewalls and related features eligible for E-rate Category 2 support beginning in 2024; (2) increase Category 2 funding levels, within the E-rate program's existing aggregate cap, to cover modern firewalls; and (3) provide this limited E-rate cybersecurity support in a manner that is minimally burdensome to applicants and permits schools and libraries to select the modern firewall technology most aligned to their needs.

The Bureau can help the schools and libraries struggling on the wrong side of the cybersecurity poverty line by modernizing the E-Rate's definition of "Firewall or Firewall Service" to encompass advanced or next generation firewalls. The Bureau should adopt and apply a single, revised Firewall or Firewall Service definition across the E-rate program. The new definition should specify that the term encompasses advanced or next generation services consistent with the concepts described by these comments. The Bureau should also periodically review the new, expanded definition of advanced firewall and network security tools to ensure that it reflects technological changes, and other improvements to firewalls over time.

Modernizing E-rate to support advanced or next generation firewalls and related features aligns with the Communications Act and satisfies the Federal Communications Commission's ("Commission") requirements and balancing test for determining whether to include services on the E-rate Eligible Services List. This needed program update serves a vital educational purpose, and will help to ensure continuous, uninterrupted broadband connectivity. The benefits this improvement will deliver to schools and libraries far outweigh the limited related costs and can be accomplished well within the program's aggregate cap which has vastly exceeded applicant demand since at least 2019.

Table of Contents

COMMENTS RESPONDING TO THE WIRELINE BUREAU'S PUBLIC NOTICE REGARDING ALLOWING THE USE OF E-RATE FUNDS FOR ADVANCED OR NEXT-GENERATION FIREWALLS AND OTHER NETWORK SECURITY SERVICES

The Consortium for School Networking (CoSN), the State Educational Technology Directors Association (SETDA), the Council of Chief State School Officers (CGCS), the Council of the Great City Schools (CGCS), the Schools, Health & Libraries Broadband (SHLB) Coalition, the State E-rate Coordinators' Alliance (SECA), the National Association of State Boards of Education (NASBE), the National School Boards Association (NSBA), All4Ed, the Center for Democracy and Technology (CDT), and the Benton Institute For Broadband & Society submit these comments responding to the Wireline Competition Bureau's ("Bureau") request for public input regarding the use of E-rate program funds to enable schools and libraries to acquire certain limited cybersecurity.[1] Our organizations represent and support school, school district, state education agency, library, and other anchor institution leaders with responsibility for delivering secure broadband access to schools and libraries. The E-rate program is the only federal program that provides ongoing technology support for schools and libraries. Cybersecurity is integral to the school and library connectivity that the E-rate program facilitates. Thus, we respectfully urge the Bureau to: (1) make advanced or next generation firewalls and related features eligible for E-rate Category 2 support beginning in 2024; (2) increase Category 2 funding levels, within the E-rate program's existing aggregate cap, to cover modern firewalls; and (3) provide this limited E-rate cybersecurity support in a manner that is minimally burdensome to applicants and permits schools and libraries to select the modern firewall technology most aligned to their needs.

[1] Public Notice, 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 (DA 22-1315, released December 14, 2022).

Expanding E-rate to support advanced or next generation firewalls and related features is consistent with the Communications Act and satisfies the FCC's requirements and balancing test for determining whether to include services on the E-rate Eligible Services List. As demonstrated below, such a program update is not only needed to help protect our most vulnerable institutions, but it also serves a vital educational purpose, and ensures continuous, uninterrupted student and library patron connectivity. The cybersecurity benefits it would extend to schools and libraries far outweigh the limited related costs.

Like access to high capacity broadband and connected devices, access to best in class cybersecurity is often uneven and can differ substantially among schools and libraries. Some cybersecurity experts have described this disparity as the "cybersecurity poverty line".[2] On one side of the cybersecurity poverty line are organizations with "a mature security posture". These organizations have the personnel and financial resources that enable them to protect mission critical networks and sensitive personal data. On the line's other side are organizations, including many schools and libraries (especially those serving the nation's lowest wealth communities), that lack the infrastructure, technical resources, expertise, and policy influence to defend their telecommunications and information systems and sensitive personal and other data.[3] While all schools and libraries face this threat, 52.2% of American public school students are eligible for federal free or reduced price lunch, a key federal measure of student poverty, which means tens of millions of learners are at unnecessarily high risk to harmful cyberattacks.[4]

