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.

Robert A. Turner,
Field Chief Information Security
Officer – Education
FORTINET, INC.
899 Kifer Road
Sunnyvale, CA 94086

September 27, 2021

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] 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 2022 funding year.[2] Risks related to fraud, identify theft, ransomware, and data privacy have exploded online. Criminals, terrorists, and state-sponsored actors are targeting cyberattacks at schools, libraries, and other anchor institutions that serve as foundations of our communities. To help address some of the risks that schools and libraries face, 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" includes: (1) next-generation firewalls; (2) endpoint detection and protection, such as anti-malware software; (3) advanced+ services, such as multi-factor authentication; and (4) such

[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 21-1062 (WCB rel. Aug. 27, 2021) ("*FY2022 E-Rate ESL PN*").

other services necessary to meet the emerging cyber threats confronting schools and libraries in the United States.

I. INTRODUCTION AND SUMMARY

For more than twenty years, the E-Rate program has been critical to supporting schools' and libraries' connectivity needs. Over that period of time, the internet's role in education has grown from novelty to necessity. The E-Rate program has needed to evolve to keep pace with schools' and libraries' connectivity needs.

As the benefits of a technology increase, so too do the potential harms from that technology losing functionality. For that reason, the United States must secure the internet infrastructure it helps build. It makes little sense to spend federal funds building roads without guardrails or dams without spillways. And yet, for years, the E-Rate program has supported internet services without also supporting comprehensive safety measures to mitigate cybersecurity risks to the nation's teachers and students. While earlier funding years may have left open questions about the need for cybersecurity safeguards, the evidence today is overwhelming: schools and libraries have become the primary targets for cyberattacks. Ransomware gangs and international criminal syndicates know American schools and libraries heavily rely on unsecured IT infrastructure for educational and administrative functions. And 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 become more sophisticated.

Schools and libraries cannot win this battle without more resources. The risks to schools and libraries are profound and pervasive. Cyberattacks have taken down many school systems' core networks and forced schools to cancel many days of class time. Cyberattacks against schools have been recorded in all 50 states across schools large and small, whether in rural or urban America. And the risk goes beyond vulnerabilities in any given school's IT infrastructure. Schools and libraries maintain a trove of highly sensitive, personally identifiable information ("PII") for students, staff, and library patrons. Data breaches through school networks have led to identity theft and other types of fraud that, for students unaccustomed to monitoring for identify theft, can go undetected for years and upend a student's professional life for decades.

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 two years have shown otherwise. Fortunately, the Commission has delegated authority to the Bureau to update the E-Rate ESL, including by clarifying that network security solutions[3] are eligible for E-Rate Category Two support. In particular, the Bureau can include network security solutions in the ESL by: (1) expressly enumerating the types of network security solutions that would meet the definition of "basic maintenance of eligible broadband internal connections"; *or* (2) adding a new note clarifying that "firewall services and firewall components" include "network security solutions."

Because network security solutions are necessary for schools and libraries to function, Fortinet's proposed clarifications would follow the Commission's E-Rate modernization efforts,

[3] As used in these comments and consistent with the proposals of the Consortium for School Networking ("CoSN") and others, "network security solutions" refers to (1) next-generation firewalls, (2) endpoint protection and detection, such as anti-malware software, (3) advanced+ services, such as multi-factor authentication, and (4) such other services that meet the emerging threats that schools and libraries face. *See* Petition for Declaratory Relief and Petition for Rulemaking of CoSN *et al.*, WC Docket No. 13-184 (filed Feb. 8, 2021). "Basic firewalls" refers to those currently E-Rate-eligible firewall services and components, whereas "next-generation firewalls" include the functionality of a basic firewall *and* additional, E-Rate-*in*eligible functions that must be cost-allocated.

which are designed to keep the E-Rate program updated as the connectivity needs of schools and libraries evolve. Clarifying that network security solutions are E-Rate-eligible would also follow Congress's high prioritization of cybersecurity issues.[4] Fortinet's proposed clarifications are 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 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 schools and libraries face and clarify in the FY2022 ESL that network security solutions qualify as "basic maintenance of eligible broadband internal connections" or "firewall services and firewall components."

[4] *See, e.g.*, Letter from Sens. Cantwell and Wicker to Secretary Raimondo, Dept. of Commerce (sent July 28, 2021), https://bit.ly/3kl7Btt ("Reliance on cyber-enabled systems provides an attractive target for U.S. adversaries and cybercriminals. Separate threat assessments by the Director of National Intelligence and the Department of Homeland Security ranked cyberattacks as an acute threat to government at all levels as well as to the private sector. . . . Cybersecurity threats are growing and evolving, so the federal response must do so as well."); Statement of Congressman Pallone (July 21, 2021), https://bit.ly/3kkJCui ("Today I am proud that the Energy and Commerce Committee came together to pass urgently needed legislation that will promote more secure networks and supply chains, bringing us one step closer to a safer and more secure wireless future."); Hannah Farrow, *Congress Heightens Emphasis on K-12 Cybersecurity During COVID-19*, EDUCATION WEEK (July 14, 2020), https://bit.ly/3hP0wQj; *see also supra* note 63 and accompanying discussion.

