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

In the Matter of	)	
	)	
Modernizing the E-Rate Program for Schools and Libraries	)	WC Docket No. 13-184
	)	

COMMENTS OF FORTINET, INC.

Hugh P. Carroll
Robert A. Turner
FORTINET, INC.
899 Kifer Road
Sunnyvale, CA 94086

Michele C. Farquhar
J. Ryan Thompson
HOGAN LOVELLS US LLP
555 Thirteenth St. NW
Washington, DC 20004
(202) 637-5600

Counsel to Fortinet, Inc.

September 21, 2022

TABLE OF CONTENTS

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

In the Matter of	)	
	)	
Modernizing the E-Rate Program for Schools and Libraries	)	WC Docket No. 13-184
	)	

COMMENTS OF FORTINET, INC.

Fortinet, Inc.[1] ("Fortinet") submits these comments in response to the Wireline Competition Bureau's ("Bureau's") request for comment on the proposed eligible services list ("ESL") for the E-Rate program's 2023 funding year.[2] Risks related to online fraud, identity theft, ransomware, and data privacy have exploded. Criminals and bad actors continue to target cyberattacks at schools, libraries, and other anchor institutions that serve as the foundations of our communities. Fortunately, the E-Rate program is well positioned to help schools and libraries defend themselves. Fortinet urges the Bureau to clarify that Category Two funding under the subcategories "basic maintenance of eligible broadband internal connections" or "firewall services and firewall components" can be used for next-generation firewalls.

I. INTRODUCTION AND SUMMARY

For over twenty years, the E-Rate program has been critical to supporting schools' and libraries' connectivity needs. Over that period, the internet's role in education has grown from

[1] Fortinet is a global leader in cybersecurity solutions provided to a wide variety of organizations, including enterprises, communication service providers, government organizations, and small businesses. Our cybersecurity solutions are designed to provide broad visibility and segmentation of the digital attack surface through our integrated platform, which features automated protection, detection, and response. Fortinet focuses its business on security-driven networking, infrastructure security, dynamic cloud security, and IoT and AI-based security solutions. See www.fortinet.com for more information about the company.

[2] *Wireline Competition Bureau Seeks Comment on Proposed Eligible Services List for the E-Rate Program*, Public Notice, WC Docket No. 13-184, DA 22-878 (WCB rel. Aug. 22, 2022).

novelty to necessity. And through various orders and yearly ESLs, the Commission and Bureau updated the E-Rate program to keep pace with schools' and libraries' connectivity needs. Yet, for years, the E-Rate support for E-Rate-eligible internal networks has excluded the necessary tools for mitigating evolving cybersecurity risks to those networks. What's more, the evidence is overwhelming: schools and libraries are now primary targets for cyberattacks. American schools and libraries heavily rely on unsecured IT infrastructure for educational and administrative functions. And cybercriminals know it. It is no secret that cybersecurity and IT budgets are often limited. At many (if not most) schools and libraries across the country, lean IT teams wage a daily battle to secure obsolete infrastructure with limited tools and resources as malicious actors grow smarter. Schools and libraries cannot win this battle without access to tools designed to protect against the growing cyber threat.

The risks to schools and libraries are profound and pervasive. In September 2022, the Federal Bureau of Investigation ("FBI"), Cybersecurity and Infrastructure Security Agency ("CISA"), and the Multi-State Information Sharing and Analysis Center ("MS-ISAC") issued a joint advisory noting that (1) the "[i]mpacts from [cyber]attacks have ranged from restricted access to networks and data, delayed exams, canceled school days, and unauthorized access to and theft of personal information regarding students and staff" and (2) these attacks "may increase as the 2022/2023 school year begins and criminal ransomware groups perceive opportunities for successful attacks."[3] Cyberattacks have already taken down many school systems' core networks and forced schools to cancel many days of class time. Cyberattacks

[3] Alert (AA22-249A), #StopRansomware: Vice Society, CISA (last revised Sept. 8, 2022), https://bit.ly/3qrnlNE (emphasis added) ("Sept. 2022 K-12 JCA").

against schools have been recorded in all 50 states across districts large and small, rural and urban.

Moreover, the risk goes beyond bad actors simply disabling the basic functions of schools' and libraries' networks. Schools and libraries maintain troves of highly sensitive, personally identifiable information ("PII") for students, teachers, staff, and library patrons. Children's PII is particularly valuable for identity thieves because of the clean credit history and lack of monitoring. It is no surprise that data breaches have led to identity theft and other types of fraud that have gone undetected for years. In addition, many schools and libraries use cloud-based solutions to store workloads and data, including sensitive PII about students, teachers, and staff. Next-generation firewalls are necessary for safely using these cloud-based tools, and basic firewalls are wholly insufficient for secured cloud connectivity.

