December 8, 2022

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

Re: *Modernizing the E-rate Program for Schools and Libraries, WC Docket No. 13-184*
FY 2023 Draft Eligible Services List, DA 22-878, *Ex Parte Letter*

Dear Secretary Dortch:

The State E-rate Coordinators' Alliance (SECA) strongly supports broader and more comprehensive eligibility of firewall components and the elimination of the current cost allocation requirement for various network security features. SECA supports and appreciates the recent advocacy efforts of Funds for Learning, SHLB Coalition, CoSN and other stakeholders to seek action on this matter for the FY 2023 Eligible Services List.[1]

Based on an eight-year old definition of basic firewall protection that is now obsolete, certain inherent protective features of firewalls must be deducted from E-rate funding requests such as: intrusion protection and detection, malware protection, application control, content filters and DDoS mitigation.

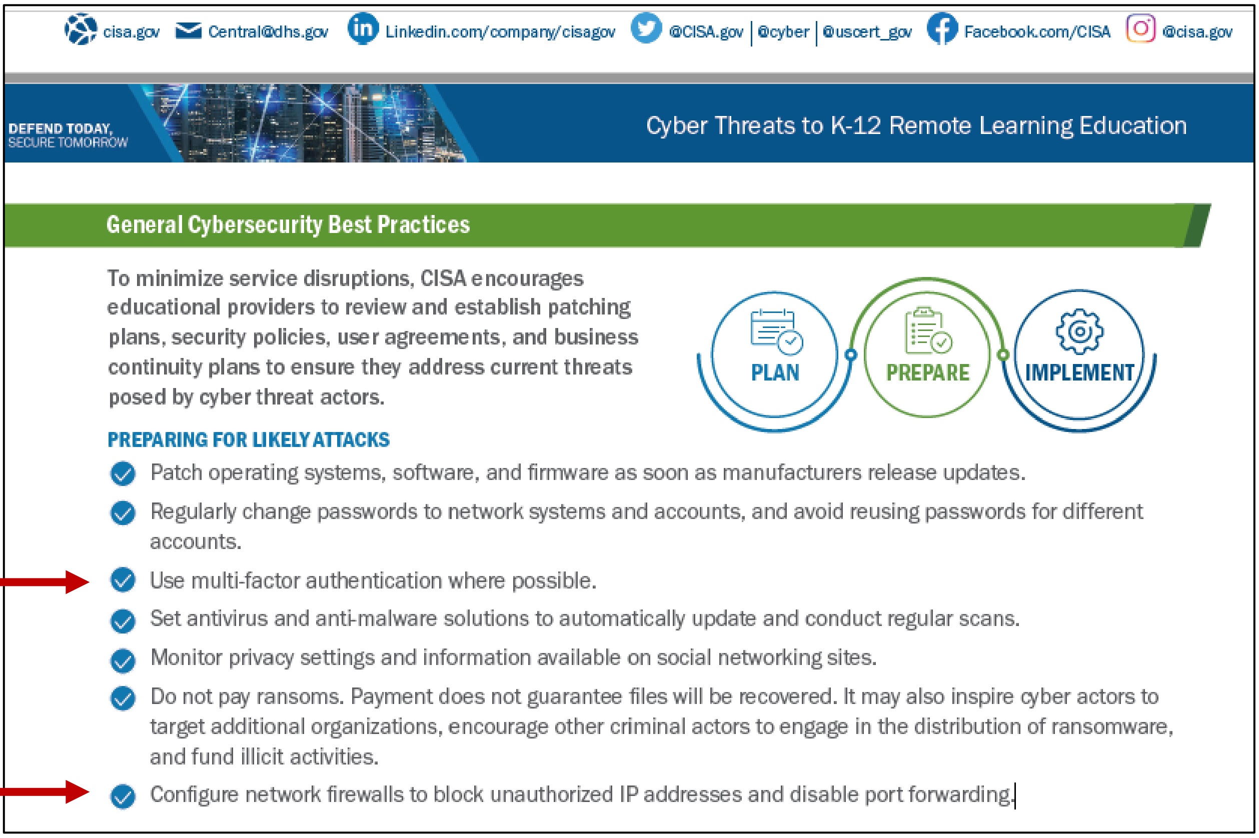
The basic firewall protection definition was created initially in the July 2014 First Modernization Order and then subsequently confirmed in the annual Eligible Services Lists.[2]

[1] Funds for Learning filing dated November 15, 2022 - https://www.fcc.gov/ecfs/document/111630719929/1; Consortium for School Networking Ex Parte Filing dated November 22, 2022 - https://www.fcc.gov/ecfs/document/1123278977697/1; Fortinet, Inc., Cisco Systems, Inc., ENA by Zayo, Hewlett Packard Enterprise, Microsoft Corporation Joint Ex Parte Filing dated November 22, 2022 - https://www.fcc.gov/ecfs/document/1122275903360/1; SHLB Coalition Ex Parte Filing dated November 23, 2022; Alabama Supercomputer Authority Ex Parte Filing dated November 22, 2022 - https://www.fcc.gov/ecfs/document/1125054671818/1; Cisco Systems, Inc. Ex Parte Filing dated November 22, 2022 - https://www.fcc.gov/ecfs/document/112507410880/1.