II. SCHOOLS AND LIBRARIES FACE CRIPPLING CYBER RISKS WITHOUT AFFORDABLE ACCESS TO NETWORK SECURITY.

A. Cyberattacks on Schools and Libraries Are Widespread and Rapidly Increasing.

In 2014, the Commission first decided to narrowly limit the E-Rate eligibility of network security solutions. That decision happened more than a broadband generation ago, when the threat of cyberattacks on schools and libraries and risk of harm was relatively limited.[5] That risk has changed dramatically: the nation's schools and libraries face an onslaught of cyberattacks today.

The education sector is among the most heavily targeted by a broad array of cyberattacks. The latest Global Threat Landscape Report by Fortinet's threat intelligence and research team at FortiGuard Labs finds:

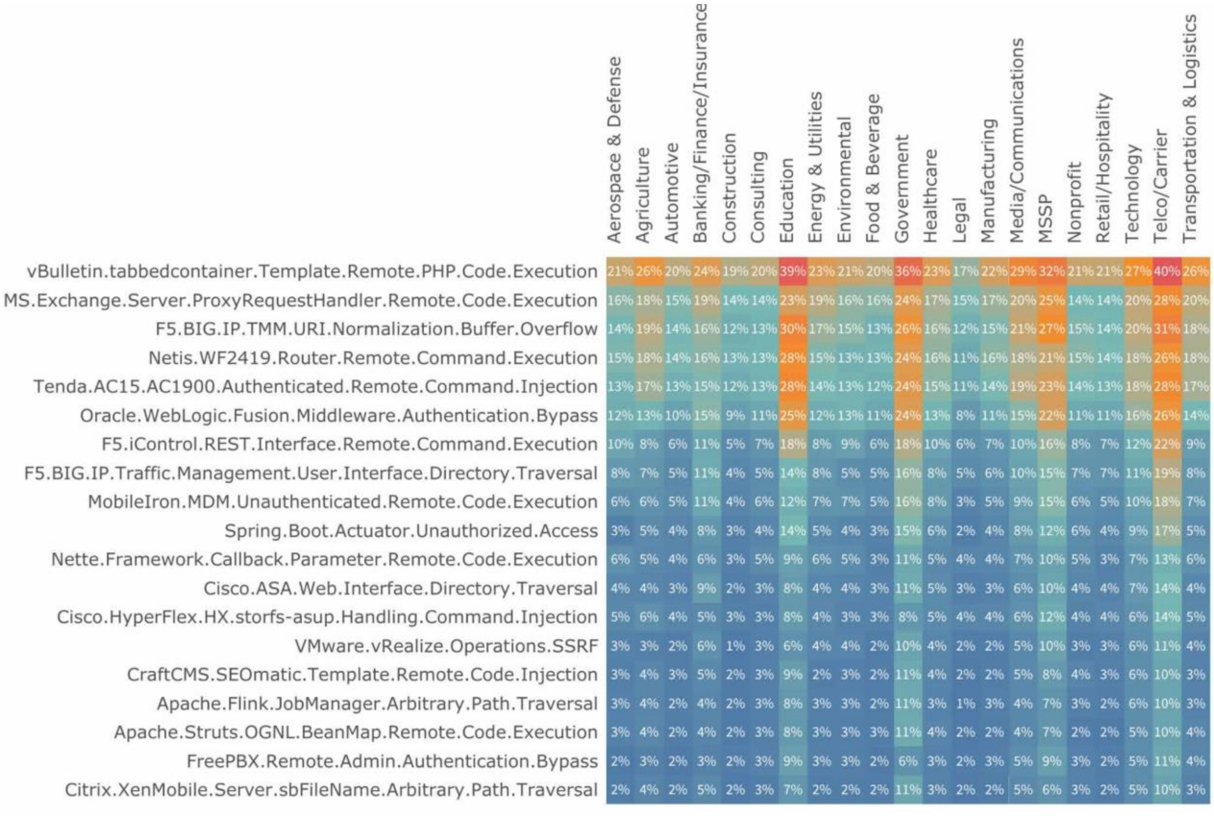
> [C]ertain sectors see higher levels of activity, regardless of the specific exploit in question. Education, Government, Managed Security Service Providers (MSSPs), and Telecommunications are visibly "hotter" across the board, often doubling or tripling the prevalence exhibited in other sectors. Organizations in these sectors tend to have a high number of devices . . . . And some of them—most notably educational institutions—traditionally have looser control over the security and usage of those devices.[6]

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

Figure 1 illustrates Fortiguard Labs' findings.

