February 13, 2023

Comments of the Cybersecurity Coalition and the Information Technology Industry Council
To the Federal Communications Commission, Wireline Competition Bureau

Re: 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

WC Docket No. 13-184

The Cybersecurity Coalition (the Coalition) and the Information Technology Industry Council (ITI) submit this comment in response to the Federal Communications Commission's (FCC) Wireline Competition Bureau's (WCB) request for comment on the use of E-Rate funding for advanced firewalls and other network security services.[1]

We join more than a thousand US school districts in calling on the FCC to authorize the permanent use of E-Rate program funds to bolster and maintain IT security Infrastructure.[2] The E-Rate program has evolved in many areas since its inception, but it has not kept pace with changes in the cybersecurity threat landscape. The Coalition and ITI strongly support expanding the permissible uses of E-Rate program funds to support advanced firewalls and other network security services to defend against cybersecurity attacks that increasingly disrupt education and connectivity in schools. We believe the FCC should ensure school districts are provided the flexibility to select a variety of solutions, including end point, network, cloud, and device security solutions, as they tailor their cybersecurity protections to meet their unique risk profiles. The Coalition and ITI appreciate the opportunity to provide these comments and engage in this important discussion.

The Coalition is composed of leading companies with a specialty in cybersecurity products and services dedicated to finding and advancing consensus policy solutions that promote the

[1] 88 Fed. Reg. 1035 (2023).
[2] School districts coalition letter on E-Rate to FCC, Local Educational Agencies and Organizations Across the Country Urge the FCC Authorize the Use of E-Rate Funds to Combat Cyber Security Threats at Public Schools, Sep. 21, 2022, https://alair.ala.org/bitstream/handle/11213/18887/School%20Districts%20Coalition%20Letter%20on%20E-Rate%20to%20FCC_Final%20%2009.21.22.pdf.

development and adoption of cybersecurity technologies.[3] We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management. We are supportive of efforts to identify and promote the adoption of cybersecurity best practices, information sharing, and voluntary standards throughout the global community.

ITI is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, and related industries. Cybersecurity and cybersecurity technology are critical to ITI members. Facilitating the protection of our customers (including governments, businesses, and consumers), securing, and protecting the privacy of individuals' data, and making our technology and innovations available to our customers to enable them to improve their operations are core drivers for our members.

E-Rate is a critical program for school and library cybersecurity.

The Coalition and ITI urge the FCC to protect its investment in school connectivity by ensuring that school networks are resilient against cyberattacks. Cybersecurity has become essential to the safety and reliability of the networks that keep schools and libraries connected, and lack of cybersecurity can hamper the adoption of digital learning tools.[4] Yet many K-12 schools cite lack sufficient funding and personnel for cybersecurity as top security concerns.[5] In calling for E-Rate fund access to cybersecurity services, school districts warned the FCC that they face "significant risk of disruption to instruction, home to school transportation, or access to nutritious meals that would be catastrophic for students and their learning."[6]

State and local officials also have reported that cybersecurity incidents resulted in significant loss of learning and connectivity in educational institutions, and incur considerable expenses, in the last three years.[7] Impacts from cyberattacks include disrupted access to networks and

[3] The views expressed in this comment reflect the consensus views of the Coalition and do not necessarily reflect the views of any individual Coalition member. For more information on the Coalition, see www.cybersecuritycoalition.org.
[4] Lily Hay Newman, Schools Already Struggled With Cybersecurity. Then Came Covid-19, Wired, Jul. 1, 2020, https://www.wired.com/story/schools-already-struggled-cybersecurity-then-came-covid-19.
[5] MS-ISAC and Center for Internet Security, K-12 Report, pg. 6, Nov. 2022, https://learn.cisecurity.org/k-12-report.
[6] School districts coalition letter on E-Rate to FCC, Local Educational Agencies and Organizations Across the Country Urge the FCC Authorize the Use of E-Rate Funds to Combat Cyber Security Threats at Public Schools, Sep. 21, 2022, https://alair.ala.org/bitstream/handle/11213/18887/School%20Districts%20Coalition%20Letter%20on%20E-Rate%20to%20FCC_Final%20%2009.21.22.pdf.
[7] Government Accountability Office, Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity, pg. 12, Oct. 2022, https://www.gao.gov/assets/gao-23-105480.pdf.