---

[2] Security Intelligence, *Chasing the Cyber 1%: How to Beat the Cybersecurity Poverty Line, (2022)* https://securityintelligence.com/articles/rise-above-cybersecurity-poverty-line/.
[3] "Buying down Risk: Cyber Poverty Line." Atlantic Council. May 3, 2022. https://www.atlanticcouncil.org/content-series/buying-down-risk/cyber-poverty-line/.
[4] U.S. Department of Education, National Center for Education Statistics, Common Core of Data (CCD), "Public Elementary/Secondary School Universe Survey," 2000-01, 2010-11, 2017-

Cyberattacks impose substantial costs on communities and institutions and severely harm individuals, including through lost instructional time, identity theft (students, library patrons, and school and library employees), loss of community trust, increased administrative burdens for state and local government, and the theft and waste of scarce public resources.[5] When evaluating a proposed modernization of the E-rate program to include updated cybersecurity, the Bureau must consider these and other community and individual costs as part of its cost effectiveness analysis. Failing to properly account for the costs associated with *inaction*, will compromise the validity of the Bureau's cost benefit analysis.

Absent proper cybersecurity, online learning, sensitive education records, and employee data are at risk. Effective data use is essential to schools' instructional and administrative decisions, including current national efforts to promote learning recovery following school closures and disruptions caused by the COVID-19 pandemic.[6] Data breaches caused by cyberattacks not only fundamentally disrupt learning when they happen, they also create long term negative consequences for education by damaging community trust in education data collection and use. Attacks also harm teachers and other school personnel. Within the past few weeks, San Benito Consolidated Independent School District (TX) shared details of a cyberattack in which Social Security numbers and bank account information were stolen from

---

18, 2018-19, and 2019-20. (This table was prepared November 2021) https://nces.ed.gov/programs/digest/d21/tables/dt21_204.10.asp.

[5] Government Accountability Office, "As Cyberattacks Increase on K-12 Schools, Here Is What's Being Done." (2022) https://www.gao.gov/blog/cyberattacks-increase-k-12-schools-here-whats-being-done#:~:text=The%20financial%20impacts%20on%20schools,cybersecurity%20to%20prevent%20future%20attacks.

[6] Data Quality Campaign, *September Assessment Update: Using Data to Support Students During COVID-19 Recovery,* https://dataqualitycampaign.org/data-to-support-students-during-covid-19-recovery/.

staff. [7] Furthermore, schools are often forced to not only stop digital learning, but they are also frequently forced to cease all instruction as demonstrated by the recent multiday closures of the Albuquerque School District, (NM),[8] the Des Moines Public Schools (IA), and schools in Jackson County and Hillsdale County (MI).[9] Recently, ransomware attacks closed schools in Nantucket, Massachusetts[10] and Tucson, Arizona.[11]

Studying the national K-12 cybersecurity challenge at Congress's direction, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) wrote in January 2023, that "[c]ybersecurity risk management must be elevated as a top priority for administrators, superintendents, and other leaders at every K–12 institution."[12] Schools have long recognized the need to prioritize this work, but they need assistance to secure their broadband networks including the connections subsidized by E-rate. For example, CoSN's 2022

---

[7] San Benito Consolidated School District, *Notice of Data Security Incident,* https://www.sbcisd.net/apps/pages/index.jsp?uREC_ID=3521596&type=d&pREC_ID=2396486.
[8] https://www.usnews.com/news/best-states/new-mexico/articles/2022-01-18/albuquerque-schools-confirm-ransomware-attack-resume-class.
[9] USA Today, *Ransomware Attack Closes Schools in Two Michigan Counties For Third Consecutive Day, https://www.usatoday.com/story/news/education/2022/11/16/michigan-ransomware-attack-schools-closed/10710003002/;* Des Moines Register, *What To Know About The Des Moines Public Schools Cyberattack and How It Affects Classes,* https://www.desmoinesregister.com/story/news/education/2023/01/11/des-moines-public-schools-dmps-cyberattack-class-cancelations-calendar-school-year/69796855007/.
[10] CNN Politics, *Ransomware attack closes schools in Nantucket,* https://www.cnn.com/2023/01/31/politics/ransomware-attack-schools-nantucket/index.html.
[11] Arizona Republic, *Cyberattack Impairs Systems at Tucson Unified District,* https://www.azcentral.com/story/news/local/arizona/2023/01/31/cyberattack-impairs-systems-at-tucson-unified/69859608007/.
[12] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, *Protecting or Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats,* p.3, (January 2023) (emphasis in original).

