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

PETITION FOR DECLARATORY RELIEF AND PETITION FOR RULEMAKING ALLOWING ADDITIONAL USE OF E-RATE FUNDS FOR K-12 CYBERSECURITY

CONSORTIUM FOR SCHOOL NETWORKING
Keith Krueger, CEO

ALLIANCE FOR EXCELLENCE IN EDUCATION
Phillip Lovell, Vice President

STATE EDUCATIONAL TECHNOLOGY DIRECTORS ASSOCIATION
Julia Fallon, Executive Director

COUNCIL OF THE GREAT CITY SCHOOLS
Michael Casserly, Executive Director

STATE E-RATE COORDINATORS' ALLIANCE
Debra Kriete, Chair

SCHOOLS, HEALTH & LIBRARIES BROADBAND COALITION
John Windhausen, Jr., Executive Director

February 8, 2021

Executive Summary

Pursuant to §1.2 and §1.401(a) of the Commission's Rules ("Rules") the above-named petitioners ("Petitioners") respectfully ask the Commission to modernize the Schools and Libraries Program ("E-rate") by: (1) defining all firewall and related features as "basic" beginning in funding year 2021; (2) increasing the five-year Category 2 budget cap in future funding years to support needed additional cybersecurity investments; and (3) updating the agency's broadband definition to include cybersecurity.

The Federal Bureau of Investigation, Department of Homeland Security, and the Multi-State Information Sharing and Analysis Center report that K-12 cyberattacks are not only persistent and expanding, but they also constituted a majority (58%) of all ransomware attacks in August and September 2020. Cyberattacks have become so pronounced that they represent a material threat to the educational broadband access that Congress intended to facilitate through the E-rate program. Across the country, recent cyberattacks have robbed students and teachers of invaluable instructional time, limited school districts' abilities to operate, and breached the confidential personally identifiable information of students and staff. The problem is expanding at a time when school districts, forced by the COVID-19 pandemic, are teaching tens of millions of students online while wrestling with varying levels of economic uncertainty. Schools require assistance to combat this multifaceted and highly technical problem.

Consistent with the Commission's criteria for determining the non-telecommunications services to be covered by the E-rate, the program changes requested by this petition are necessary to ensure continued consistent delivery of high-speed broadband service to schools. The Commission must add cybersecurity to the E-rate program not only to achieve the Communications Act's ("Act") call to "enhance access" to educational broadband but to preserve such access and promote the public interest. As described in greater detail by the petition, the Act provides the Commission with clear authority to specify the E-rate program's services and supports. This authority is consistent with Congress's recognition that achieving the Act's broadband connectivity goals requires the Universal Service Fund programs, including E-rate, to adjust alongside evolving technologies and needs.

With cyberattacks threatening the broadband networks and data of schools, including the school systems serving some of the country's most economically and academically vulnerable students, the Commission must update the E-rate program to cover firewalls and related features. The Commission must also provide schools with a sufficient level of investment to address this need, as described by the petition and the attached cost estimate, consistent with the program's longstanding and successful need-based structure. Achieving broadband equity for students will not be possible if school networks and sensitive student and employee data remain at the mercy of cyber-attackers. The Commission should address this need expeditiously to help schools prevent further attacks during the expanded remote learning required by the pandemic.

Table of Contents

PETITION FOR DECLARATORY RELIEF AND PETITION FOR RULEMAKING ALLOWING ADDITIONAL USE OF E-RATE FUNDS FOR K-12 CYBERSECURITY

The Consortium for School Networking, the Alliance for Excellent Education, the Council of the Great City Schools, the Schools, Health, & Libraries Broadband Coalition, the State Educational Technology Directors Association, and the State E-rate Coordinators' Alliance, pursuant to §1.2 and §1.401(a) of the Commission's Rules ("Rules"), hereby petition the Commission to initiate a rulemaking to amend Part 54 of the Rules to update the Schools and Libraries Program of the Universal Service Fund (Rules are found at Part 54 Subpart F (Section 54.5 et seq.). The Petitioners respectfully urge the Commission to strengthen the Schools and Libraries Program ("E-rate") by adopting an expanded focus on protecting schools from the rising tide of cyberattacks threatening their networks and confidential data.[1] Specifically, Petitioners encourage the Commission to: (1) define all firewall and related features as "basic" beginning in funding year 2021; (2) increase the five-year Category 2 budget cap in future funding years to support needed additional cybersecurity investments; and (3) update the agency's broadband definition to include cybersecurity. In order to implement relief immediately for FY 2021, petitioners also request that the Commission issue a declaratory order or waive the Eligible Services List adopted pursuant to Section 54.502(a)(2) of the Rules to allow for firewalls to be fully eligible for Category 2 funding in FY 2021 without the need to perform cost-allocation of embedded features that previously were considered "further network security services" over six years ago when the Commission adopted its 2014 Modernization Orders.[2] In support thereof, Petitioners respectfully submit the following:

[1] While this petition focuses on school network security issues, the petitioners readily acknowledge that libraries confront the same challenges.

[2] Modernizing the E-rate Program for Schools and Libraries, WC Docket No. 13-184, Report and Order and Further Notice of Proposed Rulemaking, 29 FCC Rcd 8870, 8933 para. 121 n. 275 (2014), ("*July 2014 Modernization*

I. INTRODUCTION

The Consortium for School Networking ("CoSN") is a 501(c)(3) professional association for school system technology leaders. CoSN provides thought leadership resources, community, best practices and advocacy tools to help leaders succeed in the digital transformation. CoSN represents over 13 million students in school districts nationwide. The Council of the Great City Schools ("Council") is the only national organization exclusively representing the needs of urban public schools. Composed of 76 large city school districts, the Council's mission is to promote the cause of urban schools, advocate for inner-city students, and build capacity in urban education with programs to boost academic performance and narrow achievement gaps; improve professional development; and strengthen leadership, governance, and management. The State Educational Technology Directors Association ("SETDA") is a 501(c)(3) not-for-profit membership association launched by state education agency leaders in 2001 to serve, support and represent their emerging interests and needs with respect to the use of technology for teaching, learning, and school operations. The State E-rate Coordinators' Alliance ("SECA") is a 501(c)(3) nonprofit professional association for state E-rate coordinators who support applicants across the country. SECA members, representing 40 states and two territories, provide year-round E-rate training, technical assistance and helpdesk support to school, library and consortium applicants to facilitate their success with obtaining E-rate funding and complying with program rules. The Schools, Health & Libraries Broadband ("SHLB") Coalition is a nonprofit, 501(c)(3) advocacy organization that strives to close the digital divide by promoting high-quality broadband for

Order"). The Commission declined to make eligible "further network security services and other proposed services." Footnote 275 clarified that these services and features included "intrusion protection and detection, malware protection, application control, content filters, DDoS mitigation, and Unified Threat Management technology … DDOS, cybersecurity services, and cloud storage … traffic shaping appliances, network security management, and more."

anchor institutions and their communities. Our members include a diverse mix of over 175 commercial and nonprofit organizations who support our mission. The Alliance for Excellent Education's ("All4Ed") Future Ready Schools initiative works with school and district leaders to implement student-centered learning strategies to target existing inequities; remedy disparities in in-school and out-of-school technology access; and use technology to create equitable learning opportunities for all students.