Modern cybersecurity solutions are highly effective at protecting school and library networks against the most common intrusions and vulnerabilities. While the Commission determined in 2019 that these tools, aside from basic firewalls, were not "truly necessary" for the functioning of school networks, the past three years have shown otherwise. Fortunately, the Commission has delegated authority to the Bureau to update the E-Rate ESL, including by clarifying that next-generation firewalls are eligible for Category Two support.[4] In particular,

[4] Fortinet had urged the Commission to permit E-Rate reimbursements for (1) endpoint detection and protection, such as antimalware software; (2) advanced+ services, such as multi-factor authentication; and (3) such other services necessary to meet the emerging cyber threats confronting schools and libraries in the United States. Comments of Fortinet, Inc., WC Docket No. 13-184 (filed Sept. 27, 2021). As detailed in Sections II and III, these tools are also critical for securing school and library networks. Given the Commission's past reluctance to fund network security solutions through E-Rate reimbursements, these comments urge the Bureau, at a minimum, to take the incremental step of permitting advanced firewalls for E-Rate Funding Year 2023. In paring back its recommendations from last year's comments, Fortinet seeks to address concerns that expanding E-Rate eligibility for cybersecurity solutions could lead schools and libraries to use a significant segment of E-Rate funds for such tools. As discussed below,

the Bureau can include next-generation firewalls in the ESL by (1) expressly identifying next-generation firewalls as meeting the definition of "basic maintenance of eligible broadband internal connections" or (2) adding a new note clarifying that "firewall services and firewall components" include "next-generation firewalls."

Because network security is necessary for school and library networks to function, Fortinet's proposed clarifications would follow the Commission's E-Rate modernization efforts, which were meant to keep the E-Rate program updated as the connectivity needs of schools and libraries evolve. Implementing the proposed clarifications is long overdue.

Schools and libraries would retain the flexibility to choose how to connect and secure their networks most efficiently. And because E-Rate Category Two budgets are fixed, the proposed clarifications would not and could not deplete the E-Rate fund.

Authorizing schools and libraries to use E-Rate funds on cybersecurity software and services is a long overdue measure to empower educational institutions to combat a pervasive and costly threat. Fortinet urges the Bureau to recognize the scope and scale of cybersecurity risks that schools and libraries face and clarify in the FY2023 ESL that next-generation firewalls qualify as "basic maintenance of eligible broadband internal connections" or "firewall services and firewall components."

those concerns are unfounded due to how the Commission has structured Category 2 funding caps. *See infra* Section IV. And by expanding Category 2 eligibility only to next-generation firewalls, the Bureau can monitor how schools and libraries shift their spending of E-Rate funds.

II. SCHOOLS AND LIBRARIES FACE CRIPPLING CYBER RISKS THAT REQUIRE ADEQUATE CYBERSECURITY TOOLS.

A. Cyberattacks on Schools and Libraries Are Widespread and Damaging.

In 2014, the Commission first decided to narrowly limit the E-Rate eligibility of network security solutions to basic firewalls and uninterruptible power supply/battery backup. That decision was more than a wireless broadband generation ago when the threat of cyberattacks on schools and libraries and the risk of harm was relatively limited.[5] And the underlying premise is no longer true: the nation's schools and libraries are facing an epidemic of cyberattacks.

Between 2018 and 2021, the number of *reported* K-12 cyberattacks increased 318%.[6] While this stark increase is itself alarming, staff at the K12 Security Information Exchange state that "anecdotal evidence suggests perhaps 10 to 20 times more K-12 cyber incidents go undisclosed every year."[7]

Indeed, Fortinet's threat intelligence and research team at FortiGuard Labs found the education sector is among the most heavily targeted by a broad array of cyberattacks:

> [C]ertain sectors see higher levels of activity, regardless of the specific exploit in question. Education, Government, Managed Security Service Providers (MSSPs), and Telecommunications are visibly "hotter" across the board, often doubling or tripling the prevalence exhibited in other sectors. Organizations in these sectors tend to have a high number of devices . . . . And some of them—most notably

[5] *Modernizing the E-Rate Program for Schools and Libraries*, Report and Order and Further Notice of Proposed Rulemaking, 29 FCC Rcd 8870 ¶ 121 (2014) ("*First E-Rate Modernization R&O*").

[6] Douglas A. Levin, *The State of K-12 Cybersecurity: Year in Review – 2022 Annual Report*, K12 Security Information Exchange (K12 SIX) (2022) ("*The State of K-12 Cybersecurity: Year in Review – 2022 Annual Report*").

[7] *Id.*

> educational institutions—traditionally have looser control over the security and usage of those devices.[8]

Federal officials agree. On September 6, 2022, the FBI, CISA, and MS-ISAC issued a Joint Cybersecurity Advisory highlighting the risk to the education sector:

> Over the past several years, the education sector, especially kindergarten through twelfth grade (K-12) institutions, have been a frequent target of ransomware attacks. Impacts from these attacks have ranged from restricted access to networks and data, delayed exams, canceled school days, and unauthorized access to and theft of personal information regarding students and staff. *The FBI, CISA, and the MS-ISAC anticipate attacks may increase as the 2022/2023 school year begins and criminal ransomware groups perceive opportunities for successful attacks. School districts with limited cybersecurity capabilities and constrained resources are often the most vulnerable*; however, the opportunistic targeting often seen with cyber criminals can still put school districts with robust cybersecurity programs at risk. K-12 institutions may be seen as particularly lucrative targets due to the amount of sensitive student data accessible through school systems or their managed service providers.[9]

In 2021, ransomware attacks became the most-reported type of cyberattack cataloged by the K12 Security Information Exchange.[10] The FBI, CISA, and MS-ISAC report that one prominent group of cyberattackers is "disproportionately targeting the education sector with ransomware attacks."[11] Worse, the ransomware threat continues to evolve. Over the first half of 2022, Fortiguard Labs identified "10,666 ransomware variants across [the Fortinet] platform,

[8] *Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs*, Fortinet, at 6 (Aug. 2021), https://bit.ly/3AgwA6C.