Figure 1: Prevalence of new Fortinet Intrusion Prevention System detections during 1H 2021[7]



	Aerospace & Defense	Agriculture	Automotive	Banking/Finance/Insurance	Construction	Consulting	Education	Energy & Utilities	Environmental	Food & Beverage	Government	Healthcare	Legal	Manufacturing	Media/Communications	MSSP	Nonprofit	Retail/Hospitality	Technology	Telco/Carrier	Transportation & Logistics
vBulletin.tabbedcontainer.Template.Remote.PHP.Code.Execution	21%	26%	20%	24%	19%	20%	39%	23%	21%	20%	36%	23%	17%	22%	29%	32%	21%	21%	27%	40%	26%
MS.Exchange.Server.ProxyRequestHandler.Remote.Code.Execution	16%	18%	15%	19%	14%	14%	23%	19%	16%	16%	24%	17%	15%	17%	20%	25%	14%	14%	20%	28%	20%
F5.BIG.IP.TMM.URI.Normalization.Buffer.Overflow	14%	19%	14%	16%	12%	13%	30%	17%	15%	13%	26%	16%	12%	15%	21%	27%	15%	14%	20%	31%	18%
Netis.WF2419.Router.Remote.Command.Execution	15%	18%	14%	16%	13%	13%	28%	15%	13%	13%	24%	16%	11%	16%	18%	21%	15%	14%	18%	26%	18%
Tenda.AC15.AC1900.Authenticated.Remote.Command.Injection	13%	17%	13%	15%	12%	13%	28%	14%	13%	12%	24%	15%	11%	14%	19%	23%	14%	13%	18%	28%	17%
Oracle.WebLogic.Fusion.Middleware.Authentication.Bypass	12%	13%	10%	15%	9%	11%	25%	12%	13%	11%	24%	13%	8%	11%	15%	22%	11%	11%	16%	26%	14%
F5.iControl.REST.Interface.Remote.Command.Execution	10%	8%	6%	11%	5%	7%	18%	8%	9%	6%	18%	10%	6%	7%	10%	16%	8%	7%	12%	22%	9%
F5.BIG.IP.Traffic.Management.User.Interface.Directory.Traversal	8%	7%	5%	11%	4%	5%	14%	8%	5%	5%	16%	8%	5%	6%	10%	15%	7%	7%	11%	19%	8%
MobileIron.MDM.Unauthenticated.Remote.Code.Execution	6%	6%	5%	11%	4%	6%	12%	7%	7%	5%	16%	8%	3%	5%	9%	15%	6%	5%	10%	18%	7%
Spring.Boot.Actuator.Unauthorized.Access	3%	5%	4%	8%	3%	4%	14%	5%	4%	3%	15%	6%	2%	4%	8%	12%	6%	4%	9%	17%	5%
Nette.Framework.Callback.Parameter.Remote.Code.Execution	6%	5%	4%	6%	3%	5%	9%	6%	5%	3%	11%	5%	4%	4%	7%	10%	5%	3%	7%	13%	6%
Cisco.ASA.Web.Interface.Directory.Traversal	4%	4%	3%	9%	2%	3%	8%	4%	4%	3%	11%	5%	3%	3%	6%	10%	4%	4%	7%	14%	4%
Cisco.HyperFlex.HX.storfs-asup.Handling.Command.Injection	5%	6%	4%	5%	3%	3%	8%	4%	3%	3%	8%	5%	4%	4%	6%	12%	4%	4%	6%	14%	5%
VMware.vRealize.Operations.SSRF	3%	3%	2%	6%	1%	3%	6%	4%	4%	2%	10%	4%	2%	2%	5%	10%	3%	3%	6%	11%	4%
CraftCMS.SEOmatic.Template.Remote.Code.Injection	3%	4%	3%	5%	2%	3%	9%	2%	3%	2%	11%	4%	2%	2%	5%	8%	4%	3%	6%	10%	3%
Apache.Flink.JobManager.Arbitrary.Path.Traversal	3%	4%	2%	4%	2%	3%	8%	3%	3%	2%	11%	3%	1%	3%	4%	7%	3%	2%	6%	10%	3%
Apache.Struts.OGNL.BeanMap.Remote.Code.Execution	3%	4%	2%	4%	2%	3%	8%	3%	3%	3%	11%	4%	2%	2%	4%	7%	2%	2%	5%	10%	4%
FreePBX.Remote.Admin.Authentication.Bypass	2%	3%	2%	3%	2%	3%	9%	3%	3%	2%	6%	3%	2%	3%	5%	9%	3%	2%	5%	11%	4%
Citrix.XenMobile.Server.sbFileName.Arbitrary.Path.Traversal	2%	4%	2%	5%	2%	3%	7%	2%	2%	2%	11%	3%	2%	2%	5%	6%	3%	2%	5%	10%	3%