Cyberattacks on schools have grown steadily in recent years, including a surge of new attacks in 2020 as tens of millions of students transitioned to full-time or part-time online learning as a result of the COVID-19 pandemic. These costly attacks caused lost instructional time, hamstrung administrative activities, compromised confidential data, and severely harmed school budgets. Given the persistent and increasing number of these attacks, and consistent with the Commission's criteria for determining the non-telecommunications services to be covered by the E-rate, Petitioners believe the policy and regulatory changes requested by this petition are now absolutely necessary to ensure continued delivery of high-speed broadband service to schools and students. Broadband must no longer be deemed to be sufficient by regulators and policymakers if it is not secure.

II. SCHOOLS FACE PERSISTENT AND EXPANDING CYBERATTACKS THAT THREATEN THEIR NETWORKS, DISRUPT INSTRUCTION AND OPERATIONS, AND RISK DISCLOSURE OF CONFIDENTIAL STUDENT AND EMPLOYEE DATA.

Cyberattacks pose a serious threat to school districts' networks, the continuity of classroom instruction and administrative operations, sensitive student and employee data, and budgets. The Federal Bureau of Investigation ("FBI"), the Cybersecurity and Infrastructure

Security Agency ("CISA"), and the Multi-State Information Sharing and Analysis Center ("MS-ISAC") published an alarming Joint Cybersecurity Advisory ("JCA") in December 2020 that concisely describes the frightening cybersecurity problem confronting the nation's schools. The JCA confirms what many school district and state education leaders regrettably know from direct experience; "cyber actors are targeting kindergarten through twelfth grade (K-12) educational institutions, leading to ransomware attacks, the theft of data, and the disruption of distance learning services."[3]

Perhaps most troubling, cyber attackers are disproportionately focused on schools and use a variety of criminal strategies to target them. Cyberattacks on K-12 entities not only worsened in 2020, but they also recently represented a majority of all ransomware attacks. The JCA notes that the "percentage of reported ransomware incidents against K-12 schools increased at the beginning of the 2020 school year. In 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." Private sector experts confirm cyber attackers focus on education. Microsoft Security Intelligence data reported in January 2021 lists education as the most affected industry subject to malware attacks in the last 30 days.[4] Ransomware and malware are not the only serious problem facing education entities, schools are also routinely subject to distributed denial of service attacks, social engineering (e.g., phishing schemes), and video conferencing disruptions.[5]

[3] Joint Cybersecurity Advisory, Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data, FBI, CISA, and MS-ISAC, p.1 (Dec. 2020), available at https://us-cert.cisa.gov/ncas/alerts/aa20-345a.

[4] Microsoft Security Intelligence, Global Threat Activity, https://www.microsoft.com/en-us/wdsi/threats (last visited Jan. 21, 2021).

[5] Joint Cybersecurity Advisory at pp. 1-3.

Cyber-attackers' alarming focus on schools may, in part, be attributable to the massive expansion of virtual learning during the COVID-19 pandemic, but it is not a new problem. The U.S. Census Bureau reports that nearly 93% of households with school-age children report some form of distance learning during the pandemic, which has created new network vulnerabilities that are well known to hackers.[6] The growing number of cyberattacks on schools, however, is also consistent with pre-pandemic trends. For example, the K-12 Cybersecurity Resource Center reported that the number of K-12 cybersecurity incidents nearly tripled from 2018 to 2019.[7] The trend is also consistent with the longstanding concerns expressed by the school district technology professionals that are responsible for managing the vast array of networks and devices that support instructional and administrative operations in schools. CoSN's *2020 State of Ed Tech Leadership Report*, a national survey of school district technology leaders, found that cybersecurity remains technology leaders' number one priority for the third straight year.[8]

Recent attacks on large, medium, and small school districts show how disruptive and costly they can be for school administrators, teachers, and students. A ransomware attack on the Baltimore County Public School system in November 2020 caused a multiday, districtwide shutdown affecting 115,000 students.[9] The district's closure was temporary but viewed in aggregate the lost days amounted to thousands of hours of lost instructional time for students. In September, hackers published highly sensitive data, including employee Social Security numbers and student grades, held by the 320,000 student Clark County School District in Las Vegas,

[6] Schooling During the COVID-19 Pandemic, U.S. Census Bureau, available at https://www.census.gov/library/stories/2020/08/schooling-during-the-covid-19-pandemic.html.

[7] Levin, Douglas A., "The State of K-12 Cybersecurity: 2019 Year in Review," Arlington, VA: EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center (2020), available at: https://k12cybersecure.com/year-in-review/.

[8] The State of Ed Tech Leadership in 2020, CoSN, available at https://www.cosn.org/focus-areas/leadership-vision/state-edtech-leadership.

[9] Paybarah, Azi, "Ransomware Attack Closes Baltimore County Public Schools," The New York Times (Nov. 29, 2020), https://www.nytimes.com/2020/11/29/us/baltimore-schools-cyberattack.html.

Nevada.[10] The loss of this sensitive data may plague students and teachers for years to come. In March 2020, the Sheldon Independent School District in Houston, Texas paid $206,931 in bitcoin in response to a ransomware attack. Despite the payment, the 10,000-student district was ultimately unable to recover about 10% of its files.[11] Attackers also threaten some of the nation's smallest school districts. In March 2020, Mitchell County Schools, located in rural North Carolina, was subject to a ransomware attack. By August of 2020, four additional North Carolina school districts were subject to similar attacks.[12] These troubling, costly attacks are just a few striking examples among hundreds of others that occurred in recent years.[13]

III. LOW INCOME COMMUNITIES FACE A CYBERSECURITY EQUITY GAP AND THE PANDEMIC CAUSED ECONOMIC DOWNTURN IS MAKING IT MORE DIFFICULT FOR ALL SCHOOL DISTRICTS TO PROTECT THEIR NETWORKS

School districts often do not have the significant resources required to defend their networks from sophisticated cyberattacks. Schools in lower wealth communities are at a particular disadvantage relative to their better resourced peers when it comes to assembling the technical, human, and other safeguards that are part of a multifaceted cybersecurity strategy. The FBI, CISA, and MS-ISAC published JCA recognizes that many schools face resource constraints

[10] Hobbs, Tawnell D., "Hacker Releases Information on Las Vegas-Area Students after Officials Don't Pay Ransom," The Wall Street Journal (Sept. 28, 2020), https://www.wsj.com/articles/hacker-releases-information-on-las-vegas-area-students-after-officials-dont-pay-ransom-11601297930.

[11] Hobbs, Tawnell D, and Justin Clemons, "Schools Struggling to Stay Open Get Hit by Ransomware Attacks," The Wall Street Journal (Nov. 13, 2020), https://www.wsj.com/articles/my-information-is-out-there-hackers-escalate-ransomware-attacks-on-schools-11605279160.

[12] Gordon, Brian, "Rise of Ransomware Attacks on NC Schools Hinder Virtual Learning," The Asheville Citizen Times (Aug. 28, 2020), https://www.citizen-times.com/story/news/local/2020/08/28/ransomware-cyberattacks-nc-schools-rise-during-covid-19-pandemic/5644879002/.

[13] Levin, Douglas A., "The State of K-12 Cybersecurity: 2019 Year in Review," Arlington, VA: EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center (2020), available at https://k12cybersecure.com/year-in-review/.

that hinder their cybersecurity practices. The advisory notes that "[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."[14] For the nation's poorest school districts, making these investments is not just challenging but almost impossible; creating a serious cybersecurity gap between wealthy and poor communities that mirrors other educational opportunity gaps.