State of Ed Tech Leadership Survey found that only 15% of school districts felt "very" or "extremely" prepared to address their cybersecurity needs.[13]

While cyberattacks on school systems sometimes receive more publicity, public libraries are also frequent cyberattack targets. Libraries are sometimes forced to suspend digital and in-person services, including cancelling important education and workforce programs, until problems created by cyberattacks can be remediated.[14] Cyberattacks cause other library disruptions as well. For instance, the Mexico-Audrain Library in Missouri suffered a ransomware attack in January 2023 that affected its circulation system and e-service module.[15] The Rochester Library in Minnesota suffered a cyber-attack in December 2022 in which cyber-criminals allegedly stole e-mail addresses and names of library patrons.[16]

This proceeding offers the Bureau an opportunity to cost effectively begin addressing this systemic problem for schools and libraries by modernizing, consistent with the breathtaking technological changes and the field's needs since the program's inception in 1996, the E-rate program's firewall definition and making related changes to the Eligible Services List.

THE BUREAU SHOULD ADOPT A SINGLE, UPDATED FIREWALL DEFINITION THAT INCLUDES ADVANCED OR NEXT GENERATION FIREWALLS AND APPLY IT WITH FIDELITY TO THE ANNUAL ELGIBLE SERVICES LIST.

---

[13] CoSN *State of Ed Tech Leadership Survey* (2022) available online at https://www.cosn.org/edtech-topics/state-of-edtech-leadership/.

[14] Government Technology, *Cyber Attack Disrupts Local Library Service in Washington*, (June 2022), https://www.govtech.com/security/cyber-attack-disrupts-local-library-service-in-washington.

[15] KXEO, *Mexico-Audrain County Library District Resumes Some Services Following Ransomware Attack,* https://kxeo.com/2023/01/25/mexico-audrain-county-library-district-resumes-some-services-following-ransomware-attack/.

[16] KTTC, *Data breach at Rochester Public Library,* https://www.kttc.com/2022/12/16/data-breach-rochester-public-library/.

The E-Rate's definition of "Firewall or Firewall Service", which the program describes as "a hardware and software combination that sits at the boundary between an organization's network and the outside world and protects the network against unauthorized access or intrusions," is accurate but must be modernized to encompass advanced or next generation firewalls. Modern firewalls and other cybersecurity facilitate and are integral to the reliable delivery and use of broadband for "educational purposes" as described by the Commission's E-rate regulations.[17] Notably, advanced firewalls are often part of or integrated into the network services purchased by E-rate participants today; thus, rendering the program's outdated definition under the E-rate program confusing, unreliable, and unworkable for applicants.

Firewalls have been part of the E-rate program's Eligible Services List since the list's inception, but the Bureau must now improve and remove any ambiguity associated with the program's firewall definitions. The program's general Firewall or Firewall Service definition has been mooted because the Bureau carves-out, each year, a separate concept of "Basic Firewall" within the E-rate program's annual Eligible Services List.[18] The Bureau compounds confusion over the program's general Firewall or Firewall Service definition by not describing what it means by "Basic". The ambiguity of the term "Basic" has created unnecessary complexity and burden for E-rate applicants who must make an educated guess about what "Basic" means to the Bureau based on the Universal Service Administrative Company's ("USAC") approval or rejection of past applications. However, even more detrimental for schools and libraries, the

[17] 47 CFR §54.504

[18] *See e.g.* Modernizing the E-Rate Program for Schools and Libraries*,* (DA 22-1313, released December 22, 2022) (WCB) (Funding Year 2023 Eligible Services List). https://docs.fcc.gov/public/attachments/DA-22-1313A1.pd, .

Bureau's definition has locked-in a technologically limited and antiquated concept of Firewall or Firewall Service into the program.