[9] Sept. 2022 K-12 JCA (emphasis added).

[10] *The State of K-12 Cybersecurity: Year in Review – 2022 Annual Report* at 7.

[11] *See supra* note 9.

compared to just 5,400 in the previous six months,"[12] which is being driven by "plug-and-play" Ransomware-as-a-Service.[13]

FortiGuard Labs recently highlighted some of the most significant cybersecurity trends that IT staff in the education sector need to keep in mind:

- **IoT and CMS threats –** With several major exploits targeting IoT devices and content management systems ("CMS"), institutions should look for vulnerabilities in these categories. Vulnerable CMSs can make soft targets for easy access into enterprise environments. Attackers also seek to subvert the less-than-enterprise-grade security inherent to many IoT devices used in home networks.
- **Phishing attacks –** Phishing attacks can inject code and redirect users to malicious sites. These attacks are all the more prevalent because of remote and hybrid learning.
- **Ransomware –** The continued evolution of Ransomware-as-a-Service means schools and libraries must guard against demands made by cybercriminals who threaten to disclose sensitive student data.
- **Malware –** One vector that bad actors targeted was Microsoft systems and applications used by students and educators. These include 32-bit Windows executables, MS Office products, Visual Basic, and the Microsoft Intermediate Language. Common document formats such as PDF and RTF are also prime targets, as are web browsers.

Each of these threats can disable a school network, allow for the exfiltration of sensitive data, and lead to the theft of school funds. But with next-generation firewalls, schools and libraries can detect and stop these threats to ensure that school networks remain up and running.

B. Cybersecurity Is Central to the Operation of Schools and Libraries.

Many K-12 school districts are rapidly transforming their networks to implement eLearning and other digital programs to enhance student learning across distributed campuses. The need for remote learning during the first two years of the COVID-19 pandemic brought

[12] *Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs*, Fortinet, at 3 (Aug. 2022), https://bit.ly/3eC9v8L.

[13] *Id.* at 13.

enduring changes in how schools and libraries digitally serve the public. As educational networks evolve to deliver better learning experiences, funding shortfalls force school districts to deprioritize cybersecurity. It is no surprise, then, that schools and libraries are prime targets for cybercriminals.

CISA's K-12 cybersecurity guidance reports, "Malicious cyber actors are targeting school computer systems, slowing access, and rendering the systems inaccessible to *basic functions*."[14] Cyberattacks have forced schools to cancel school days and postpone classes. Cybercriminals have destroyed student records[15] and stolen students' PII.[16]

School districts and libraries in all 50 states have reported being the victims of cyberattacks.[17] For example, within the past couple of weeks, the nation's second-largest school district, Los Angeles Unified School District, was the victim of a massive cyberattack. "The private data of more than 400,000 students could be at risk," according to the Los Angeles Times.[18] The full extent of the damage may not be known for months or years. The

[14] Cyber Threats to K-12 Remote Learning Education, CISA (Dec. 2020), https://bit.ly/2VkoNFF (emphasis added).

[15] James Carr, *Schools lose Covid testing data and student coursework after 'spike' in cyber attacks*, SCHOOLS WEEK (Mar. 23, 2021), https://bit.ly/3yKKY5C.

[16] Douglas A. Levin, *The State of K-12 Cybersecurity: 2020 Year in Review*, K-12 Cybersecurity Resource Center and the K12 Security Information Exchange (2021), at n.5 https://bit.ly/3l0S1Cj ("The true figure of U.S. K-12 students who have had personal information exposed by their school districts and/or their vendors [between 2016 and 2020] is likely to be at least in the tens of millions . . . .").

[17] *The State of K-12 Cybersecurity: Year in Review – 2022 Annual Report* at 12 ("School districts in all 50 states and the District of Columbia (DC) have been cataloged on the K-12 Cyber Incident Map.").

[18] Howard Blume and Alejandra Reyes-Velarde, *Student information remains at risk after massive cyberattack on Los Angeles Unified*, LOS ANGELES TIMES (Sept. 7, 2022), https://lat.ms/3RPgV6H; *see also id.* ("'We're still going through student files because . . . the student management system was touched,' Supt. Alberto Carvalho said at a downtown news conference . . . .").