Schools' cybersecurity equity problems may be compounded by the serious ongoing economic challenges facing states as a result of the ongoing pandemic. Writing in January 2021, the National Conference of State Legislators said, "[t]he COVID-19 pandemic had a big impact on state budgets. Economic shutdowns led to severe revenue reductions as commerce slowed and businesses shuttered." The national group added, "as COVID-19 continues to spread in the United States, the pandemic shows no sign of abating until later in 2021, when most Americans are expected to have received vaccines. More revenue uncertainty lies ahead for state budgets."[15] The significant federal emergency assistance provided to school districts by the CARES Act (P.L.116-136) and the Consolidated Appropriations Act, 2021 (P.L. 116-260) has helped to soften the educational and administrative blow of the economic downturn. However, additional state economic problems on the horizon may make it even harder for school districts to fend off future cyberattacks because schools receive about half (47%) of their funding from state tax revenues.[16]

[14] Joint Cybersecurity Advisory at p. 1.

[15] Cantlon, McKenzie, "Rainy Days Are Here: States Tap Reserve Funds to Plug Budget Holes," National Conference of State Legislators (Jan. 11, 2021), available at https://www.ncsl.org/research/fiscal-policy/rainy-days-are-here-states-tap-reserve-funds-to-plug-budget-holes.aspx.

[16] Public School Revenue Sources, National Center for Education Statistics (updated April 2020), available at https://nces.ed.gov/programs/coe/indicator_cma.asp.

IV. THE COMMISSION SHOULD UPDATE THE E-RATE ELIGIBLE SERVICES LIST TO DEFINE ALL FIREWALL AND RELATED FEATURES AS "BASIC" BEGINNING IN FUNDING YEAR 2021, INCREASE THE E-RATE CATEGORY 2 BUDGET CAP, AND ADOPT A NEW BROADBAND DEFINITION INCLUSIVE OF CYBERSECURITY

The E-rate program provides a logical and practical way to help schools enhance their cybersecurity. The E-rate already helps most schools across the United States acquire broadband access, including subsidizing basic firewalls, so it is natural outlet for this assistance. School leaders are also well versed in using the E-rate, including using the program's forms, procedures, and deadlines. Furthermore, the Communications Act clearly provides the Commission with the authority required to make this desperately needed program change.

The E-rate presently covers basic firewall services and firewall components separate from basic firewall protection when provided as a standard component of a vendor's Internet access service.[17] The Commission noted in the July 2014 E-rate Modernization Report and Order and Further Notice of Proposed Rulemaking that firewall services are "necessary to ensure delivery of high-speed broadband services." Specifically, the Commission said,

> *In order to help deploy LANs/WLANs necessary to permit digital learning in schools and libraries throughout the nation, we focus the category two ESL on broadband. With one narrow exception, we limit internal connections support to those broadband distribution services and equipment needed to deliver broadband to students and library patrons: routers, switches, wireless access points, internal cabling, racks, wireless controller systems, firewall services, uninterruptable power supply, and the software supporting each of these components used to distribute high-speed broadband throughout school buildings and libraries. Some form of each of these services has previously been designated as eligible for E-rate support, and we find they are necessary to ensure*

[17] *See* Schools and Libraries Program 2021 Eligible Services List, available at https://docs.fcc.gov/public/attachments/DA-20-1418A1.pdf.

delivery of high-speed broadband services to students and library patrons via LANs/WLANs.[18]

Sections 254(c)(1), (c)(3), (h)(1)(B), and (h)(2) of the Communications Act provides the Commission authority to specify the services that will be supported for eligible schools and libraries and to design the specific mechanisms for support.[19] The Commission noted in the *July 2014 Modernization Order*, "[t]his authority reflects Congress's recognition that technology needs are constantly 'evolving' in light of 'advances in telecommunications and information technologies and services.'"[20] This includes non-telecommunications services such as firewalls and other cybersecurity protections. The Commission said in the *July 2014 Modernization Order*, consistent with the authority provided by the Act, that it "…reasoned that such services enhance access to advanced telecommunications and information services for public and non-profit elementary and secondary school classrooms and libraries." The Commission noted in the *July 2014 Modernization Order* that it adopted a narrow vision of covered services to maximize support for connectivity investment, but the rising tide of cyberattacks make cybersecurity among the components the Commission should now consider "needed to deliver broadband to students" and that "are essential to education, public health, or public safety."[21]

Thus, given the dramatic increase in cyberattacks on schools since the 2014 E-rate modernization, the Commission must add cybersecurity to the E-rate program not only to "enhance access" to educational broadband but to preserve such access. Preventing cyberattacks must be a core E-rate focus with the program alongside efforts to provide high speed

[18] July 2014 Modernization Order, 29 FCC Rcd 8870, 8917 para. 119.
[19] 47 U.S.C. §§ 254(c)(1), (c)(3), (h)(1)(B), (h)(2).
[20] July 2014 Modernization Order, 29 FCC Rcd 8870, 8895 para. 67.
[21] July 2014 Modernization Order, 29 FCC Rcd 8870, 8917 para. 119; 47 U.S.C. § 254(c)(1)(A).

connectivity. Absent such protections, the connectivity will not meet the needs of the schools and students Congress designed E-rate to serve.

Thus, the Commission should update E-rate to cover cybersecurity and direct the Universal Service Administration Company to treat all firewall components as "basic" beginning in funding year 2021 and allow for E-rate to fully fund firewall devices and services without requiring any cost-allocation.[22] This clarification will have no financial impact to the program but will allow applicants to have more flexibility in managing their Category 2 budgets.

In addition to treating all firewall components as "basic", the Commission should issue a notice of proposed rulemaking seeking comments on the E-rate eligibility of advanced security measures and increasing the five-year Category 2 budget cap for the purpose of covering all firewall components in future funding years.

This requested budget cap increase is based on a detailed cost estimate published by CoSN and Funds for Learning in January 2021, which is attached as an addendum to this petition. The report concludes that to cover the costs of basic firewalls in the Category 2 program, an additional $81 per student is required to be added to the per-student budget multiplier. The cost estimate is based on an analysis of the third-party hardware, software, and cloud-based services required to protect schools from attacks. The paper organizes the security measures into three "layered categories which build upon one another: (1) next-generation firewalls, (2) endpoint protection, such as anti-malware software, and (3) advanced+ services, such as multi-factor authentication." "The cost to offer discounts on the three levels of

[22] July 2014 Modernization Order, 299 FCC Rcd 8870, 8895 para.68. While in 2014 the named "network security services" in the *First Modernization Order* may have been separate services and devices, the technology has evolved to embed many of these features within firewalls. The distinction between network security services and firewalls no longer stands up. Since FY 2015, USAC has required the costs of these network security services and features to be removed from funding requests.

cybersecurity were calculated for every school that currently participates in the E-rate program. These estimates account for the E-rate's existing investment in basic firewall protections. Averaging the results, an overall annual cost to the E-rate program was calculated for the three above levels of protection: (1) $0.738 billion to support next-generation firewalls; (2) $1.606 billion to support next-generation firewalls and endpoint security features; and (3) $2.389 billion to support all layers, including advanced+ services. These cost assumptions are based on five-year price models with the assumption that Category 2 E-rate budgets would be increased to accommodate an enhanced eligible services list."[23] Notably, the cost estimate analysis shows that cybersecurity protections prices decline as the size of purchases grows, so the Commission should consider encouraging bulk purchasing.

Lastly, the Commission should adopt a new broadband vision and definition inclusive of comprehensive cybersecurity protections. As the CoSN and FFL cost estimate report notes, "digital learning will not be truly equitable unless all schools – including those serving low income, rural and other marginalized populations - have high-capacity access and advanced network security. These two elements – speed and security - are not distinct from an engineering and network design perspective and should no longer be treated as distinct in federal law and regulation." The Commission should seek ways to integrate this new definition into the agency's new broadband mapping initiative and include it in future Broadband Progress Reports.