SETDA – composed of state education agency experts with responsibility for applying for E-rate support – provides the following input that might help the Bureau modernize and properly expand the program's Firewall or Firewall Service definition. Like the E-rate program's Firewall or Firewall Service definition, SETDA says firewalls are designed to ensure continued network operation by preventing unauthorized access or intrusions. SETDA also notes, however, that advanced or next-generation firewalls provide a further layer of protection beyond traditional firewalls, citing capabilities such as application awareness and control, integrated intrusion prevention, comprehensive network visibility, and cloud-delivered threat intelligence.[19]

Our organizations encourage the Bureau to address the limitations inherent in the E-rate program's general Firewall or Firewall Service definition and in the separate references to Basic Firewalls in the Bureau's past Eligible Services List Orders. The Bureau should adopt and apply a single definition across E-rate to simplify and improve the program. The new definition should build on the program's existing "Firewall or Firewall Service" definition by specifying that the term encompasses advanced or next generation firewalls consistent with the concepts advanced by SETDA and other cybersecurity technology experts commenting in this proceeding. Finally, the Bureau should periodically review the new, expanded definition of advanced firewall and network security tools to ensure that it reflects technological changes, and other improvements to firewalls over time.

THE BUREAU SHOULD SUPPORT LOCAL DECISION MAKING BY PERMITTING SCHOOLS AND LIBRARIES TO ACQUIRE A RANGE OF ADVANCED OR NEXT-GENERATION FIREWALLS.

[19] SETDA, *Cybersecurity Policy Brief* (2022), Available in OER Commons *https://www.oercommons.org/courses/setda-cybersecurity-policy-brief-october-2022*.

E-rate applicants are best positioned to determine which firewall and cybersecurity services will best protect their school or library. This principle has been central to the E-rate since the First Report & Order (1997) when the Commission said, "...in an environment of rapidly changing and improving technologies, empowering schools and libraries, regardless of wealth and location, to choose the telecommunications services they will use as tools for educating their students will enable them to use and teach students to use state-of-the-art telecommunications technologies as those technologies become available."[20] Thus, we urge the Bureau to adopt an expansive, but technology neutral approach that describes a range of firewalls. CoSN and Funds for Learning wrote in their 2021 cybersecurity cost study previously submitted to the Commission that "common security features included with next-generation firewalls include:

- Intrusion Prevention System / Intrusion Detection System (IPS/IDS): detecting and stopping network activity which violates pre-defined security policies
- Virtual Private Network (VPN): creating secure channels for data transmission from inside private networks over public networks;
- Distributed Denial-of-Service protection (DDoS): protecting against attempts to overload a network with malicious traffic, which can halt its operation; and
- Network Access Control (NAC): preventing network disruptions by authenticating entrants based on risk profile profiles."[21]

[20] In the Matter of Federal-State Joint Board Universal Service, CC Docket No. 96-45, First Report & Order, 12 FCC Rcd. 8776, 9007, ¶ 433 (1997).
[21] CoSN, Funds for Learning, *E-rate Cybersecurity Cost Estimate* (2021), Available on the CoSN website https://www.cosn.org/tools-and-resources/resource/e-rate-cybersecurity-cost-estimate-january-2021/.

Similarly, SETDA suggests that the following advanced firewall services should be among the functions supported by the program: application awareness and control, integrated intrusion prevention, comprehensive network visibility, and cloud-delivered threat intelligence.[22]

Given the wide range of technologies applicants may reasonably elect to use to protect their networks and data, including technology that may be required by an applicant's cybersecurity insurance policies, the Bureau should not circumvent local control by attempting to pick and choose advanced or next generation firewall priorities.[23] Instead, we urge the Bureau to limit the program's overall cybersecurity investments by providing the newly expanded definition of firewalls and network security tools as eligible only through E-rate Category 2. With Category 2 funding capped by the Commission, taking this step will also control overall costs.

Using E-rate Category 2 is a proven strategy for reasonably limiting the program's Wi-Fi investments and it will appropriately limit the program's cybersecurity allocations. The Category 2 model will equip applicants with maximum local flexibility to decide if, and which, firewall investments are best for their schools and libraries. Our organizations do not recommend eliminating existing Category 1 support for firewall services provided at no additional cost as a standard component of a vendor's Internet access service.