systems, loss of sensitive data, delayed exams, and canceled school days.[8] The estimated number of students affected yearly by ransomware alone are now in the hundreds of thousands - exponentially larger than the number of students affected before 2018.[9] The education sector continues to be a lucrative target for cybercriminals, and we anticipate continued threats as schools increasingly leverage digital learning tools.[10]

The Coalition and ITI recognize school connectivity as a major priority, but connected schools must rely on security resiliency to stay connected. Cybersecurity is already an established part of the E-Rate program, and E-Rate is the only federal program dedicated to broadband connectivity for K-12 schools with a cybersecurity element. For example, other school connectivity programs like the Emergency Connectivity Fund expressly exclude cybersecurity.[11] The Elementary and Secondary School Emergency Relief Fund resources are broadly used for non-cybersecurity purposes, such as teacher salaries, school operations, and cleaning and sanitizing materials.[12] The State and Local Cybersecurity Grant Program is also open to non-educational state and territory agencies, subject to the state Cybersecurity Plan.[13] Simply put: E-Rate's cybersecurity options help address an important gap in school and library funding support.

The FCC has an important role to play in administering E-Rate support for cybersecurity services related to school and library connectivity. The FCC has long regulated cybersecurity of telecommunications supply chains, customer proprietary network information, the emergency alert system, among many other areas.[14] The FCC's work puts network security front and center, and we encourage the FCC to avoid the appearance of deferring this responsibility to other agencies in the context of E-Rate.

Separately from the E-Rate program, the Commission should continue working with its federal partners to explore holistic approaches to address and prevent cyberattacks against K-12 schools and libraries. This should include training, implementing cybersecurity frameworks and programs for schools and libraries, and incident response support. However, this assistance

[8] Cybersecurity and Infrastructure Security Agency, Alert AA22-249A, #StopRansomware: Vice Society, Sep. 8, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-249a.
[9] Government Accountability Office, Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity, pg. 15, Oct. 2022, https://www.gao.gov/assets/gao-23-105480.pdf.
[10] See K-12 Security Information Exchange, K-12 Cyber Incident Map, https://www.k12six.org/map (last accessed Jan. 9, 2023).
[11] Federal Communications Commission, Eligible Services List for Emergency Connectivity Fund Program, FCC 21-58, pg. 2, https://www.fcc.gov/sites/default/files/ecf_esl.pdf (last visited Jan. 9, 2023).
[12] U.S. Department of Education, Office of Elementary and Secondary Education, Frequently Asked Questions about the Elementary and Secondary School Emergency Relief Fund, pg. 4, https://oese.ed.gov/files/2020/05/ESSER-Fund-Frequently-Asked-Questions.pdf (last visited Jan. 9, 2023).
[13] Cybersecurity and Infrastructure Security Agency, State and Local Cybersecurity Grant Program, Frequently Asked Questions, pg. 1, https://www.cisa.gov/sites/default/files/publications/SLCGP_FAQ-FINAL_508c.pdf (last visited Jan. 9 2023).
[14] Federal Communications Commission, Rosenworcel Statement: FCC Acts to Strengthen the Security of Nation's Alerting Systems, pg.1, Oct. 27, 2022, https://www.fcc.gov/document/fcc-acts-strengthen-security-nations-alerting-systems/rosenworcel-statement.

does not replace the need for funds to install and operate technologies and services to secure school and library networks, which E-Rate should help provide.

E-Rate would be served best by expanding the program to include a range of security services, not just firewalls.

E-Rate support for modern cybersecurity technologies and services can make an important impact in avoiding disruption to school and library networks. There is no one-size-fits all approach to security, and an effective cybersecurity program should be tailored to mitigate an organization's risks. The FBI, CISA, and MS-ISAC recommend that educational institutions apply mitigations to prevent, detect, and recover from cybersecurity incidents.[15] However, these key mitigations are not presently E-Rate eligible services. Currently, the only security option listed on the E-Rate eligible services list (ESL) are firewall services and firewall components.[16] Although firewalls are a good first step, firewalls alone are not enough to protect against today's cyber threats, in part because of the increasingly porous perimeter of internal networks.