V. CONCLUSION

Based on the scope and seriousness of the cybersecurity challenges facing the nation's schools and consistent with the Commission's authority, as described herein, we respectfully

[23] 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 (Jan. 2021), available at https://www.cosn.org/advocacy

urge the Commission to grant the Petitioners' request for declaratory relief and rulemaking, including defining all firewall and related features as "basic" beginning in funding year 2021; increasing the five-year Category 2 budget cap in future funding years to support needed additional cybersecurity investments; and updating the agency's broadband definition to include cybersecurity.

Respectfully submitted,

/s/ Keith Krueger
Keith Krueger, CEO
Consortium for School Networking

/s/ Phillip Lovell
Phillip Lovell, Vice President
Alliance for Excellence In
Education

/s/ Michael Casserly
Michael Casserly, Executive Director
Council of the Great City Schools

/s/ John Windhausen
John Windhausen, Jr., Executive Director
Schools, Health & Libraries
Broadband Coalition

/s/ Julia Fallon
Julia Fallon, Executive Director
State Educational Technology
Directors Association

/s/ Debra Kriete
Debra Kriete, Chair
State E-Rate Coordinators' Alliance

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

JANUARY 2021

COSN
LEADING EDUCATION INNOVATION

FUNDS FOR LEARNING
YOUR E-RATE GUIDES

Table of Contents

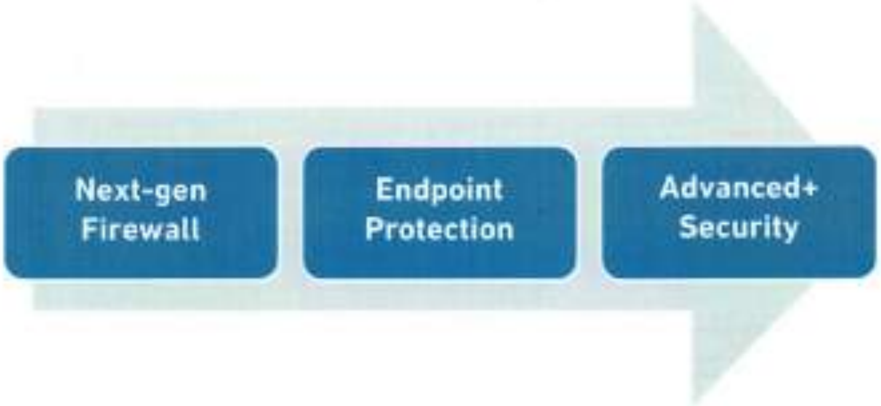
1.0

Executive Summary

K-12 schools increasingly find themselves under sophisticated cyberattacks that cause significant damage and disruption, and risk our commitment to protecting student data, as well as ensuring equitable and safe Internet access for learning. The FBI has recently issued warnings that K-12 is the most targeted public sector due to ransomware attacks.

As schools scramble to train users, shore up their networks and deploy electronic countermeasures, there is a growing awareness by educators, policymakers, and the public that existing school technology budgets are inadequate for the increased security challenge. More support is needed; and expanding the federal E-rate program's existing basic network security investments could bring timely financial aid to help defend school networks.

This report offers an estimate of the cost to include a more appropriate cybersecurity focus in the E-rate program. The costs are based on third-party hardware, software, and cloud-based services intended to guard schools from online attacks. Security measures have been segregated into three layered categories which build upon one another: (1) next-generation firewalls, (2) endpoint protection, such as anti-malware software, and (3) advanced+ services, such as multi-factor authentication. All these components are essential to modern cybersecurity protection.



Detailed cost models were gathered from three leading cybersecurity manufacturers who provided in-depth pricing information on a confidential basis. The models were validated by school district leaders. The cost to offer discounts on the three levels of cybersecurity were calculated for every school that currently participates in the E-rate program. These estimates account for the E-rate's existing investment in basic firewall protections.

Averaging the results, an overall annual cost to the E-rate program was calculated for three levels of protection:

- **$0.738 billion to support next-generation firewalls**
- **$1.606 billion to support next-generation firewalls and endpoint security features**
- **$2.389 billion to support all layers, including advanced+ services**

These cost assumptions are based on five-year price models with the assumption that Category 2 E-rate budgets would be increased to accommodate an enhanced eligible services list.

2.0

Introduction

K-12 schools increasingly find themselves under growing sophisticated cyberattacks. As schools scramble to train users, shore up their networks and deploy electronic countermeasures, there is a growing awareness that existing school technology budgets and their networks are inadequate for the challenge.

The federal E-rate program, which serves 95.4% of K-12 students in the country[1], provides a natural conduit for timely financial aid that could be leveraged to assist schools in the United States with their cybersecurity efforts. Schools are familiar with the E-rate program's forms, procedures, and deadlines, and only regulatory changes would be necessary to provide the additional support.

To address this serious problem, it is essential to understand the scope and costs of the services that are necessary to protect K-12 school networks. For purposes of this analysis, the cost is estimated for all schools who currently participate in the E-rate program.

[1] https://www.fundsforlearning.com/blog/2020/12/e-rate-supports-95-percent-of-k-12-students

2.1 What Costs Are Included?

The focus of this report is the hardware, software and cloud-based security functions offered by third-party solution vendors. Cost calculations are tied to purchased or licensed items, i.e., expenditures that have a SKU or barcode associated with them. These types of purchases align well with the E-rate competitive bidding rules and eligible services list, and it is assumed that they are the most likely candidates to receive E-rate discounts.

This report does not estimate the costs that result from a cybersecurity attack (e.g. ransom payments, data recovery, downtime, school closings, school reputation, data breaches, etc.) Nor are there expenses included for training, security assessments, consulting services, or school staff. These are all important items with very real costs; however, it is considered less likely that the E-rate program could easily accommodate these sorts of costs and they therefore are not included in the cost estimates.

2.2 Increased E-rate C2 Budgets

The cost calculations in this analysis assume that there would be additional Category 2 ("C2") funding available for cybersecurity and that every K-12 school would fully utilize it. If cybersecurity were made fully eligible without additional C2 funding, there would be very little benefit for schools because C2 funds are already highly utilized and capped. Therefore, discussions about the eligibility of cybersecurity should also consider a corresponding increase in Category 2 budgets/caps.

2.3 Additional Cybersecurity Resources

Whether or not E-rate funding is provided for cybersecurity, schools must take action to secure their network resources and student data. CoSN offers resources to help with this effort and they are available at **www.cosn.org/cybersecurity**.

3.0 Methodology

The total expense to provide cybersecurity for all K-12 schools was estimated by calculating the cost to protect each individual K-12 school participating in the federal E rate program and then summing the total. The price model is driven by the number of sites and users within a school or school district, the level of security being utilized, Internet bandwidth, and the range of fees charged by networking manufacturers for their various security goods and services.

3.1 Count of Applicants, Sites, and Users

In total, there currently are 21,107 K-12 E-rate applicants in the United States. These represent 119,502 K-12 schools; 53,990,412 students; and an estimated 3,363,997 school staff. The following table summarizes this data, and organizes it based on the number of sites within a school district.