THE BENEFITS OF MAKING ADVANCED OR NEXT GENERATION FIREWALLS ELIGIBLE FOR E-RATE SUPPORT FAR OUTWEIGH ASSOCIATED COSTS, AND THE E-RATE PROGRAM HAS PROVEN INTERNAL MECHANISMS FOR PROMOTING COST EFFECTIVENESS

[22] SETDA, *Cybersecurity Policy Brief* (2022), Available in OER Commons https://www.oercommons.org/courses/setda-cybersecurity-policy-brief-october-2022.
[23] See 2023 Eligible Service List comments filed by the Val Verde Unified School District.

Benjamin Franklin advised fire-threatened Philadelphians in 1736 that "An ounce of prevention is worth a pound of cure."[24] Like the threat of fire to 18th Century cities, the cybersecurity threat in 2023 has serious negative economic and social implications for many communities and individual students, teachers, library patrons, and other school and library personnel. The Government Accountability Office reported in October 2022 that attacks on K-12 schools caused learning losses associated with downtime and recovery affecting over two million students.[25] When weighing whether investments in next generation or advanced firewalls should be allowed from a cost effectiveness perspective, the Bureau must consider the significant costs that will be imposed on schools, libraries, and individuals, especially those in the nation's lowest-wealth communities, if advanced or next generation firewall services are not covered by E-rate. For example, the Buffalo Public Schools reported recovery costs of around $10 million in 2021[26] and Baltimore County Public Schools reported recovery costs of around $9.7 million after its November 2020 attack.[27] Not all cyberattack recoveries are this expensive, but these examples demonstrate just how harmful attacks can be for school districts and the communities they serve.

The E-rate program promotes cost effectiveness by aligning the amount of internet and internal connections assistance it provides based on poverty levels and cost measures while also

---

[24] Founders Online, *On Protection of Towns from Fire, 4 February 1735*, https://founders.archives.gov/documents/Franklin/01-02-02-0002.

[25] Government Accountability Office, *Critical Infrastructure Protection: Additional Federal Coordination is Needed to Enhance K-12 Cybersecurity*, (October 2022).

[26] Buffalo News, *Buffalo Schools Didn't Pay Rason in Cyberattack, but Response Cost Nearly $10 million*, https://buffalonews.com/news/local/education/buffalo-public-schools-didnt-pay-ransom-in-cyberattack-but-response-cost-nearly-10m/article_f0265112-2de2-11ec-bfa9-cf4404e9f9b5.html.

[27] Washington Post, *A 2020 ransomware attack is still harming Baltimore teachers,* https://www.washingtonpost.com/politics/2022/04/18/2020-ransomware-attack-is-still-harming-baltimore-teachers/.

requiring a meaningful local contribution.[28] For example, even the most low-wealth and geographically isolated applicants must contribute at least 15% of project costs and the very nature of Category 2 support necessarily requires a large applicant contribution. Requiring applicants, including applicants eligible for the largest subsidies, to make a significant financial commitment helps to ensure that E-rate supported projects are efficiently designed to meet local needs and are not inflated. This pre-established mechanism would similarly constrain applicants requesting assistance for acquiring advanced or next-generation firewalls.

E-rate applicants must also satisfy other meaningful financial, fiduciary, and ethical obligations that promote cost effectiveness. For example, applicants must comply with state and local procurement requirements that direct them to acquire the highest quality E-rate supported services at the lowest possible prices. Furthermore, applicants' annual technology and broadband budgets are limited, and their connectivity requirements are often significant and costly to address which discourages waste. Applicants must also comply with the E-rate program's competitive bidding rules which apply market pressures that push down costs. Specifically, the Commission's regulations say that "[a]ll entities participating in the schools and libraries universal service support program must conduct a fair and open competitive bidding process…"[29] With these safeguards in place, schools and libraries will purchase advanced or next generation firewalls at the most cost-effective price consistent with their local broadband connectivity and cybersecurity needs.

THE E-RATE PROGRAM'S CAP IS SUFFICIENTLY HIGH ENOUGH TO PERMIT A MODEST INCREASE TO CATEGORY 2 FOR THE PURPOSE OF FUNDING ADVANCED OR NEXT-GENERATION FIREWALLS AND SERVICES

[28] 47 CFR § 54.505
[29] 47 CFR § 54.503

The Bureau's Public Notice points out that the E-rate program has limited funds, but we remind the Bureau that over $2 billion of E-rate authorized funds were left undisbursed to schools and libraries for each of the program years 2019, 2020, and 2021.[30] Similarly, the Bureau estimated that in 2022 total application demand was $3.153 billion which was approximately $1.3 billion below the 2022 funding cap of $4.456 billion. In aggregate for the past four years, over $7 billion of E-rate funds could have been made available for advanced or next-generation firewalls.