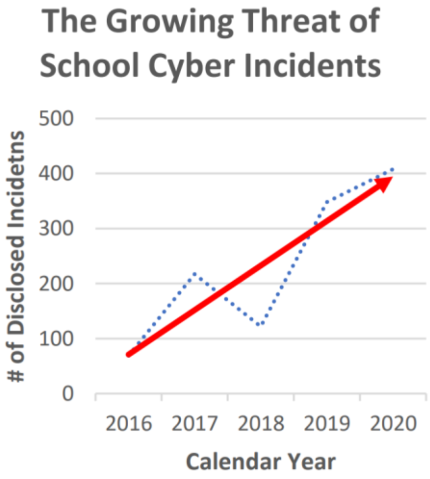
Targeted cyberattacks on schools and libraries continue to rapidly increase. The K-12 Cybersecurity Resource Center—"the most complete source of information on K-12 data breaches" according to the Government Accountability Office—found *a 491% increase in school cyber incidents*[8] *between 2016-2020.*[9] Figure 2 depicts this disturbing trend.

[7] *Id.* at 5.

[8] A cybersecurity incident is an event that actually or potentially jeopardizes a system or the information it holds.

[9] Douglas A. Levin, *The State of K-12 Cybersecurity: 2020 Year in Review*, K-12 Cybersecurity Resource Center and the K12 Security Information Exchange (Mar. 10, 2021), at 1, 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 . . . .") ("*State of K-12 Cybersecurity 2020*").

Figure 2: Reported U.S. K-12 Cyber Incidents, 2016 – 2020



The Center for Internet Security, which operates the Multi-State Information Sharing and Analysis Center ("MS-ISAC"), expects that school cybersecurity incidents could increase by 86% *this year*.[10] Moody's Investors Service says the rate of *attacks on schools has "increased exponentially"* since it began tracking cyberattacks in 2018.[11]

Our nation's law enforcement and security agencies have repeatedly identified rapidly increasing, targeted cyberattacks as threats to K-12 schools. A recent CISA blog post reports that, "[i]n August and September, *57% of ransomware incidents reported to the MS-ISAC involved K-12 schools*, compared to 28% of all reported ransomware incidents from January through July."[12] Earlier this year, the FBI issued a flash advisory that "ransomware targeting

[10] Benjamin Freed, *Cyber incidents against K-12 schools expected to rise by 86%*, EDSCOOP (Aug. 5, 2021), https://bit.ly/3lPzxVS (emphasis added); *see also* Joseph Marks, *The Cybersecurity 202: Schools are another prime ransomware target*, WASHINGTON POST (July 12, 2021), https://wapo.st/3u8hDS3.

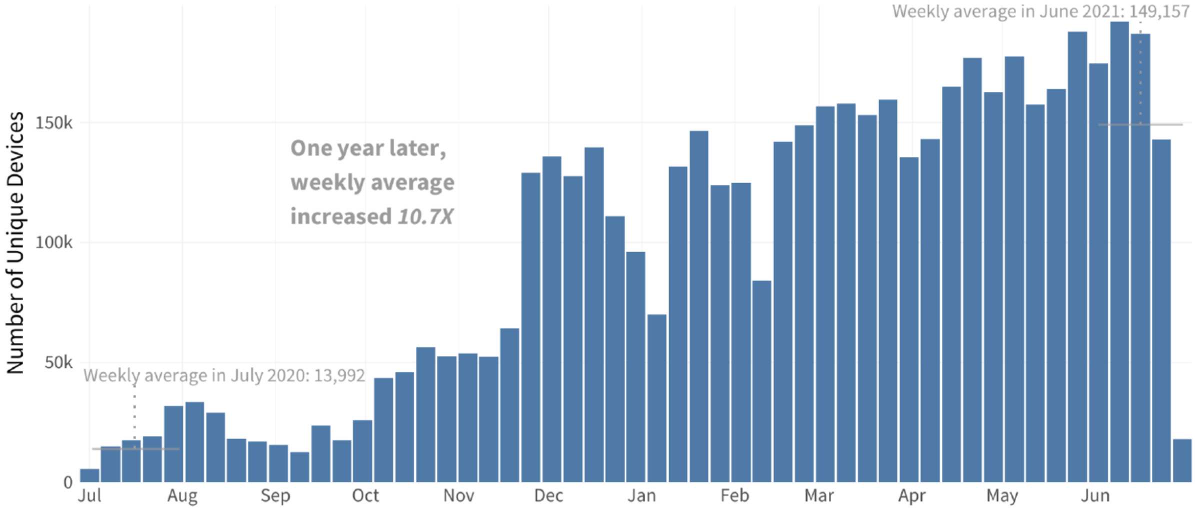
[11] Nic Querolo and Shruti Singh, *Schools Brace for More Cyberattacks After Record in 2020*, BLOOMBERG (Aug. 9, 2021), https://bloom.bg/3l2xFJ2 (emphasis added) ("*Schools Brace for More Cyberattacks After Record in 2020*").