K-12 E-rate Applicants, Site Counts, Student Enrollment, and Estimated Staff

Applicant Size by count of school sites	Count of Applicants	Count of Sites	Count of K-12 Students	Count of Staff	Total Count of Users
A: Single	8,432	8,432	2,848,598	181,172	3,029,770
B: 2-4	7,242	20,483	6,888,099	431,452	7,319,551
C: 5-9	3,176	20,262	9,636,945	600,135	10,237,080
D: 10-24	1,560	22,844	11,675,484	725,975	12,401,459
E: 25-49	422	14,502	8,262,790	513,422	8,776,212
F: 50+	275	32,979	14,678,496	911,841	15,590,337
Grand Total	**21,107**	**119,502**	**53,990,412**	**3,363,997**	**57,354,409**

The total count of K-12 E-rate applicants, sites, and users is the fundamental driver for the cybersecurity cost model. The primary source for this information is E-rate funding application data. When E rate funds are requested, a school must include on their application a list of sites that will receive service along with the student enrollment at each site. Taken together, these applications form a comprehensive picture of the K-12 schools who participate in the E-rate program and are eligible to apply for cybersecurity financial support.

Almost all security expenses are tied directly or indirectly to the number of individuals who utilize devices connected to a computer network. For a school district, the number of users would include both students and staff. Because the count of school staff in not included on E-rate application forms, this number was estimated based on an average of 16.1 students per teacher[2] .

[2] See Table 208.10; Public elementary and secondary pupil/teacher ratios, by selected school characteristics; Fall 2017; https://nces.ed.gov/programs/digest/d19/tables/dt19_208.10.asp

3.2 Levels of Security

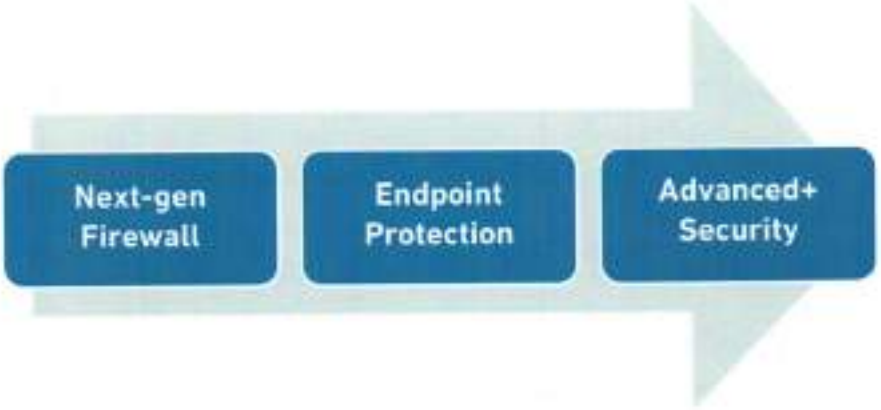
Effective cybersecurity outcomes require a multilayered set of hardware, software and services working in conjunction with each other[3]. Cybersecurity is not a single activity, but a suite of goods and services working in conjunction to guard networks, devices, and data from unauthorized access. There is no one piece of hardware or single software subscription that mitigates all cybersecurity risk. Like guarding a physical building with locks, video cameras, security guards, and motion detectors, it takes a myriad of resources to reduce the potential for malicious network activity.

Furthermore, the recommended security measures for a particular school will vary in direct proportion to its level of technology adoption: the more devices, locations, local and remote users, cloud-based services, virtual connections, and so on, the more entry points that need to be guarded, increasing the need for security services.

For purposes of this analysis, cybersecurity has been segmented into three categories, each corresponding to deeper levels of network defense and traffic inspection.

- **Next-generation firewalls**
- **Endpoint protection**
- **Advanced+ security**

For purposes of the cost calculations, the features embedded in each level are cumulative, with subsequent levels building on previous levels. It also should be noted that in real world applications the distinction between levels can be somewhat muddled. In fact, the specific transition point from level-to-level can be difficult to identify because of overlapping functionality between security services, particularly when different security platforms from different vendors are involved.



[3] Another key compoonent is human behavior

3.2.1 Next-Gen Firewalls

Like other network electronics, modern firewalls have evolved significantly since their introduction. They are more sophisticated than first generation models, but their function remains the same: ensuring continued network operation by preventing unauthorized access or intrusions. Common security features included with next-generation ("next-gen") firewalls include:

- **Intrusion Prevention / Intrusion Detection (IPS/IDS)**: detecting and stopping network activity which 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

3.2.2 Endpoint Protection

Malicious software poses a significant threat to the reliable operation of a network. "Anti-X" security measures guard network endpoints from being coopeted for nefarious purposes. It typically includes the following:

- **Anti-virus and anti-malware**: protect endpoints from malicious software which can be used as an attack vector by a third party to disrupt network operation
- **Anti-spam**: protects endpoints

3.2.3 Advanced+ Security

Authenticating user identities and segmenting online access protects networks by limiting attack vectors and securing sensitive data.

- **Domain Name System (DNS) security**: protecting DNS servers from malicious attacks. Because DNS servers are often accessed by many network endpoints, a compromised server can result in DDoS attacks or network downtime
- **Blocking and filtering**: ensuring that network endpoints are prevented from accessing websites or other network resources known to be malicious
- **Cloud application protection and multi-factor authentication (MFA)**: ensuring that sensitive data stored in cloud applications and services are only accessed by authorized users

3.3 Security Appliance Throughput

As the number of security functions deployed on a network increase, so does the demand for processing power provided by security appliance hardware. This results in network security appliances that require higher throughputs (e.g., the ability to inspect more megabits per second of network activity) which can result in additional security costs. To account for this additional overhead, the required network throughput is increased by a fixed percentage that is calculated based on the number of users in a school or school district.

Throughput Adjustment Factor For Firewalls

User Count	Additional Firewall Throughput
Up to 9,999	40%
10,000 to 24,999	30%
25,000 or more	25%

As more users are added to a network, and as the size of a local network increases, there is a greater chance that data will be available on the local network. This can reduce the bandwidth requirements for encrypted broadband data. For example, if a VPN function is utilized on a network that support 1,000 users, the required throughput of the network security appliance is assumed to increase by 40%. However, if the network supports 25,000 users, the throughput is assumed to increase by a smaller amount, 25%.

3.4 Manufacturer Price Variations

Network equipment manufacturers offer a diverse range of goods and service to protect networks. There are numerous cybersecurity philosophies, strategies, and technologies present in the marketplace. Each has varying levels of functionality, interoperability, and pricing. This can make apples-to-apples price comparisons difficult.

Further complicating price calculations is the fact that schools choose cybersecurity solutions for reasons that are not entirely independent of other factors. For example, if a school has a large installed base of equipment from a particular manufacturer, it may be more effective to select a security system that more easily integrates into its existing network, even if it is has a slightly more expensive list price.

For these reasons, this report provides a range of prices for each level of security, rather than a one-size-fits-all cost calculation. To achieve a diverse range of options, detailed pricing data was provided by three leading cybersecurity manufacturers[4]. Pricing was based on the best K-12 discount pricing available, and, where applicable, five-year licenses.

For each K-12 school, there were nine price calculations, reflecting the three levels of security offered by each of three different manufacturers. The price at each level was then averaged across the manufacturers to estimate the overall investment required. The table below illustrates how the price would vary for a specific school district with an enrollment of 4,750 students. The school district has 9 school sites with an estimated staff count of 296. The average annual cost to provide all three levels of cybersecurity for this school is estimated at $383,708.

Sample Annual Cybersecurity Cost Calculations for a School with 4,750 Students

Security Level	Vendor A	Vendor B	Vendor C	AVERAGE
Next-gen Firewall	$204,439	$255,254	$72,638	$177,444
Endpoint	$183,927	$86,791	$52,638	$107,785
Advanced+	$132,980	$119,086	$43,373	$98,479
Total Annual Cost	**$521,346**	**$461,131**	**$168,648**	**$383,708**

The cost shown is the total annual cost, based on a five-year service agreement. The price for each vendor is calculated separately and then averaged. It is important to note that the costs are incremental across security levels and cannot be separated (i.e., the incremental cost to add endpoint protection presumes the use of a next-gen firewall).