Superintendent recently wrote to the FCC Commissioners highlighting the need for E-Rate funding:

> We feel that supporting cybersecurity tools through the E-Rate program is not only appropriate under the FCC's existing goals for Universal Service, but also has reached a critical point as illustrated by the scope of the attack on Los Angeles Unified. . . . [I]t is imperative for FCC to take immediate action to enable school districts nationwide to strengthen their ability to prevent these IT infrastructure breaches in the future.[19]

Iowa's Cedar Rapids school district was forced to pay a ransomware ransom "in hopes of keeping personal data compromised in a cyberattack . . . from being released."[20] Late last year, Missouri's Eldon School District canceled classes for two days to recover from a ransomware attack that "close[d] down the internet altogether, including the district's phones, paging systems, and *security cameras*,"[21] which could have resulted in an intruder's unknown entry into the building, putting the physical safety of school occupants at risk. And a ransomware attack in Bergen County, New Jersey, forced a school district to cancel final exams for all high school students.[22] "There are no plans to reschedule them."[23]

A cyberattack can be devastating for schools and libraries. One recent study of ransomware attacks on U.S. schools found that schools suffered an average downtime of over

[19] Letter from Alberto M. Cavalho, Superintendent of Schools, Los Angeles Unified School District, to Jessica Rosenworcel, Chairwoman, FCC, *et al.* (Sept. 14, 2022), https://bit.ly/3xA4y70.

[20] Grace King, *Cedar Rapids schools pay ransom in cyberattack*, The Gazette (Aug. 12, 2022), https://bit.ly/3RwMLp8.

[21] Karl Wehmhoener, *Eldon School District canceled classes Tuesday due to ransomware attack*, ABC (Dec. 7, 2021), https://bit.ly/3A3YCDy (emphasis added).

[22] Jackie Roman, *Final exams canceled in N.J. school district after ransomware attack cripples computers*, NJ.com (June 8, 2022), https://bit.ly/3whfDcj.

[23] *Id.*

four days and spent nearly a month recovering from the attack.[24] The downtime alone is estimated to have cost education institutions $3.56 billion in 2021.[25]

Schools and libraries are not the only victims of cyberattacks. Data breaches can gravely injure students, teachers, and staff years after the fact. For example, "[i]n 2021, ransomware gangs published data from more than 1,200 American K-12 schools."[26] Schools and libraries are troves of PII, including banking information, health data, and Social Security numbers, that can be stolen and sold on the dark web. School and library systems use this information for completing and submitting homework, attending lectures, participating in extracurricular activities, scheduling transportation, and performing administrative functions. But bad actors can use this same information for malicious purposes.

C. Cybersecurity Is Unaffordable for Many School Districts.

The Commission's Equity Action Plan notes that the "Commission was given the incredibly important responsibility in the [Infrastructure Investment and Jobs Act] to adopt rules to 'facilitate equal access' to broadband, taking into account technical and *economic* feasibility."[27] Likewise, "availability" is a core Universal Service principle, and the FCC's recent *Report on the Future of the Universal Service Fund* reaffirmed that "cybersecurity" is an "important concept[]" that was "captured by [the Commission's] existing availability goals."[28]

[24] Paul Bischoff, *Ransomware attacks on US schools and colleges cost $3.56bn in 2021*, Comparitech (June 23, 2022), https://bit.ly/39eFupv (emphasis added).

[25] *Id.*

[26] Kevin Collier, *Hackers are leaking children's data — and there's little parents can do*, NBC NEWS (Sept. 10, 2021), https://nbcnews.to/3zbVumN.

[27] Equity Action Plan, FCC, DOC-382389 (2022), https://bit.ly/3RLUrDA.

[28] *Report on the Future of the Universal Service Fund*, Report, WC Docket No. 21-476 ¶ 14 (rel. Aug. 15, 2022).

Yet the draft ESL fails to accord with the Commission's view by nearly fully excluding network security solutions from the E-Rate program.

One of the reasons budget-constrained schools and libraries are so often targeted is they lack the resources to invest in cybersecurity. For example, a survey conducted by the State Educational Technology Directors Association ("SETDA") of school officials nationwide found that "only 6% of respondents said their state provides ample funding for cybersecurity, 37% said the state provides cybersecurity tools to Local Education Agencies, and 57% said their state provides very little or a small amount of funding for cybersecurity."[29]

Overburdened IT teams have struggled to simply ensure that students have the tools and connections they need to connect to school remotely. And teachers have had to wrestle with unfamiliar technology to upload and download lesson plans and homework assignments, broadcast their classrooms, and provide one-on-one assistance for struggling pupils. There has been little time or money left over for adequate security measures.

Under-resourced schools in both urban and rural areas are at a particular disadvantage due to the cost of acquiring the technical and human safeguards needed for robust cybersecurity. Indeed, as the FBI, CISA, and MS-ISAC advisory noted, "[t]hese issues will be particularly challenging for K-12 schools that face resource limitations; therefore, educational leadership, information technology personnel, and security personnel will need to balance this risk when determining their cybersecurity investments."[30]

[29] Liz Cohen and Evo Popoff, *2022 State EdTech Trends Report*, SETDA, at 13 (2022), https://bit.ly/3TVLcmi.

[30] Alert (AA20-345A), Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data, CISA (Dec. 10, 2020), https://bit.ly/3tjoO9z ("Dec. 2020 CISA K-12 JCA"); *see also* Sept. 2022 K-12 JCA.

Investing in cybersecurity can be an almost impossible challenge for the nation's resource-constrained school districts, leading to large cybersecurity gaps between wealthy and poor communities. The cost of not implementing adequate security measures can be crippling for some school systems. For one thing, ransomware and legal costs from the attack itself can easily reach millions of dollars.[31] Cybersecurity threats are increasing the cost of financing.[32] Premiums for risk and liability insurance are also increasing.[33] And properly investing in cybersecurity means that funding for other priorities is no longer available.