[12] Eric Goldstein, Back to School Campaign, CISA (Aug. 9, 2021), https://bit.ly/3hgO8be (emphasis added).

education institutions in 12 US states and the United Kingdom . . . specifically target[ing] higher education, K-12 schools, and seminaries . . . . [is being used] to exfiltrate data from victims prior to encrypting victim's systems to use as leverage in eliciting ransom payments."[13]

These trends will only worsen. The first six months of 2021 saw a surge in the volume and sophistication of attacks targeting individuals and organizations.[14] For example, as Figure 3 shows, FortiGuard Labs found a tenfold increase in detected ransomware activity in just one year.

Figure 3: Growth in ransomware detections from July 2020 – June 2021[15]



The information technology trade publication TechRepublic confirms the escalating cadence of cyberattacks against schools: "For July 2021, schools and research facilities experienced an

[13] FBI Alert CP-000142-MW, FBC (Mar. 16, 2021), https://bit.ly/3hCphij.

[14] Derek Manky, *Critical Cyber Threat Landscape Insights from 2021 for CISOs*, Fortinet (Sept. 7, 2021), https://bit.ly/3kbsOpy.

[15] *See Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs*. Likewise, researchers at Cisco found a "48X increase in ransomware traffic in the K-12 space" between mid-July and December 2020. Austin, McBride, *CISA Reports: Increased ransomware attacks targeting K-12 school districts*, Cisco (Mar. 2, 2021), https://bit.ly/2X5NGWq.

average of 1,739 cyberattacks per organization each week. That volume showed a 29% increase from the first half of 2021."[16]

FortiGuard Labs outlines some of the most significant cybersecurity trends that the education sector needs to be aware of in the coming year:

- **IoT and CMS threats:** With nine of the top 10 exploits targeting IoT devices and content management systems ("CMS"), institutions should look out for vulnerabilities in these categories. Vulnerable CMSs can make soft targets for easy access into enterprise environments. Attackers are also seeking 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 (RaaS) 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.[17]

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 the right network security solutions, schools and libraries can detect, stop, and mitigate 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.

[16] Lance Whitney, *Education and research sector hit by highest number of cyberattacks in July*, TECHREPUBLIC (Aug. 18, 2021), https://tek.io/3CcdcZ6.

[17] Renee Tarun, *Threats Impacting Education Cybersecurity*, Fortinet (Mar. 30, 2021), https://bit.ly/3AlB5gl; *see also Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs.*

The necessity of remote learning has brought enduring changes in the way schools and libraries digitally serve the public. As educational networks evolve to deliver better learning experiences, school districts under-prioritize cybersecurity due to funding challenges. It is no surprise, then, that schools and libraries are prime targets for cybercriminals.

For schools systems, a cyberattack can be devastating. Cyberattacks have forced schools to cancel school days and[18] postpone classes.[19] Cybercriminals have destroyed student records[20] and stolen students' PII.[21] In a joint report with the K12 Security Information Exchange, the K-12 Cybersecurity Resource Center highlighted the severity of the problem, finding "many of these incidents were significant: resulting in school closures, millions of dollars of stolen taxpayer dollars, and student data breaches directly linked to identity theft and credit fraud."[22]

Indeed, one recent study of 39 ransomware attacks on U.S. schools found that "*schools suffered an average downtime of just under 7 days in 2020*."[23] CISA guidance reports that "[m]alicious cyber actors are targeting school computer systems, slowing access, and rendering the systems inaccessible to *basic functions*."[24] Another survey of 2020 ransomware attacks

[18] *See infra* note 27.

[19] Safia Samee Ali, *Miami-Dade Public Schools' remote learning platform endures days of cyberattacks*, NBC NEWS (Sept. 2, 2020), https://nbcnews.to/3hcK6Rf.

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

[21] *State of K-12 Cybersecurity 2020* at n.5 ("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 . . . .").

[22] *Id.* at 2.

[23] Paul Bischoff, *Ransomware attacks on US schools and colleges cost $6.62bn in 2020,* Comparitech (Aug. 31, 2021), https://bit.ly/39eFupv (emphasis added).

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

found that "many schools have been subject to double-extortion attempts where hackers not only lock them out of critical systems but steal data and threaten to post it online if the ransom isn't paid."[25]

Reported cyberattacks against schools and libraries in all 50 states confirm these expert findings.[26] One ransomware cyberattack shut down all Baltimore County Public Schools network systems, prompting the district to cancel classes for more than 115,000 students for multiple days.[27] Smaller school districts have been forced to shut down too. California Newhall School District was forced to cancel classes at 10 elementary schools serving 6,000 students due to a ransomware attack that disabled the district's server and email.[28] Investigative journalists at CBS Dallas-Ft. Worth "found in the past two years at least 67 school districts in Texas have suffered a cybersecurity breach."[29] In Broward County, Florida, cybercriminals published

[25] *See supra* note 23.