[4] By design, the names of these manufacturers have not been included in this report. CoSN does not endorse or promote a particular cybersecurity vendor; and, as already described, there is no one right choice when it comes to security. The manufacturers that provided data are considered leading providers of cybersecurity goods. According to one respected source, the three manufacturers that shared cost data have a combined global market share of 23%. The manufacturers provided CoSN/Funds for Learning with confidential access to detailed information about their cost models and education discounts. The aggregate results of these pricing models have been reviewed by a large group of over 30 school CIOs on behalf of CoSN.

Following a similar methodology, the table below shows the estimated average cost for the three levels of security at five sample school districts.

Average Cybersecurity Cost Calculations: Total Annual Expense for Five Sample School Districts

Level of Security			School District Enrollment				
Next-gen Firewall	Endpoint	Advanced+	3,000 Students	4,750 Students	12,550 Students	20,755 Students	42,205 Students
x			$129,657	$177,444	$395,163	$606,671	$1,270,325
x	x		$201,279	$285,229	$663,616	$1,044,961	$2,123,556
x	x	x	$267,699	$383,708	$890,031	$1,416,826	$2,791,410

As enrollment increases, the overall cost increases; however, the cost per student gradually declines for most schools and security levels, as shown.

Average Cybersecurity Cost Calculations: Annual per Student Expense for Various School District Enrollments

Level of Security			School District Enrollment				
Next-gen Firewall	Endpoint	Advanced+	3,000 Students	4,750 Students	12,550 Students	20,755 Students	42,205 Students
x			$43.22	$37.36	$31.49	$29.23	$30.10
x	x		$67.09	$60.05	$52.88	$50.35	$50.32
x	x	x	$89.23	$80.78	$70.92	$68.26	$66.14

3.5 Adjustment for Existing E-rate Eligible Functionality

This report estimates the net cost to the E-rate program if cybersecurity was considered eligible for discounts. The E-rate program administrator currently approves limited funding for firewalls. Therefore, to calculate the net cost to the E-rate program of cybersecurity, the existing eligible portion of each firewall is subtracted from the overall cost. The resultant amount is the net new cost that would be discounted.

For example, assume that a Model XYZ firewall costs $10,000 and currently is considered 40% eligible. Its E-rate funding request would be based on an eligible pre-discount cost of $4,000. If 100% of the firewall was eligible, the result would be an additional pre-discount expense of $6,000 that would qualify for support.

The results presented in this report reflect the net additional expense to the E-rate program.

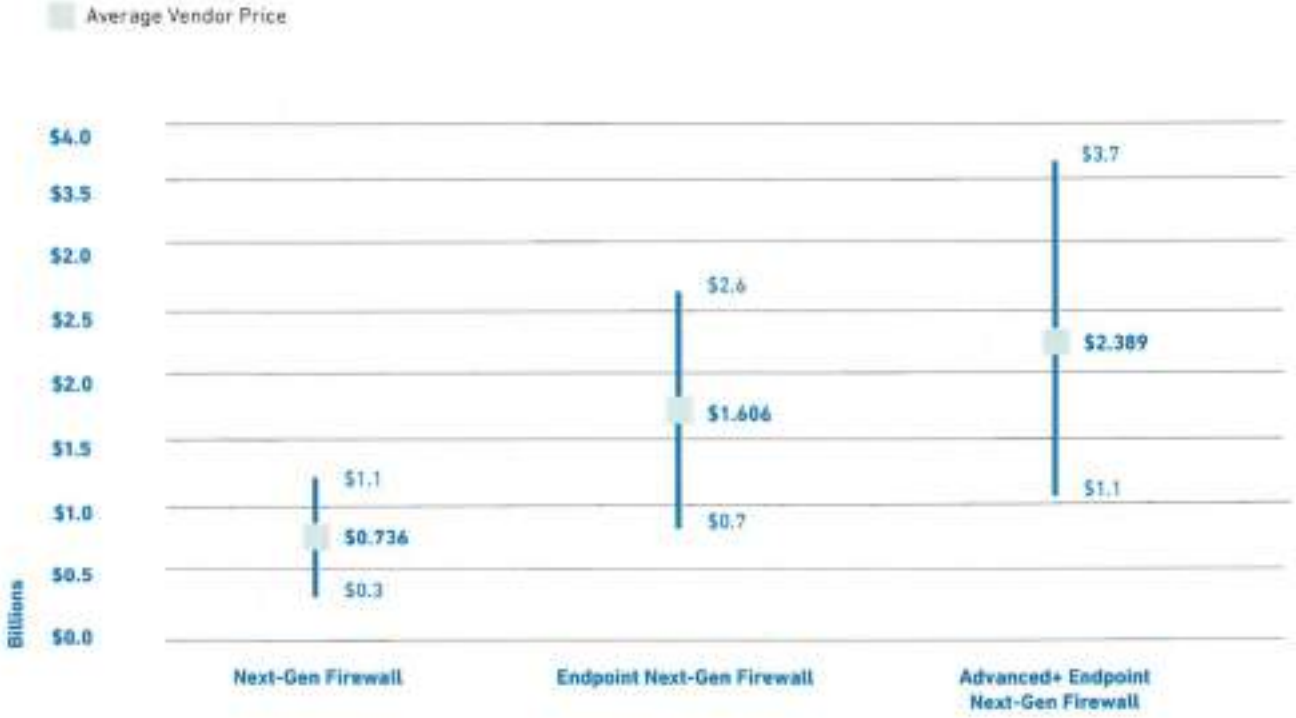
4.0

Results and Analysis

The annual E-rate cost to provide support for all three levels of cybersecurity is estimated at $2.389 billion. If support were only provided for next-gen firewalls, the minimum level of cybersecurity, there would be an estimated annual cost to the E-rate program of $0.736 billion. Adding endpoint protection, the second level of security, along with next-gen firewalls, would results in a total annual E rate expense of $1.606 billion.

The chart below illustrates how the annual E-rate budget would increase as additional cybersecurity functions were added to the eligible services list. The average cost is shown, as well as the high and low cost for the range of manufacturer pricing.

Additional Annual E-rate Funding for Cybersecurity
Est. Range of Costs for Security Levels by Various Manufacturers