Private organizations are stepping up to do their part. For example, Fortinet recently announced that its information security awareness and training service would be made available to faculty and staff of all K-12 schools across the United States free of cost.[34] The announcement coincided with the White House National Cyber Workforce and Education Summit, where Fortinet participated in important discussions around solutions to help address

[31] A recent ransomware attack on Broward County Public Schools sought a $40 million ransom to unlock school systems and data. Scott Travis, *Hackers post 26,000 Broward school files online*, SOUTH FLORIDA SUN SENTINEL (Apr. 19, 2021), https://bit.ly/3qqh8S9 ("Hackers who demanded up to $40 million from the Broward School District have now published nearly 26,000 files stolen from district servers.").

[32] *Cyber Risk In A New Era: The Increasing Credit Relevance Of Cybersecurity*, S&P Global (July 14, 2021), https://bit.ly/3h7z148 ("Over the last 12 months we have seen attacks on the U.S. city of Hartford and numerous Texas school districts, across municipal utility sectors, and, more recently, on the Irish healthcare system. To help mitigate the potential negative credit impact of cyberattacks, robust cybersecurity remains vital.").

[33] Don Fancher *et al.*, *Seven hidden costs of a cyberattack*, Deloitte ("Deloitte conducted informal research among leading providers of cyber insurance and found that it is not uncommon for a policyholder to face a 200 percent increase in premiums for the same coverage, or possibly even be denied coverage until stringent conditions are met following a cyber incident.") (last visited Sept. 5, 2022).

[34] Press Release, Fortinet, Fortinet Announces Free Training Offering for Schools at White House National Cyber Workforce and Education Summit (July 19, 2022), https://bit.ly/3T20A03.

the significant talent shortage affecting the cybersecurity industry in the United States.[35] This commitment builds on Fortinet's pledge to train one million people globally over the next five years through its Training Advancement Agenda initiatives and Network Security Experts Training Institute programs.[36]

But no matter how robust these efforts are, private sector philanthropy is no substitute for Commission-driven financial support for critical cybersecurity software, hardware, and services.

III. AT A MINIMUM, CLARIFYING THAT NEXT-GENERATION FIREWALLS QUALIFY FOR E-RATE SUPPORT WILL BETTER PROTECT SCHOOL AND LIBRARY NETWORKS.

Fortinet supports and recognizes the need for schools and libraries to have access to broader network security solutions to meet these critical current needs, as highlighted by the Los Angeles Unified School District Superintendent. Should the Bureau need to move more slowly in providing access to E-Rate funding, however, the best first step is for the Bureau to modestly expand and clarify the scope of the FY2023 E-Rate Eligible Services List. In particular, the Bureau can include next-generation firewalls in the ESL by (1) expressly identifying next-generation firewalls as meeting the definition of "basic maintenance of eligible broadband internal connections" or (2) adding a new note clarifying that "firewall services and firewall components" include "next-generation firewalls."

The Bureau has ample legal authority to address the dearth of E-Rate funding for next-generation firewalls. The Commission delegated to the Bureau the authority to clarify that next-

[35] FACT SHEET: National Cyber Workforce and Education Summit, Executive Office of the President (July 21, 2022), https://bit.ly/3c22gpF ("Fortinet is furthering its commitment to close the cyber skills gap by making its information security awareness and training service available for free for all K-12 school districts across the U.S.").

[36] Press Release, Fortinet, Fortinet Pledges To Train 1 Million People to Help Close the Cybersecurity Skills Gap Following White House Summit (Sept. 8, 2021), https://bit.ly/3EsHs3I.

generation firewalls are considered "basic maintenance" in the ESL. For the same reasons, the Bureau could alternatively determine that next-generation firewalls fall within the "[f]irewall services and firewall components" category.

A. The Proposed ESL Does Not Identify Next-Generation Firewalls as E-Rate-Eligible.

"Firewall and firewall components" are the only network security-related Category 2 items expressly listed in the draft ESL. So far, the Bureau has opted not to clarify that next-generation firewalls are E-Rate eligible. The Commission, however, "le[ft] the record open on these services to allow for further comment."[37]

Before the FY2015 ESL proceeding, E-Rate ESLs included an extensive glossary of terms on which applicants could rely. In the FY2015 ESL proceeding, the Bureau eliminated the long-form glossary, leaving terms undefined and directing applicants to refer to the non-binding Universal Service Administrative Company ("USAC") ESL glossary.[38] The Universal Service Administrative Company defines an E-Rate-eligible "firewall" as "a hardware and software

[37] *First E-Rate Modernization R&O* ¶ 121 ("[W]e decline at this time to designate further network security services and other proposed services . . . . [W]e leave the record open on these services to allow for further comment . . . ."); *Modernizing the E-Rate Program for Schools and Libraries*, Order, 32 FCC Rcd 7414 ¶ 5 (2017) ("[T]he Commission kept the record open in this proceeding to allow for further comment on [network security] services . . . .").