[26] *State of K-12 Cybersecurity 2020* at 12 ("For the 5-year period from 2016-2020, there were a total of 1,164 publicly-disclosed incidents involving 988 education organizations across all 50 states.").

[27] Jenny Fulginiti *et al.*, *Ransomware attack prompts Baltimore County Public Schools to close*, WBAL-TV (Nov. 25, 2020), https://bit.ly/3l5fgLL ("The superintendent said a timeline was not immediately known as to when students will return to class. . . . 'What has occurred is very disturbing. We have 115,000 students relying on us to provide education and other opportunities,' Board of Education Chairwoman Kathleen Causey said."). Other school systems have had to similarly shut. *See, e.g.*, *Cyber-attack concerns behind Norfolk canceling virtual classes on Monday*, WVEC-TV (Nov. 5, 2020), https://bit.ly/3BIFXME; Michael Gold, First Pandemic, Now Ransomware: Attack Forces Hartford to Postpone School, NY TIMES (Sept. 8, 2020), https://nyti.ms/3h9ruS2. The year before, Gov. Edwards of Louisiana declared a state of emergency before school even started due to ransomware attacks targeting three school systems within a week. Madeline Holcombe, *Louisiana's governor declares an emergency after cyberattacks on several school systems*, CNN (July 25, 2019), https://cnn.it/3yRWZX5.

[28] Andrew J. Campa, *Ransomware attack hits Newhall schools, halting online classes*, LA TIMES (Sept. 15, 2020), https://lat.ms/3o51HyT.

[29] Brian New, *Has Your Kid's Texas School District Been Hammered By Cyberattacks? I-Team Investigation*, CBS DFW (Aug. 16, 2021), https://cbsloc.al/3uba6BP.

thousands of stolen files, including some confidential information, after district officials refused to pay a $40 million ransom.[30] And just last month, the Boston Public Library "experienced a systemwide technical outage due to a cybersecurity attack, pausing public computer and public printing services, as well as some online resources."[31] In sum, the past two years show that network security solutions are *necessary* for schools' and libraries' internal networks, which are, in turn, necessary for the basic functioning of schools and libraries.

Schools and libraries are not the only victims of cyberattacks: data breaches can gravely injure students, teachers, and staff years after the fact. Individuals use school and library systems to complete and submit homework, attend lectures, participate in extracurricular activities, schedule transportation, and perform administrative functions necessary for school and library operations. To enable these basic public services, school IT systems must collect and manage sensitive data about students, their parents, guardians, and families, educators, other school staff, and school district operations. The large amounts of financial and PII that must be protected include banking information, health data, and Social Security numbers.[32]

This rich trove of PII makes schools and libraries attractive targets for criminals: "In 2021, ransomware gangs published data from more than 1,200 American K-12 schools."[33] In February, after a data breach of Toledo Public Schools systems led to the disclosure of students'

[30] *Schools Brace for More Cyberattacks After Record in 2020*.

[31] Marc Fortier, *Boston Public Library Hit by Cyberattack*, NBC Boston (Aug. 27, 2021), https://bit.ly/3lWNaTd.

[32] Indeed, federal and state policymakers understand how important it is to secure students' PII. Laws like the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232G, Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501 *et seq.*, and the California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100 *et seq.*, among others, underscore the federal and state policy of protecting the privacy of children.

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

and staff members' names and Social Security numbers, cybercriminals began using the information to open up credit card accounts and apply for car loans.[34]

C. Cybersecurity Is Unaffordable for Many School Districts.

Budget constraints mean schools and libraries face greater cybersecurity challenges than in other industry sectors. In a joint advisory with the FBI and MS-ISAC, CISA noted that cybersecurity "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."[35] By allowing E-Rate eligibility for network security solutions, the Commission can help school administrators avoid making either-or choices between necessary network protections.

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. Rural districts and schools with lower headcounts may face special disadvantages because smaller student populations mean lower scale economies for IT staffing. Lean IT teams often find it difficult to meet the growing demands of security for K-12 school districts—many of which do not have a dedicated cybersecurity employee—while also supporting day-to-day operations. In a recent survey of 170 school IT leaders, respondents said cybersecurity was their

[34] Shaun Hegarty, *Toledo Public School students seeing effects of massive data breach*, WTVG (Feb. 22, 2021), https://bit.ly/3luOg8C.