E-RATE DISBURSEMENTS AND APPROXIMATE UNUSED PROGRAM FUNDING

E-rate Funding Year	Annual Inflation Adjusted E-rate Cap	USAC Disbursed E-rate Funds	Approximate Unused E-rate Funding
2022	$4.45 billion	$3.15 billion (FCC demand estimate)[31]	$1.3 billion
2021	$4.27 billion	$2.15 billion	$2.12 billion
2020	$4.23 billion	$2.09 billion	$2.13 billion
2019	$4.15 billion	$1.98 billion	$2.16 billion
Estimated Total Unused E-rate Funds 2019-22			$7.71 billion

The Bureau should not allow E-rate funds to continue going unused when schools and libraries desperately need assistance to acquire advanced and next generation firewalls to protect the

[30] Universal Service Administrative Company Annual Reports for 2019, 2020, and 2021. https://www.usac.org/about/reports-orders/annual-report/ The funding estimate for 2022 is drawn from the Wireline Bureau's E-rate demand estimate released on August 30, 2022.

[31] *Wireline Competition Bureau Directs USAC to Fully Fund Eligible Category One and Category Two E-Rate Requests,* (DA 22-902, released August 30, 2022) (WCB) https://www.fcc.gov/document/wcb-directs-usac-fully-fund-eligible-c1-and-c2-e-rate-requests-2.

integrity of their broadband connections, networks, and data. To accommodate that increased need, the Commission should raise Category 2's pre-discount budget accordingly. Funding schools' and libraries' modern firewall needs can easily be accomplished by the Bureau under Category 2 without raising the program's inflation-adjusted total cap.

THE COMMISSION HAS THE LEGAL AUTHORITY TO ADD ADVANCED OR NEXT-GENERATION FIREWALLS AND SERVICES AS AN ELIGIBLE SERVICE FOR THE E-RATE PROGRAM

We agree with the February 2021 Petition for Rulemaking filed by CoSN and its partners that the Commission has the legal authority to add advanced or next generation firewalls and services as an eligible service for the E-rate program.[32] Sections 254(c)(1), (c)(3), (h)(1)(B), and (h)(2) of the Communications Act grant the Commission authority to specify the services that will be supported for eligible schools and libraries and to design the specific mechanisms for support.[33] As the Commission noted in past Orders, "[t]his authority reflects Congress's recognition that technology needs are constantly 'evolving' in light of 'advances in telecommunications and information technologies and services."[34] The related statutory language reads, "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."[35] The Communications Act also states, "In addition to the services included in the definition of universal service under paragraph (1), the Commission may designate additional services for such support mechanisms for schools,

[32] Petition of CoSN et al. for Declaratory Relief and Petition for Rulemaking Allowing Additional Use Of E-Rate Funds for K-12 Cybersecurity, WC Docket No. 13-184, at 2 (filed Feb. 8, 2021), https://www.fcc.gov/ecfs/filing/102081871205710 (CoSN Petition).
[33] 47 U.S.C. §§ 254(c)(1), (c)(3), (h)(1)(B), (h)(2).
[34] *July 2014 Modernization Order*, para.67.
[35] 47 U.S.C. §254(c)(1)

libraries, and health care providers for the purposes of subsection (h)."[36] The authority described above includes addressing non-telecommunications services such as advanced and next generation firewalls that "enhance access" to advanced telecommunications and information services schools and libraries. "Advanced firewalls are needed to deliver broadband to students" and "are essential to education, public health, or public safety."[37]

THE COMMISSION SHOULD COORDINATE WITH THE U.S. DEPARTMENTS OF EDUCATION AND HOMELAND SECURITY

As the Commission implements expanded E-rate support for advanced or next generation firewalls, we also encourage the agency to collaborate with other federal stakeholders in K-12 cybersecurity, particularly the U.S. Department of Education (USED) and the Cybersecurity and Infrastructure Security Agency (CISA) within the U.S. Department of Homeland Security (DHS). USED and CISA are both charged with responsibility to coordinate cybersecurity in the education sector,[38] which DHS has long considered critical infrastructure.[39] The Government Accountability Office recently said that the failure to coordinate between USED and CISA has hampered K-12 cybersecurity,[40] and CISA stated that it intends to pursue coordination with USED in its recent K-12 cybersecurity report.[41] Because robust technical measures like those the