[38] *See Schools and Libraries Universal Service Support Mechanism et al.*, Order, 29 FCC Rcd 13404 ¶ 7 (2014) ("To provide further guidance for applicants and vendors, we direct USAC to include an ESL Glossary on its webpage.") ("*2014 ESL Order*"); *id.*, App. C ("Additional guidance from USAC about the E-Rate application process and about eligible services, including a glossary of terms, is available at USAC's website at http://www.usac.org/sl/. Those documents on USAC's website are not incorporated by reference into the ESL and do not bind the Commission. Thus, they will not be used to determine whether a service or product is eligible. Applicants and service providers are free to refer to those documents, but just for informal guidance.").

combination that sits at the boundary between an organization's network and the outside world, and protects the network against unauthorized access or intrusions."[39]

Basic firewalls alone cannot protect against the cyberattacks schools and libraries face today. CISA's Joint Cybersecurity Advisory to schools identified ransomware, malware, and Distributed Denial of Service attacks as the three main threats to schools' networks and data.[40] Basic firewalls alone cannot protect against these attacks. Nor can these basic firewalls mitigate the damage caused.[41]

By contrast, next-generation firewalls often do so much more than just fence the boundaries between trusted internal networks and untrusted external networks. As CoSN and Funds for Learning point out, next-generation firewalls offer a suite of security enhancements that include:

- **Intrusion Prevention / Intrusion Detection (IPS/IDS) –** detecting and stopping network activity that violates pre-defined security policies
- **Virtual Private Network (VPN) –** creating secure channels for data transmission from inside private networks over public networks

[39] *Schools and Libraries (E-Rate) Program: Eligible Services List (ESL) Glossary*, https://bit.ly/2Vtmf8i (last visited Sept. 6, 2022).

[40] Dec. 2020 CISA K-12 JCA.

[41] *See, e.g.,* Security Tip (ST04-004), Understanding Firewalls for Home and Small Office Use, CISA (last revised Nov. 14, 2019), https://bit.ly/2XA0RiZ ("Though properly configured firewalls may effectively block some attacks, do not be lulled into a false sense of security. Firewalls do not guarantee that your computer will not be attacked. Firewalls primarily help protect against malicious traffic, not against malicious programs (i.e., malware), and may not protect you if you accidentally install or run malware on your computer."); Reply Comments of Cox Communications, Inc., WC Docket No. 13-184, at n.5 (filed Sept. 4, 2020) ("[C]ertain types of reflective DDoS attacks . . . can saturate Internet broadband circuits, leaving local firewall appliances helpless to restrict unwanted traffic."); Comments of Funds for Learning, LLC, WC Docket No. 13-184, at 7 (filed Aug. 14, 2020) ("When schools, libraries, and service providers discuss firewalls, they are referring to multi-function advanced security devices, not the basic firewall definition . . . .").

- **Distributed Denial-of-Service protection (DDoS) –** protecting against attempts to overload a network with malicious traffic, which can halt its operation
- **Network Access Control (NAC) –** preventing network disruptions by authenticating entrants based on risk profiles[.][42]

Many of these functions can be cost-effectively combined into a single security solution. For example, next-generation firewalls such as Fortinet's FortiGate include firewall, antivirus, application control, and intrusion prevention capabilities.[43] This eliminates the need for school districts to deploy and manage separate tools, such as a secure web gateway or intrusion prevention system, which can also lead to additional IT staffing requirements. FortiGate also performs secure sockets layer ("SSL") packet decryption and inspection, enabling content filtering in completely SSL-encrypted environments.

B. The Bureau Has the Legal Authority to Add New Technologies to the E-Rate Program Through Clarifications to the ESL.

The Bureau has yet to clarify that any cybersecurity tools, aside from basic "firewall services and firewall components," are E-Rate eligible. The Commission, however, "le[ft] the record open on these services to allow for further comment."[44] Indeed, the *First E-Rate Modernization R&O* noted that the Commission's expansive authority to define E-Rate eligibility "reflects Congress's recognition that technology needs are constantly 'evolving' in light of 'advances in telecommunications and information technologies and services.'"[45]

[42] *E-Rate Cybersecurity Cost Estimate: Calculating the annual expense to provide Universal Service Funding support for K-12 school network security in the United States*, CoSN and Funds for Learning, at 9 (Jan. 2021), https://bit.ly/3qUsePE.

[43] *See Charting the Security Journey for K-12 Schools*, Fortinet, https://bit.ly/3uds2f5 (last visited Sept. 6, 2022).

[44] *First E-Rate Modernization R&O* ¶ 121; *Modernizing the E-Rate Program for Schools and Libraries*, Order, 32 FCC Rcd 7414 ¶ 5 (2017) ("[T]he Commission kept the record open in this proceeding to allow for further comment on [network security] services . . . .").

[45] *First E-Rate Modernization R&O* ¶ 67.