[35] 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 ("CISA K-12 JCA").

top unmet technology need—"by a large margin."[36] One survey respondent said the need for more cybersecurity funding was "desperate."[37]

Private organizations are stepping up to do their part. For example, to address the cybersecurity skills gap, Fortinet recently pledged to train 1 million people globally over the next five years through its Training Advancement Agenda ("TAA") initiatives and Network Security Experts ("NSE") Training Institute programs.[38] Fortinet's TAA initiative includes a strong focus on attracting greater diversity through the NSE Security Academy Program, Education Outreach Program, and Veterans Program as part of its Corporate Social Responsibility efforts.

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. For under-resourced schools and libraries, investing in cybersecurity can be an almost impossible challenge, leading to large cybersecurity inequities. These inequities can widen even further when cyberattacks do occur. For example, the school district in Scott County, KY (which has a population of less than 60,000) lost $3.7 million as a result of a phishing scam.[39] Local governments are finding that the cost of borrowing is increasing because of cybersecurity

[36] *EdTech Trends 2021 Members: Share Their Experiences*, The Consortium for School Networking, https://bit.ly/3n9GDXF.

[37] *Id.* After receiving more than 250 applications from U.S. K-12 school districts for cybersecurity funding grants, one cybersecurity grant program found that "50% of applicants had less than $100,000 for cybersecurity spending – for the entire school district" and "[m]ore than 55% of school districts are operating without security training." Press Release, IBM, *IBM Selects Six School Districts to Receive a Total of $3 Million in Education Security Preparedness Grants* (June 6, 2021), https://ibm.co/3nbyfH0.

[38] 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.

[39] *Scott County Schools victim of $3.7 million scam*, WKYT (Apr. 24, 2019), https://bit.ly/3AfxSyT.

threats.[40] And if a ransomware attack occurs, schools and libraries may be forced to choose between protecting their networks and data and paying multi-million-dollar ransoms.

Cybersecurity for K-12 schools and libraries requires a unified, cost-effective solution to connect and secure their networks. An integrated approach—beyond basic firewalls—can both alleviate the strain on lean IT teams and help them achieve their ultimate goal—delivering a network that streamlines education while securing school networks and students. By including E-Rate eligibility for network security solutions, the Commission can empower schools and libraries with the flexibility to connect and secure their networks with these much-needed tools.

III. CLARIFYING THAT NETWORK SECURITY AND MONITORING SERVICES QUALIFY FOR E-RATE SUPPORT WILL BETTER PROTECT SCHOOL AND LIBRARY NETWORKS.

The Bureau can assist schools and libraries in maximizing their Category Two E-Rate funding by clarifying the scope of the FY2022 E-Rate ESL. In particular, the Bureau can include network security solutions in the ESL by: (1) expressly enumerating the types of network security solutions that would meet the definition of "basic maintenance of eligible broadband internal connections"; *or* (2) adding a new note clarifying that "firewall services and firewall components" include "network security solutions."

"Eligible schools and libraries may seek E-Rate support for eligible Category One telecommunications services, telecommunications, and Internet access, and Category Two internal connections, basic maintenance, and managed internal broadband services."[41] The

[40] *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.").

[41] *FY2022 E-Rate ESL PN*, Attachment at 1; *see also* 47 C.F.R. §§ 54.501 *et seq.*

"basic maintenance of internal connections" subcategory does not include network security solutions, although the category includes technical support and security patches. "Firewall services and firewall components" are E-Rate-eligible as part of the "internal connections" subcategory.

The Bureau has ample legal authority to address the dearth of E-Rate funding for critical "network security solutions,"[42] as discussed below. First, the Commission has delegated to the Bureau the authority to clarify that network security solutions qualify as "basic maintenance" in the ESL. For the same reasons, the Bureau can alternatively determine that network security solutions fall into the ESL's reimbursable subcategory of "[f]irewall services and firewall components."

A. The Proposed ESL Does Not Identify Network Security Solutions as E-Rate-Eligible.

"Firewall and firewall components" are the only network security-related items expressly listed in the draft ESL. Although the Commission has not defined E-Rate-eligible "firewall services and firewall components," that category appears to be limited to basic port protection, that is, the monitoring of traffic traveling across the perimeter of a network.

Before the FY2015 ESL proceeding, E-Rate ESLs included an extensive glossary of terms that applicants could rely on. 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.[43] The USAC ESL

[42] As noted above, *see* supra note 3, "network security solutions" includes (1) next-generation firewalls, (2) endpoint protection and detection, such as anti-malware software, (3) advanced security services like multi-factor authentication qualify, and (4) such other services that meet the emerging threats that schools and libraries face.

[43] *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

glossary defines “firewall” 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.”[44]

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.[45] Basic firewalls alone cannot protect against these attacks. Nor can these basic firewalls mitigate the damage caused.[46]

By contrast, next-generation firewalls often do so much more than merely fencing 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:

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.”).

[44] *Schools and Libraries (E-Rate) Program: Eligible Services List (ESL) Glossary*, Universal Service Administrative Company, https://bit.ly/2Vtmf8i (last visited Sept. 9, 2021).

