



November 23, 2022

SUBMITTED ELECTRONICALLY VIA ECFS

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
45 L Street NE
Washington, DC 20554

**Re: Ex Parte Submission
Modernizing the E-rate Program for Schools and Libraries; WC Docket No. 13-184**

Dear Ms. Dortch:

The Schools, Health & Libraries Broadband (SHLB) Coalition¹ calls upon the Federal Communications Commission (Commission) to clarify its definition of "firewall services and firewall components" eligible as Category 2 services and its definition of "basic firewall protection" eligible in Category 1 in the E-rate Eligible Services List (ESL) for Funding Year 2023. In particular, SHLB asks the Commission to clarify that Category 2 firewall services should include advanced or "next-generation" firewall services and components. SHLB also urges the Commission to develop long-term solutions to the growing cybersecurity crisis and open a rule-making proceeding to seek comment on the Petition previously filed by the Consortium for School Networking (CoSN), SHLB and other organizations in February 2021 (Petition).²

Cybersecurity is integral to the core services supported by E-rate. The Commission has done a fabulous job of modernizing the E-rate program over the years to adapt to the changing marketplace. Given the dramatic increase in cyberattacks on schools and libraries over the past

¹ The SHLB Coalition is a broad-based public interest coalition of organizations that share the goal of promoting open, affordable, high-quality broadband for anchor institutions and their communities. SHLB Coalition members include representatives of schools, libraries, health care providers and networks, state broadband offices, private sector companies, state and national research and education networks, and consumer advocates. See <http://shlb.org/about/coalition-members> for a list of SHLB Coalition members.

² Petition for Declaratory Relief and Petition for Rulemaking Allowing Additional Use of E-rate Funds for K-12 Cybersecurity, Consortium for School Networking, et. al, WC Docket No. 13-184 (Feb. 8, 2021) <https://www.fcc.gov/ecfs/document/102081871205710/1>.

few years, the Commission should now consider that protecting these networks from cyberattacks is part and parcel of its stewardship of the E-rate program. E-rate is intended to support broadband connectivity, and it is this very broadband connectivity that is increasingly at risk. In other words, cybersecurity is not a separate issue to be resolved by other government agencies; nor are firewalls separate from the networks they are designed to protect. Advanced firewalls are necessary features of effective, safe, usable communications.

Much attention has been paid to the ransomware cyberattack on the second largest school district in the United States, Los Angeles Unified School District (LAUSD) in September 2022. As part of the attack, stolen data was leaked onto a dark web leak site, prompting subsequent investigations into the extent and variety of information that was compromised.³ This attack led to an outpouring of support by school systems around the country for E-rate support. LAUSD was able to collect signatures on a [letter](#) from 1,100 districts across the nation urging the Commission to authorize the ongoing, permanent use of existing E-Rate Program funds to bolster and maintain IT security infrastructure.

But this example is unfortunately not unusual. Boston Public Library sustained a very serious cyberattack a year ago.⁴ The US Cybersecurity and Infrastructure Security Agency (CISA) issued a warning that a criminal enterprise was targeting school systems because of their vast troves of personal student data stored in their systems.⁵ It has become more apparent that schools, libraries, and other anchor institutions are particularly vulnerable to cyber-attacks.⁶ While there can be tremendous benefits for anchor institutions to digitize operations, embrace electronic and “smart” technologies, and upgrade IT systems, adoption of these technologies may open the door to unanticipated cybersecurity challenges and safety risks.

As part of a 2021 investigation to better understand ransomware attacks in the United States, the Senate Committee on Homeland Security and Governmental Affairs reported that, “[i]n recent years, ransomware attack victims have included hospitals, school systems, local, state, and federal government agencies, as well as other critical infrastructure, including the water and energy sectors. In 2021, ransomware attacks impacted at least 2,323 local governments, schools, and healthcare providers in the United States.”⁷ These reported numbers,

³ Carly Page, *Hackers Leak 500GB Trove of Data Stolen During LAUSD Ransomware Attack*, TECHCRUNCH (Oct. 3, 2022) <https://techcrunch.com/2022/10/03/los-angeles-school-district-ransomware-data/>.

⁴ <https://www.bostonglobe.com/2021/08/27/metro/bpl-hit-by-ransomware-attack-shutting-down-most-its-computer-network/>

⁵ <https://www.darkreading.com/attacks-breaches/la-unified-ransomware-cisa-warns-back-to-school-attacks>.

⁶ In its current annual study, Sophos reported an increase in the percentage of lower education organizations that were hit by ransomware in the last year (56%) compared to the findings from its 2021 survey (44% of education respondents). Its various findings “suggest that the education sector is poorly prepared to defend against a ransomware attack, and likely lacks the layered defenses needed to prevent encryption if an adversary does succeed in penetrating the organization.” Sophos, *The State of Ransomware in Education 2022*, 3 (Jul 2022) <https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-education>.