Consistent with this broad congressional mandate, the Commission retained eligibility for basic firewalls—a non-telecommunications service—and noted that it was first narrowly proscribing eligible services to maximize funding for other internal connections components and services.[46]

While the Commission in 2019 found that adding cybersecurity tools was not "truly necessary to deliver high-speed broadband to students and library patrons," it left open the prospect of revisiting that determination.[47] Then-Commissioner Rosenworcel even noted the tentative nature of the Commission's 2019 assessment:

> [I]t is important to note that we need to keep a close watch on emerging cyber vulnerabilities affecting schools and libraries. . . . As these problems grow more common, it is appropriate to consider what practices can help prevent school and library networks avoid the inconvenience and harm that follows in the wake of these attacks. So I am pleased that my colleagues agree that *the agency should be open to learning more about these challenges. I hope this will help inform policies that across the board will ensure that school and library networks remain strong and secure in the future.*[48]

Then-Commissioner Rosenworcel's comments were prescient. Many more vulnerabilities have emerged since 2019, and the lost classroom time, compromised PII, and increasingly costly and frequent ransomware attacks warrant moving past basic firewalls and instead supporting next-generation firewalls as an integral component of schools' and libraries' educational purposes. Also, excluding E-Rate support for next-generation firewalls could counterproductively undercut the utility of each dollar spent on school and library connectivity. A robust internal network means very little for a school that cannot access its own systems and

[46] *Id.* ¶ 121 ("[W]e decline *at this time* to designate further network security services and other proposed services in order to ensure internal connections support is targeted efficiently at the equipment that is necessary for LANs/WLANs.") (emphasis added).

[47] *Modernizing the E-Rate Program for Schools and Libraries*, Report and Order, 34 FCC Rcd 11219 ¶ 46 (2019) ("*Category Two R&O*").

[48] *Id.*, Concurring Statement of Commissioner Jessica Rosenworcel (emphasis added).

data due to a cyberattack. In short, if the Commission intends to spend money building networks, it needs to spend money securing networks.[49]

Literal necessity is not the standard for E-Rate eligibility. Eligible E-Rate costs already include components that are not "truly necessary" to operate a network, including "uninterruptible power supply/battery backup," "[b]asic technical support," and "[s]oftware upgrades and patches."[50] Fortunately, the five-year budget model for Category Two costs gives schools and libraries the flexibility to decide how to maximize a fixed amount of E-Rate funds to connect and secure their networks.

The Bureau has the authority to act now. In previous ESL decisions, the Bureau has acted to update E-Rate eligibility through clarifications on the scope of covered services.[51] Indeed, the Commission has made clear that the Chief of the Bureau possesses the authority to

[49] *Id.* ¶ 46.

[50] *Modernizing the E-Rate Program for Schools and Libraries*, Order, 35 FCC Rcd 13793, 13801-02 (2020).

[51] *See, e.g.*, *2014 ESL Order* ¶ 10 ("[W]e add MPLS to Category One in order to clarify that MPLS is eligible for Category One E-Rate support. . . . Clarifying that MPLS as one of the eligible Category One services is akin to the Commission's decision in 2009 to add Ethernet to the ESL as an eligible digital transmission service . . . ."); *id.* ¶ 17 ("[W]e agree with commenters that antennas that are an integral part of the LAN or WLAN are eligible for Category Two funding, because they are subsumed by or essential to the components necessary to distribute internal broadband services within a school or library. . . . Clarifying the list of Category Two components to include antennas is a logical extension of the Commission's decision in the E-Rate Modernization Order . . . ."); *Modernizing the E-Rate Program for Schools and Libraries*, Order, 30 FCC Rcd 9923 ¶ 15 (2015) ("We adopt the proposed addition of ISDN to the list of eligible voice services.").

interpret the Commission's E-Rate rules,[52] an authority the Commission reaffirmed in 2019.[53] Thus, the Bureau possesses the expressly delegated authority to update the ESL by clarifying that next-generation firewalls are eligible for E-Rate support.

The *FY2022 E-Rate ESL Order* deferred consideration of "cybersecurity services" because "Congress directed the U.S. Department of Homeland Security to conduct a study of K-12 cybersecurity risks," issue K-12 guidelines based on those risks, and then release a toolkit for school administrators and staff.[54] But despite the accompanying deadlines,[55] there is no indication of when those guidelines will be published.[56] And in light of the manifold harm to schools, libraries, students, staff, and patrons, the Bureau should not delay once again.

Given the evolving threat landscape, and consistent with the incremental approach taken in the *First E-Rate Modernization R&O* and the Communications Act, the Bureau is well-positioned to clarify—now—that next-generation firewalls are eligible for E-Rate support.

[52] *Federal-State Joint Board on Universal Service*, Third Report and Order, 12 FCC Rcd 22485 ¶ 6 (1997) ("To the extent clarification of our rules are necessary, however, we delegate to the Chief, Common Carrier Bureau the authority to issue orders interpreting our rules as necessary to ensure that support for services provided to schools and libraries and rural health care providers operate to further our universal service goals.").

[53] *Category Two R&O* at n.77 ("[W]e direct the Bureau to provide clarifying guidance consistent with the terms of this Report and Order, and publish clarifications or additional guidance with respect to the implementation and administration of district-wide and library system-wide category two budgets to the extent necessary.") (citing *id.*).

[54] *Modernizing the E-Rate Program for Schools and Libraries*, Order, WC Docket No. 13-184, DA 21-1602 ¶ 9 (WCB rel. Dec. 17, 2021) ("*FY2022 E-Rate ESL Order*") (citing K-12 Cybersecurity Act, 2021, H.R. 17-122, Pub. L. No. 117-47, 117th Cong. (2021)).

[55] Deadlines for the study, guidelines, and toolkits were February 5, April 6, and August 4, 2022, respectively.

[56] The law requires these materials to be made available on a Department of Homeland Security website. K-12 Cybersecurity Act, 2021 § 3(e).