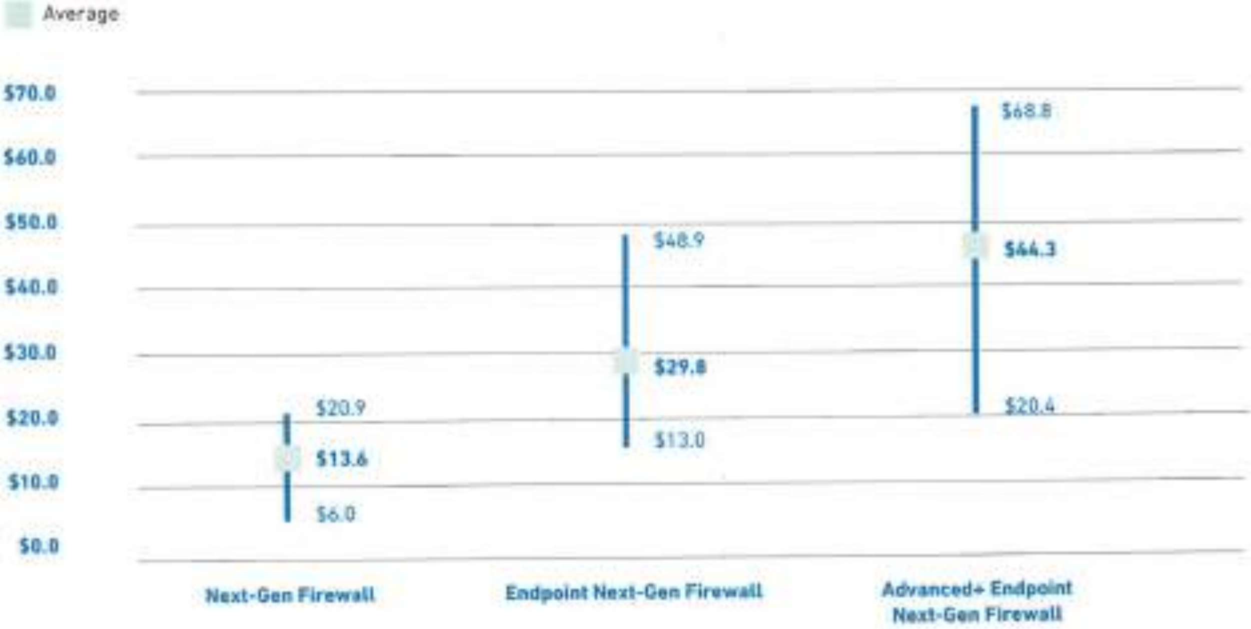


4.1 Per Student Funding

$44.26 per student is needed each year to provide comprehensive cybersecurity for schools via the E-rate program. The minimum annual amount is estimated at $13.63 per student for next-gen firewall support. If endpoint security is added, the annual cost per student would be $29.75.

Additional Annual E-rate for Cybersecurity Per Student

Est. Range of Costs for Security Levels by Various Manufacturers



4.2 Per Applicant Funding

The average annual amount of funding requested per applicant is shown in the following table. Costs are estimated based on the size of an applicant, measured by the count of its school sites. The overall average annual E-rate funding request for next-gen firewall protection is $68,333. Adding endpoint security would increase the annual E-rate expense to $109,583 per applicant. Finally, if all three levels of security were eligible and funds were available, the average applicant would request $146,682 per year.

Annual Total E-rate Cost of Cybersecurity

Level of Security			Average E-rate Funding Request by School District Size (Count of Sites)						
Next-gen Firewall	Endpoint	Advanced+	Single Site	2-to-4 Sites	5-to-9 Sites	10-to-24 Sites	25-to-49 Sites	50+ Sites	Overall Average
x			$15,994	$33,954	$86,082	$183,590	$422,215	$1,227,558	**$68,333**
x	x		$23,538	$52,118	$136,043	$300,739	$300,739	$2,027,374	**$109,583**
x	x	x	$33,403	$70,779	$182,747	$404,533	$404,533	$2,602,621	**$146,682**

5.0 Policy Recommendations

The Federal Communications Commission (FCC) should reimagine what the agency means when it says consumers – including schools and students – have access to a high-capacity internet connection. Upload and download speeds are the central factor when defining and measuring broadband access, but a high-speed connection that lacks adequate cybersecurity is like a Formula One car without seatbelts and other safety features designed to protect the driver. Digital learning will not be truly equitable unless all schools – including those serving low income, rural and other marginalized populations - have high-capacity access and advanced network security.

5.0 Policy Recommendations

These two elements – speed and security - are not distinct from an engineering and network design perspective and should no longer be treated as distinct in federal law and regulation. Cyberattacks compromise the network speed and availability of even the fastest connections. With this unified vision of broadband equity as our goal, the FCC should:

- Adopt a broadband definition describing new, appropriate minimum upload and download speeds as well the minimum cybersecurity protections that must be integrated in the network. The agency's new broadband mapping initiative and future Broadband Progress Reports should be grounded in this unified connectivity definition.

- Direct the Universal Service Administration Company to treat all firewalls as "basic" beginning in funding year 2021.

- Issue a notice of proposed rulemaking increasing the five-year Category 2 budget cap by $81 per student for the purpose of covering minimum basic firewalls as described by this report.

In addition to ensuring that the E-rate is updated to better enhance school district's cybersecurity readiness through network investments, Congress should take steps to address the human capacity and information sharing elements of comprehensive cybersecurity strategies, including by:

- Directing the Cybersecurity and Infrastructure Security Agency (CISA) Director at the Department of Homeland Security to establish a Cybersecurity Clearinghouse to disseminate information, best practices, and grant opportunities to improve cybersecurity.

- Establish a Cybersecurity Registry within CISA to track incidents of cyberattacks in K-12 schools;

  and

- Establish a K-12 Cybersecurity Human Capacity Grant Program at the Department of Homeland Security

As the cyberthreat to school districts and students continues to grow, federal leaders must take these steps and more to ensure that all students – regardless of income or location - have access to secure broadband for learning. Failing to equitably fund secure networks for students served by school districts that are unable to protect them, places them at higher risk for cybercrimes compared to their counterparts in wealthier districts.

Exhibit A

Additional Tables and Charts

Included are additional tables and charts of information related to the cybersecurity cost model.

A.1 Total E-rate Cost by Security Level and Manufacturer

The following table shows the estimated annual cost to the E-rate program for varying levels of security based on the pricing provided by each manufacturer.

Annual Total E-rate Cost of Cybersecurity

Level of Security			Annual E-rate Funding Request ($ billions)			
Next-gen Firewall	Endpoint	Advanced+	Vendor A	Vendor B	Vendor C	AVERAGE
x			$1.130	$0.752	$0.325	$0.736
x	x		$2.640	$1.478	$0.701	$1.606
x	x	x	$3.712	$2.356	$2.356	$2.3889

A.2 Estimated E-rate Expense Per School District by Size

The average annual amount of funding requested per applicant is shown in the following table. Costs are estimated based on the size of an applicant, measured by the count of its school sites. The overall average annual E-rate funding request for next-gen firewall protection is $68,333. Adding endpoint security would increase the annual E-rate expense to $109,583 per applicant. Finally, if all three levels of security were eligible and funds were available, the average applicant would request $146,682 per year.

Annual Total E-rate Cost of Cybersecurity

Level of Security			Average E-rate Funding Request by School District Size (Count of Sites)						
Next-gen Firewall	Endpoint	Advanced+	Single Site	2-to-4 Sites	5-to-9 Sites	10-to-24 Sites	25-to-49 Sites	50+ Sites	Overall Average
x			$15,994	$33,954	$86,082	$183,590	$422,215	$1,227,558	**$68,333**
x	x		$23,538	$52,118	$136,043	$300,739	$300,739	$2,027,374	**$109,583**
x	x	x	$33,403	$70,779	$182,747	$404,533	$404,533	$2,602,621	**$146,682**