Cybersecurity solutions must address today's modern perimeter-less environment, which includes protecting people, devices, applications and data wherever they are located. One approach often advanced to addressing this environment is a Zero Trust approach. Zero Trust is an asset-level security approach that assumes that all network traffic is potentially untrusted and should be verified before being allowed access to resources. This approach involves solutions that:

- Authenticates and authorizes based on available data points including user identity, location, device health, data classification, and anomalies.
- Uses least privilege access, limiting user access with just in time and just enough access.
- Minimizes the potential damage of breaches, verifies appropriate encryption, and uses analytics to drive threat detection and improve defenses.

Given the range of cyber threats that can disrupt connectivity, schools and libraries should have the flexibility to choose those security products that are most suitable to their cybersecurity risk profile. This should include network, cloud, end point, and device security solutions designed to prevent, detect, and respond to external and internal threats. For example, schools and libraries should be able to apply E-Rate funds to:

[15] See CISA, Protecting Our Future: Partnering To Safeguard K-12 Organizations, pg. 13, Jan. 2023, https://www.cisa.gov/sites/default/files/publications/K-12report-24Jan23.pdf. See also, CISA, Alert AA22-249A, #StopRansomware: Vice Society, Sep. 8, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-249a.
[16] Federal Communications Commission, Wireline Competition Bureau, Modernizing the E-Rate Program for Schools and Libraries, Order, DA-22-1313, pg. 8, Dec. 14, 2022, https://www.fcc.gov/document/wcb-adopts-final-eligible-services-list-funding-year-2023.

- Incident detection and response tools and services, including tools and services that monitor data from endpoint devices that could indicate a threat. This is particularly important for early prevention of ransomware.
- Vulnerability management, penetration testing, or bug bounty solutions and services, to help schools proactively identify and prioritize the remediation of vulnerabilities that could enable an attacker to compromise a network.
- User identity and access management tools and services, including multi-factor authentication. These tools and services help prevent unauthorized users from gaining network access, detect anomalous user behavior indicating a threat, and prevent hijacked user accounts from causing broader network damage.
- Managed solutions or cybersecurity as a service, to enable schools to scale their cybersecurity programs to fit their size and budget without needing significant technical expertise to implement cybersecurity solutions in-house.
- And other services and solutions, depending on the organization's risks and security posture. The FCC should re-evaluate its product list on a periodic basis to ensure it keeps pace with the needs of schools and libraries to defend against significant current risks.

School districts are more vulnerable to cyberattacks that disrupt education and connectivity if they do not have the resources to implement defenses that are proportionate to the threats. Expanding E-Rate eligible services to include modern cybersecurity solutions and services is a prudent use of E-Rate funds that will help protect the investment that federal, state, and local governments have made in connectivity for education.

The Commission should clarify the term "firewall" to include advanced or next-gen features.

Regardless of the extent to which E-Rate is expanded to encompass additional security services, it is critical that the FCC preserve firewall components and services as eligible for E-Rate, and that FCC ensures this includes "advanced" or "next-generation" firewalls. The Coalition and ITI believe Category Two services should encompass advanced firewall services and components, including virtual or cloud-based functionalities, that are separate from firewall protection provided as a standard part of a vendor's Internet access service.[17] Category One services should encompass advanced firewall services and components, as well as other cybersecurity solutions, that are offered as part of a vendor's Internet access service.

The commonly accepted definition of firewall in the E-Rate program is "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."[18] The FCC

[17] Federal Communications Commission, Wireline Competition Bureau, Modernizing the E-Rate Program for Schools and Libraries, Order, DA-22-1313, pg. 8, Dec. 14, 2022, https://www.fcc.gov/document/wcb-adopts-final-eligible-services-list-funding-year-2023.
[18] USAC, Schools and Libraries (E-Rate) Program Eligible Services List (ESL) Glossary, at

should exercise its interpretive authority[19] to clarify that this definition is interpreted to include security features that are associated with advanced or next-gen firewalls.

In this context, the key difference between basic and advanced firewalls is the greater breadth of security features supported by advanced firewalls, which provides greater resiliency against disruptive attacks.[20] This may include intrusion prevention and detection, virtual private networks, network access controls, malware detection and filtering, application security control, anti-spam support, and SSL inspection. These advanced features should be construed to fit within the existing firewall definition as "protecting networks against unauthorized access or intrusions." No modification to the existing definition needs to be made to establish this interpretation.