[2] The July 2014 First E-rate Modernization Report and Order declined to designate "further network security services" as eligible. These "further network security services" were explicitly identified in footnote 275 to include the prohibited features listed above in the first paragraph of this letter. Modernizing the E-rate Program for Schools and Libraries, *Report and Order and Further Notice of Proposed Rulemaking,* 29 FCC Rcd 8870 (11), paragraph 21, footnote 275.
This paragraph and footnote became the basis for requiring cost allocations of these feature sets when integrated into a firewall. The Order which released the FY 2016 Eligible Services List stated, "In light of previous Commission direction, we remind commenters that firewall services other than those offered as a standard part of eligible Internet access are eligible under Category Two, and we deny the requests to designate all firewall services as Category One and to add additional network security services to the ESL. Modernizing the E-rate Program for Schools and Libraries, DA 15-1012, *Order Adopting the FY 2016 Eligible Services List,* ¶ 18, footnote 50. This requirement has continued in effect since then to the present day.

The ineligible network security features may have been add-on protections back in the 2014-2015 time frame, but in the intervening eight years, there is no question that they are essential to ensure broadband services and equipment are protected from cyber-attacks and are integrated into firewalls.

In December 2020, the Cybersecurity and Infrastructure Security Agency (CISA) published an Advisory entitled "Cyber Threats to K-12 Remote Learning Education." This bulletin contains K-12 cybersecurity best practices that specifically reference two such protections available from firewalls that are not currently eligible for E-rate funding: malware and intrusion protection.[3]



Cyber Threats to K-12 Remote Learning Education

General Cybersecurity Best Practices

To minimize service disruptions, CISA encourages educational providers to review and establish patching plans, security policies, user agreements, and business continuity plans to ensure they address current threats posed by cyber threat actors.

PREPARING FOR LIKELY ATTACKS

- ✓ Patch operating systems, software, and firmware as soon as manufacturers release updates.
- ✓ Regularly change passwords to network systems and accounts, and avoid reusing passwords for different accounts.
- ✓ Use multi-factor authentication where possible.
- ✓ Set antivirus and anti-malware solutions to automatically update and conduct regular scans.
- ✓ Monitor privacy settings and information available on social networking sites.
- ✓ Do not pay ransoms. Payment does not guarantee files will be recovered. It may also inspire cyber actors to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and fund illicit activities.
- ✓ Configure network firewalls to block unauthorized IP addresses and disable port forwarding.

Currently when schools and libraries apply for Category 2 E-rate funding, they must deduct all the costs associated with these essential security services and pay for them out of pocket. These cost allocations are complex, increase uncertainty about available funding, and are antithetical to the goals of E rate to facilitate broadband availability to students and library patrons throughout the country.

[3] https://www.cisa.gov/sites/default/files/publications/Cyber_Threats_to_K-12_Remote_Learning_Fact_Sheet_15_Dec_508_0.pdf

The increasing number of school network attacks has created an urgency for FCC action. Network security is a matter of paramount importance. Consistent with our prior advocacy, SECA urges the FCC to remove the firewall cost allocation requirement for applicants' use of their Category 2 budgets.

By providing this relief, Applicants would have more flexibility to use E-rate funds for cybersecurity without imposing an additional financial burden on E-rate. SECA is **not** requesting that the Category 2 multipliers be increased to cover more of the cybersecurity costs. SECA also is **not** requesting that the overall E-rate funding cap be increased. Last, SECA's request focuses exclusively on Category 2 eligibility and does not touch Category 1 eligibility rules.

To address the myriad of additional issues concerning K-12 and library cybersecurity, SECA encourages the FCC to convene a NPRM to address the various issues raised in the Joint Petition for Rulemaking (in which SECA joined), that was submitted on February 8, 2021.[4] The NPRM would provide the means to comprehensively develop the record on how best to address the use of E-rate funds for other cybersecurity protections beyond allowing network security features to be funded as part of Category 2 firewall eligibility.

We hope the Commission will agree that the immediate removal of firewall cost allocations for network security features, as listed above, when Applicants apply for Category 2 funding, is a win-win for all stakeholders without imposing a financial burden on the E-rate program. We also respectfully request that a NPRM be issued to address E-rate eligibility of other cybersecurity equipment and services. Please contact me if you have any questions.

Respectfully submitted,

Debra M. Kriete

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

[4] https://www.fcc.gov/ecfs/search/search-filings/filing/102081871205710