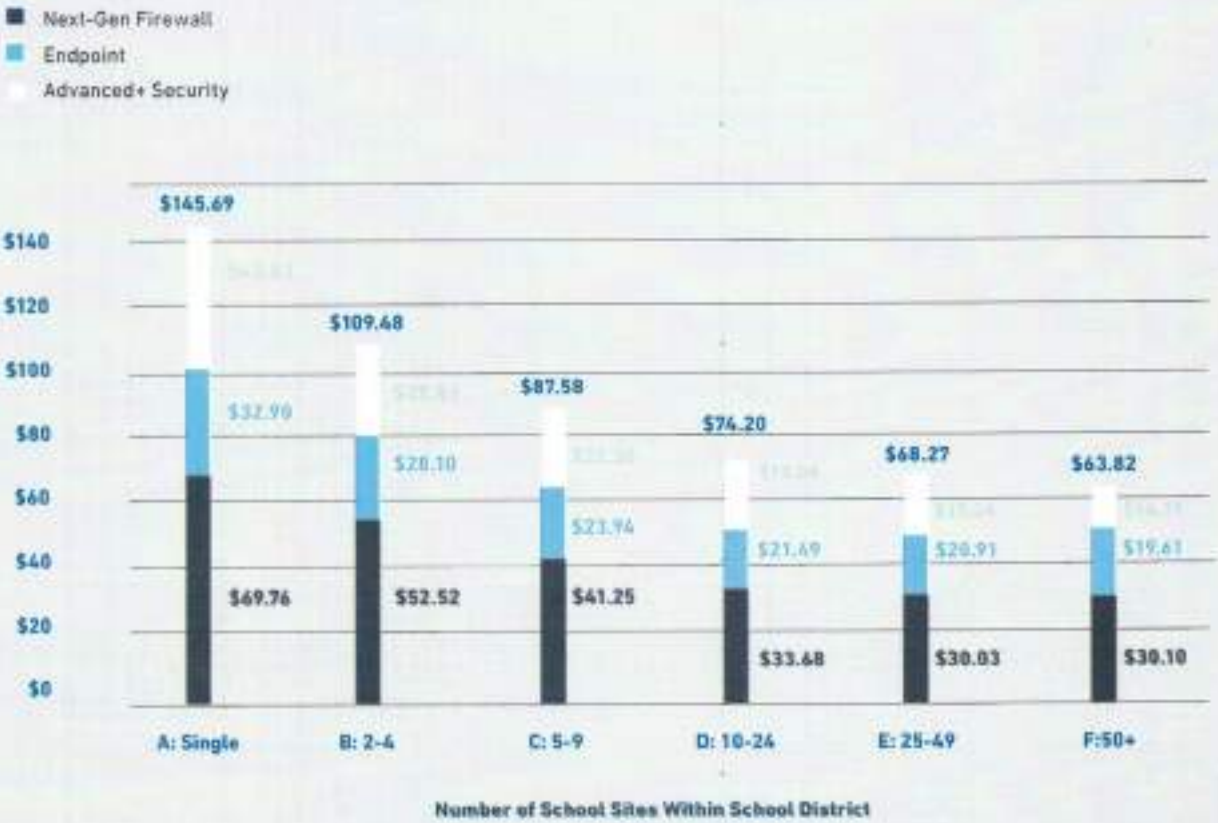
A.3 Per Student Pricing by School Size

The price per student varies significantly based on the number of students within a school district. This is because fixed costs are averaged across a higher number of students and most licenses following a sliding price scale, with lower unit prices for higher quantities.

For a single school, the estimated average annual pre-discount total cost of cybersecurity is $145.69 per student for all three levels of protection. For a district with 50 or more school locations, the average annual cost drops to $63.82 per student. This is a 56% reduction in the cost per student, demonstrating how sensitive the cost model is to the size of the entity. The more users that are being protected, the lower the per unit cost. This suggests an opportunity for cost-savings when network security can be standardized and deployed on a large scale, such as a regional or state-level initiative.

Annual "Pre-Discount" Expense Per Student

BY THE NUMBER OF SCHOOL SITES WITHIN A SCHOOL DISTRICT



A.4 Detailed Cost Calculations

The following tables provide detailed cost estimates for each level of security and manufacturer. The first table is the total annual cost for each type of security prior to any E rate eligibility considerations or discount rates. These are the overall "pre-discount" costs, reflecting the combined payment that would be made by both the applicant and the E-rate program. The average total annual expense for the three levels of cybersecurity support is calculated to be $4.356 billion.

Annual Expense by Vendor and Security Level
Total Cost Prior to E-rate Eligibility and Existing Discounts

	Next-Gen Firewall	Endpoint	Advanced+	TOTAL
Vendor A	$1,914,030,862	$2,124,664,406	$1,508,303,766	$5,546,999,034
Vendor B	$3,306,631,202	$1,021,030,231	$1,235,88288,976	$5,563,490,408
Vendor C	$867,869,588	$529,774,788	$561,379,993	$1,959,024,368
AVERAGE	**$2,029,510,550**	**$1,225,156,475**	**$1,101,837,578**	**$4,356,504,603**

Most cybersecurity expenses are not considered eligible for E-rate discounts. However, certain "basic" firewall costs are currently eligible for E-rate discounts, and applicants can submit funding requests for them today. Because these items are already represented in current E-rate demand, they must be subtracted from the pre-discount cybersecurity expense to accurately calculate the increased expense associated with the added cybersecurity functions. The following table represents this incremental pre-discount cost. The adjusted average total annual expense for the three levels of cybersecurity support is calculated to be $3.362 billion.

New Pre-Discount E-rate Expense by Vendor and Security Level
Total Additional Cost Given Firewall Functions are Currently Eligible for E-rate Discounts

	Next-Gen Firewall	Endpoint	Advanced+	TOTAL
Vendor A	$1,590,387,862	$2,124,664,406	$1,508,303,766	$5,223,356,034
Vendor B	$1,058,121,984	$1,021,030,231	$1,235,828,976	$3,314,981,191
Vendor C	$456,952,988	$529,774,788	$561,379,993	$1,548,107,191
AVERAGE	**$1,035,154,278**	**$1,225,156,475**	**$1,101,837,578**	**$3,362,148,331**

E-rate discounts for Category 2 purchases range from 20% up to 85%. Each applicant calculates their specific E-rate discount based on the percentage of their students who qualify for the National School Lunch Program. The following table is the summation of each participants maximum E-rate cybersecurity funding request depending upon the level of cybersecurity and manufacturer.

The average total annual E-rate funding request is calculated to be $2.389 billion. This assumes that applicants fully utilize this option and that there is an adjustment to their Category 2 budgets caps to allow for this amount of additional funding.

Annual E-rate Funding Requests

Estimated E-rate Funding Request Amounts Based on Individual Discount Rates

	Next-Gen Firewall	Endpoint	Advanced+	TOTAL
Vendor A	$1,130,231,400	$1,509,922,506	$1,071,897,188	$3,712,051,095
Vendor B	$751,969,202	$725,609,428	$878,259,164	$2,355,837,795
Vendor C	$324,740,038	$376,491,870	$398,952,551	$1,100,184,459
AVERAGE	**$735,646,880**	**$870,674,601**	**$783,036,301**	**$2,389,357,783**

A.5 Additional C2 Budget Cap

Category 2 funding requests are subject to a budget cap that limits an applicant's cumulative funding. Given the already high utilization of Category 2 discounts[5], it would be incumbent upon the FCC to consider increasing the applicant C2 budget cap to provide additional support for cybersecurity; otherwise, E-rate applicants would be forced to choose between cybersecurity and the Category 2 goods and services that they are already purchasing.

The following table outlines the increased five-year per student budget factor necessary to meet the cybersecurity needs of K-12 school E-rate applicants. This is the extra amount of budget cap necessary to accommodate the needs of schools without compromising their other Category 2 networking requirements.

Additional Per Student Sudget Cap to Fully Meet C2 Demands

Including Cybersecurity Based on Average C2 Budget Utilization of 84%

Level of Security			Additional C2 Per Student Budget Required
Next-gen Firewall	Endpoint	Advanced+	
x			$80.53
x	x		$175.83
x	x	x	$261.55

[5] 84% of sites utilized E-rate discounts for on-campus networking during the initial pilot program of the Category 2 budget system. See the 2020 E-rate Trends Report, pg. 9, https://www.fundsforlearning.com/2020ErateTrends