An additional clarification to this definition should be considered to more fully include advanced firewalls. Advanced or next-gen firewalls and services may have different hardware deployments than basic firewalls. The hardware for Firewall-as-a-Service (FWaaS) includes cloud infrastructure, such as cloud servers, that may share functionality with other applications. FWaaS performs URL filtering, intrusion prevention, and other firewall functions from the cloud rather than from an on-premises hardware device.[21] FWaaS can be easier to scale and adapt to changing network and security demands than traditional firewalls, and may be a prudent security option for some educational and library institutions. Accordingly, we recommend the FCC clarify that a firewall is a hardware and software combination, but that the hardware element includes cloud infrastructure and need not be an on-premises device dedicated to performing firewall functions.

Preserve flexibility and existing E-Rate policies for cost-effective purchases.

The Coalition and ITI believe it would be most cost-effective to enable E-Rate funds to be used for modern cybersecurity equipment and services, so schools and libraries would have the flexibility to meet their evolving cybersecurity needs. The Coalition and ITI encourage the Commission against limiting E-Rate funds to specific cybersecurity equipment or services, such as FWaaS, to ensure schools and libraries have the ability to choose which tools and services best match their cybersecurity needs and risk profile.

Including cybersecurity in E-Rate will not divert resources from its primary focus of connecting schools and libraries. Schools should continue to manage their own budgets and choose the E-Rate eligible services that are right for them, subject to E-Rate's competitive bidding and funding cap processes.

---

https://www.usac.org/wp-content/uploads/e-rate/documents/ESL-Glossary.pdf (last visited Jan. 5, 2023).

[19] See 47 CFR 0.91, 0.291.

[20] Gartner, Information Technology Glossary, Next Generation Firewalls, https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws (last visited Jan. 9, 2023)

[21] Chad Kime, What is Firewall-as-a-Service (FWaaS)?, Datamation, Oct. 11, 2022, https://www.datamation.com/security/firewall-as-a-service.

The Commission has authority to update the Eligible services list.

The Coalition and ITI agree that the WCB has authority to update the list of technologies and services eligible for E-Rate. The Commission granted the WCB authority to interpret the rules "as necessary to ensure that support for services provided to schools and libraries… operate to further our universal service goals."[22] This includes adding advanced or next-gen firewalls and services, as well as more modern cybersecurity equipment and services, as eligible services for the E-Rate program to prevent disruptions in school and library connectivity. As the Coalition and ITI have noted above, however, the Commission does not need to modify the definition of firewall in order to clarify that advanced or next-gen firewalls and services are included as eligible firewalls under the current ESL.

However, the Commission should not stop there. It should amend its rules to give schools the flexibility to use E-Rate funding to help purchase the cybersecurity products and services they need. The WCB has repeatedly clarified the eligible services in the past,[23] in recognition of the "evolving" concept of universal service.[24] The Coalition and ITI urge the WCB to do so in the area of cybersecurity, in recognition that universal service and affordable connectivity for schools and libraries now depend on resiliency against unauthorized intrusion and disruption.

* * *

The Coalition and ITI hope that our input will be helpful to the WCB as it considers the proposed rule. Should you have any questions, or if we can assist in any other way, please contact Harley Geiger at HLGeiger@Venable.com.

Respectfully submitted,

The Cybersecurity Coalition
The Information Technology Industry Council

[22] Modernizing the E-rate Program for Schools and Libraries, Report and Order and Further Notice of Proposed Rulemaking, 29 FCC Rcd 8870, para. 133, Jul. 23, 2014, https://www.fcc.gov/document/fcc-releases-e-rate-modernization-order.
[23] See, for example, Schools and Libraries Universal Service Support Mechanism et al., Order, 29 FCC Rcd 13404, para. 10, Oct. 28, 2014, https://docs.fcc.gov/public/attachments/DA-14-1556A1.pdf. See also Modernizing the E-Rate Program for Schools and Libraries, Order, 30 FCC Rcd 9923, para. 15, Sep. 11, 2015, https://www.fcc.gov/document/fy-2016-e-rate-esl-order.
[24] 47 USC 254(c)(1).