[45] CISA K-12 JCA.

[46] *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 . . . .”).

- 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
- 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 profile profiles[.][47]

Endpoint protection and detection, such as anti-malware software, guard network endpoints against being harmed or coopted to cause harm. Advanced+ security further limits the vectors of attack and would include measures like DNS server security, filtering of malicious websites, and multi-factor authentication.

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.[48] This eliminates the need for school districts to deploy and manage separate tools, such as a secure web gateway or intrusion prevention system. 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 network security solutions, aside from "firewall services and firewall components," are E-Rate eligible. The Commission, however, "le[ft] the

[47] *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/3u0AgHp.

[48] *See Charting the Security Journey for K-12 Schools*, Fortinet, https://bit.ly/3uds2f5 (last visited Sept. 24, 2021).

record open on these services to allow for further comment."[49] Indeed, the *First E-Rate Modernization R&O* noted 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.'"[50] 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 covered services to maximize funding for other internal connections components and services.[51]

While the Commission in 2019 found that adding network security solutions was not "truly necessary to deliver high-speed broadband to students and library patrons," it left open the prospect of revisiting that determination in the future.[52] 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*.[53]

[49] *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 . . . .").

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

[51] *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).

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

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

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 network security solutions as an integral component of schools' and libraries' educational purposes. Keeping E-Rate funds from being used for network security solutions could counterproductively undercut the utility of each dollar spent for school and library connectivity. A robust internal network means very little for a school that cannot access its own systems and data due to a cyberattack. In short, if the Commission intends to spend money building networks, it needs to spend money securing networks.[54]

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."[55] 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. In previous ESL decisions, Bureau has acted to update E-Rate eligibility through clarifications on the scope of covered services.[56] Indeed, the

[54] *Id.* ¶ 46.

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

[56] *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-

Commission has made clear that the Chief of the Bureau possesses the authority to interpret the Commission's E-Rate rules,[57] an authority the Commission reaffirmed in 2019.[58] Thus, the Bureau possesses the expressly delegated authority to update the ESL by clarifying that network security solutions are eligible for E-Rate support.

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

Permitting schools and libraries to use Category Two funding for necessary network security solutions will not deplete funding for E-Rate services. 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 on how to best use a fixed amount of funding to connect and secure their networks without depleting E-Rate funding.[59]

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.").

[57] *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.").

[58] *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.*).

[59] *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.").

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

> 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.[60]

The Commission affirmed this approach in 2019 by making permanent the five-year budget model for Category Two funding.[61]

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 network security solutions. 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" network security solutions "given these limits on the total amount available."[62] 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.

Recent congressional activity in response to the COVID-19 pandemic highlights the importance of funding for cybersecurity. Congress has authorized some support for cyber, but

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

[61] *Category Two R&O* ¶ 45.

[62] *See supra* note 60.

those funds are generally non-recurring, one-time expenditures rather than ongoing support needed to respond to an ever-evolving threat environment. Schools may not even know that some funding has been made available to them. Congresswoman Matsui and Congressman Langevin recently urged the Department of Education to issue guidance clarifying that the cost of cybersecurity solutions be treated as eligible "education technology" costs under various COVID-19 support programs.[63] These congressional efforts underscore the need for a self-sustaining solution. The Commission has the legal authority to act now to close the cybersecurity gap facing underserved schools and libraries. The Bureau can help the Commission follow Congress's lead by clarifying that Category Two funds may be used for network security solutions.

V. CONCLUSION

School and library networks are under siege by cyberattacks. Since the Commission last visited the issue, the rate of attacks has increased by orders of magnitude and shows no sign of slowing down. The Commission delegated to the Bureau the authority to update the E-Rate ESL based on changed circumstances. Network security solutions are critical to the basic functioning of school and library networks and to protect sensitive financial information and PII. Given how crucial these tools have become for the basic functioning of E-Rate applicants' internal networks, the Bureau should clarify that Category Two E-Rate funds can be used for network security solutions. Doing so would follow both the Commission's E-Rate modernization efforts and

[63] Letter from Doris Matsui and Jim Langevin, Members, Congress, to Secretary Miguel Cardona, U.S. Department of Education (dated Apr. 1, 2021) ("We encourage you to issue immediate guidance to clarify that cybersecurity expenses are allowed under the [Elementary and Secondary School Emergency Relief Fund and the Governor's Emergency Education Relief Fund].").

Congress's very high prioritization placed on cybersecurity issues. Finally, updating Category Two eligibility would not risk depleting E-Rate funding because Category Two funds are fixed.

Respectfully submitted,

/s/ Robert A. Turner

Robert A. Turner,
Field Chief Information Security
Officer – Education
FORTINET, INC.
899 Kifer Road
Sunnyvale, CA 94086

September 27, 2021