Finally, at a minimum, the Bureau should remind parties in the ESL order that it possesses the authority to waive E-Rate eligibility restrictions where it is in the public interest to do so.[57]

IV. ALLOWING FUNDING FOR ELIGIBLE NETWORK SECURITY FEATURES WILL NOT DEPLETE THE E-RATE FUND.

Permitting schools and libraries to use Category Two funding for necessary next-generation firewalls will not deplete the E-Rate fund. To begin with, giving schools and libraries the option to purchase cybersecurity services would not increase the total amount of E-Rate subsidies that schools or libraries might receive. The Commission's funding approach for Category Two support is designed to give schools and libraries the flexibility to decide how to use a fixed amount of funding to connect and secure their networks—without depleting the E-Rate fund.[58]

For example, the Commission had at first proposed in its E-Rate modernization notice of proposed rulemaking to cease support for internal connections "because the same high-discount school districts received ample funding, while most school districts received none." The *First E-Rate Modernization R&O* reversed course, however, finding that the Commission could

[57] *Modernizing the E-Rate Program for Schools and Libraries*, Order, 32 FCC Rcd 1189 ¶ 7 (2017) ("The Bureau, therefore, finds that special circumstances exist to grant a limited waiver of the classification standards adopted in the FY 2017 ESL for applicants seeking support for services currently delivered pursuant to a multi-year contract . . . ."). A Commission rule may be waived for "good cause shown." 47 C.F.R. § 1.3. Good cause, in turn, may be found "where particular facts would make strict compliance inconsistent with the public interest." *Ne. Cellular Tel. Co. v. FCC*, 897 F.2d 1164, 1166 (D.C. Cir. 1990) ("*Ne. Cellular*"). In addition, the Commission may consider hardship, equity, or more effective implementation of overall policy on an individual basis. *See Ne. Cellular*, 897 F.2d at 1166.

[58] *Modernizing the E-Rate Program for Schools and Libraries*, Report, 34 FCC Rcd 319 ¶ 42 (2019) ("Under the category two budget approach, greater funding is available for internal connections, distributed to more applicants, in a more equitable and predictable manner, giving applicants more flexibility to determine how best to upgrade their systems.").

> achieve the stated goal of broader funding distribution through other means, including a reasonable and equitable limit on the total amount of E-Rate support available per student and per square foot[,] which will discipline districts and libraries in basic maintenance purchasing decisions. In particular, applicants are unlikely to seek support for unnecessary basic maintenance given these limits on the total amount available, but providing support to ensure these networks function effectively may aid those districts with limited resources.[59]

The Commission affirmed this approach in 2019 by making permanent the five-year budget model for Category Two funding.[60]

For the same reason that fixed Category Two budgets guard against overspending on internal connections and their basic maintenance, they would also guard against overspending on next-generation firewalls. In particular, because Category Two funds function as a fixed pot of money for schools and libraries, "applicants are unlikely to seek support for unnecessary" next-generation firewalls "given these limits on the total amount available."[61] Consistent with this approach, the Bureau can give schools and libraries the flexibility to spend their Category Two budgets on network infrastructure they believe to be essential to building and maintaining their networks, including security and network monitoring services. Each dollar invested in next-generation firewalls will provide a layer of protection far stronger than the security acquired by a dollar spent on the basic firewalls that are currently E-Rate-eligible.

Even though the Category Two five-year budget approach eliminates any concerns of fund depletion, it should be kept in mind, as well, that the E-Rate program is operating at a significant surplus. Total demand for all E-Rate support for Funding Year 2022 was only $3.15

[59] *First E-Rate Modernization R&O* ¶ 122.

[60] *Category Two R&O* ¶ 45.

[61] *See supra* note 59.

billion out of an overall program budget of $4.46 billion.[62] Another $500 million in rollover funds are available, too.[63] In other words, the E-Rate program will operate at more than a $1.8 billion surplus for Funding Year 2022.

V. CONCLUSION

Our nation's schools and libraries require stronger tools to protect their networks and related sensitive data from cyberattacks. The Bureau can and should take steps to help schools and libraries defend themselves against attackers that have identified these community anchors as easy targets due to their lack of adequate cybersecurity tools. At a minimum, the Bureau should clarify that schools and libraries can use Category Two E-Rate funds for next-generation firewalls. Doing so would recognize the Commission's E-Rate modernization efforts and Congress's very high prioritization of cybersecurity issues while taking targeted action to rout the onslaught of K-12 cyberattacks, which have increased 318% between 2018 and 2021.

Respectfully submitted,

/s/ Michele C. Farquhar
Michele C. Farquhar
J. Ryan Thompson
HOGAN LOVELLS US LLP
555 Thirteenth St. NW
Washington, DC 20004
(202) 637-5600

Counsel to Fortinet, Inc.

Hugh P. Carroll
Robert A. Turner
FORTINET, INC.
899 Kifer Road
Sunnyvale, CA 94086

September 21, 2022

[62] *Wireline Competition Bureau Directs USAC to Fully Fund Eligible Category One and Category Two E-Rate Requests*, Public Notice, CC Docket No. 02-6, DA 22-902 (WCB rel. Aug. 30, 2022).

[63] *Id.*