⁷ United States Senate Committee on Homeland Security and Governmental Affairs, *Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns*, 2, <https://www.hsgac.senate.gov/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report.pdf>.

however, may understate the exact magnitude of cyber issues facing these susceptible institutions. For example, there may be up to 10 or even 20 *times* more K-12 cyber incidents each year that remain undisclosed and not formally counted in reported statistics.⁸

The Commission recognized the importance of providing cybersecurity support to schools and libraries when firewalls were first included in the ESL as an eligible service under the E-rate program. Since this adoption, however, there have been dramatic changes to the technology landscape as cyber-related incidents grow more sophisticated. SHLB members have expressed a myriad of concerns, including that “basic” firewalls may not adequately protect our most vulnerable institutions against the types of recurring cyberattacks we see today. Additionally, the uncertainty regarding the scope of the Commission’s existing definition of “firewall services and firewall components” and “basic” firewalls in Category 1 and 2 in the ESL ultimately causes confusion or unworkable solutions for applicants, especially since standard network offerings in the current marketplace only include advanced components and services such as next-generation firewalls. Clarifying that these definitions include advanced firewall services and firewall components would eliminate the confusion over how to cost allocate certain services and ease the burden for both the applicant and USAC. Eliminating cost-allocation for next generation firewalls would significantly reduce the administrative burden on applicants and USAC, saving time and money

While SHLB recognizes that providing clarification of the firewall definitions in the ESL will not solve all the cybersecurity needs,⁹ we believe that it is a necessary and immediate step to address certain fundamental concerns within the current cybersecurity landscape. Modern 21st century society encourages our anchor institutions to embrace digital operations and business practices, but this means that we must also provide them with the resources they need to secure the networks and the data running over it. According to a 2022 Annual Report published by the K12 Security Information Exchange, for K-12 schools in particular “the absence of meaningful cybersecurity risk management standards for schools at either the state or federal levels—coupled with a lack of resources dedicated to meeting any such standards—all but guarantees that many districts will continue to place the safety and security of students, teachers, and community members at avoidable risk.”¹⁰

⁸ Douglas A. Levin, *The State of K-12 Cybersecurity: Year in Review – 2022 Annual Report*, K12 Security Information Exchange (K12 SIX), 2 (2022) <https://www.k12six.org/the-report> (“K12 SIX Annual Report”). Since 2016, there have been 1,331 cataloged disclosed cyber incidents affecting U.S. school districts, which averages over the last six years to more than one incident per school day. *Id.* at 3.

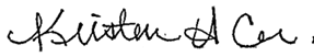
⁹ For example, companies who provide cybersecurity insurance may be demanding that their insureds carry more significant holistic network protection and prevention requirements. *See, e.g.* Comments of Val Verde Unified School District, WC Docket No. 13-184 (Sep. 21, 2022) <https://www.fcc.gov/ecfs/document/1092155232964/1>, *stating* that “[t]hose few companies who continue to offer cybersecurity insurance are increasing premiums to unprecedented levels and requiring reasonable, yet significant, protections. These requirements include not only standard network hardware such as next generation firewalls, but also include holistic protection and prevention including endpoint protection, infrastructure monitoring and prevention, penetration testing, multi-factor authentication (MFA) for all staff (including part-time and occasional substitute staffing), mandatory annual cybersecurity training and simulated phishing attacks.”

¹⁰ K12 SIX Annual Report at 4.

As reflected by the many comments submitted in the current record, including proposals from school districts,¹¹ the industry,¹² and other organizations (such as a recent proposal from Funds for Learning for a pilot program¹³), SHLB is not alone in asking the Commission to take strong and immediate action to better equip our schools and libraries against future cyberattacks.

SHLB thus urges the Commission to take immediate action now to clarify the definitions of firewall equipment and services in both Category 1 and 2 to include advanced features and functions for the next E-rate funding year. Furthermore, SHLB also urges the Commission to open a rule-making proceeding to seek comment on the aforementioned Petition and to develop long-term solutions to these issues as soon as possible.

Respectfully Submitted,



Kristen Corra
Policy Counsel
Schools, Health & Libraries Broadband (SHLB) Coalition
1250 Connecticut Ave. NW Suite 700
Washington, DC 20036
kcorra@shlb.org
571-306-3757

¹¹ See e.g. Comments of the Sacramento County Office of Education, WC Docket No. 13-184 (Nov. 14, 2022) <https://www.fcc.gov/ecfs/document/1114747822386/1>.

¹² See e.g. Ex Parte Filing of Fortinet, Inc., ENA by Zayo, Microsoft Corporation, Cisco Systems, Inc. and Hewlett Packard Enterprise, WC Docket No. 13-184 (Nov. 22, 2022).

¹³ Ex Parte Filing of Funds for Learning, WC Docket No. 13-184 (Nov. 15, 2022) <https://www.fcc.gov/ecfs/document/111630719929/1>.