[36] 47 U.S.C. §254(c)(3)
[37] 47 U.S.C. § 254(c)(1)(A)
[38] U.S. Department of Homeland Security, Government Facilities Sector-Specific Plan ii (2015), available at https:// www.cisa.gov/publication/nipp-ssp-government-facilities-2015.
[39] U.S. Department of Homeland Security & U.S. Department of Education, Education Facilities Sector-Specific Plan (2010), available at https://www.dhs.gov/xlibrary/assets/nipp-ssp-education-facilities-2010.pdf.
[40] U.S. Government Accountability Office, Critical Infrastructure: Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity 19–24 (2022), available at https://www.gao.gov/products/gao-23-105480.
[41] Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, Protecting Our Future 2 (2023), https://www.cisa.gov/protecting-our-future-partnering-safeguard-k-12-organizations-cybersecurity-threats.

Commission has proposed to support through E-rate must be accompanied by administrative and personnel measures like robust data governance, cyber incident reporting, and training, we encourage the Commission to establish a formal working relationship with CISA and USED on K-12 cybersecurity.

CONCLUSION

Congress established the E-rate a quarter century ago because leaders recognized that without expanded universal service investments the emerging digital economy would leave many schools and libraries behind. Today, the same community anchor institutions that Congress helped in 1996 are once again on the wrong side of a national digital divide. This time, community anchors – namely our schools and libraries - are falling into a cybersecurity gap that threatens students' and library patrons' private data and prevents them from fully realizing the learning, workforce, and other benefits that broadband connectivity conveys.

Given this challenge, for the reasons described above, our school and library organizations encourage the Bureau to: (1) make advanced or next generation firewalls and related features eligible for E-rate Category 2 support beginning in 2024; (2) increase Category 2 funding levels, within the E-rate program's existing aggregate cap, to cover modern firewalls; and (3) provide this limited E-rate cybersecurity support in a manner that is minimally burdensome to applicants and permits schools and libraries to select the modern firewall technology most aligned to their needs.

Respectfully submitted by:

CONSORTIUM FOR SCHOOL NETWORKING
Keith Krueger, Chief Executive Officer
1325 G St. NW, Suite 420
Washington, D.C. 20005

STATE EDUCATIONAL TECHNOLOGY DIRECTORS ASSOCIATION
Julia Fallon, Executive Director
P.O. Box 10
Glen Burnie, MD 21060

COUNCIL OF CHIEF STATE SCHOOL OFFICERS
Carissa Moffat Miller, Executive Director
One Massachusetts Avenue, NW, Suite 800
Washington, D.C. 20001

SCHOOLS, HEALTH & LIBRARIES BROADBAND COALITION
John Windhausen, Jr., Executive Director
1250 Connecticut Ave NW, Suite 700
Washington, D.C. 20036

STATE E-RATE COORDINATORS' ALLIANCE
Debra M. Kriete, Chair
1300 Bent Creek Blvd, Suite 102
Mechanicsburg, PA 17050

NATIONAL SCHOOL BOARDS ASSOCIATION
John Heim, Executive Director, and Chief Executive Officer
1680 Duke St. FL2
Alexandria, VA 22314

ALL4ED
Rebeca Shackleford, Director of Federal Government Relations
1425 K Street, NW, Suite 700
Washington, D.C. 20005

COUNCIL OF THE GREAT CITY SCHOOLS
Dr. Raymond C. Hart, Executive Director
1331 Pennsylvania Ave, N.W., Suite 1100N
Washington, D.C. 20004

NATIONAL ASSOCIATION OF STATE BOARDS OF EDUCATION
Paolo DeMaria, President and CEO
123 North Pitt Street, Suite 350
Alexandria, VA 22314

BENTON INSTITUTE FOR BROADBAND & SOCIETY
Adrianne Furniss, Executive Director
1041 Ridge Rd, Unit 214
Wilmette, IL 60091

CENTER FOR DEMOCRACY AND TECHNOLOGY
Cody Venzke, Senior Counsel Equity in Civic Technology
1401 K Street NW, Suite 200
Washington, D.C. 20005

February 13, 2023