E-Rate Program Expansion: A Pathway to Combating Cybersecurity Attacks in K-12 Schools

ABSTRACT

Every day, a K-12 school in the United States falls victim to a harmful cyberattack that can cost it millions of dollars and keep its doors closed for days or weeks. Schools are desperate for funding to purchase essential cybersecurity services and products to protect their school's networks from these cyberattacks. Such funding should be available through the Federal Communications Commission's (FCC) E-Rate program, which was established as part of the Telecommunications Act of 1996 to provide discounts for connectivity services in K-12 schools across the country. During the COVID-19 pandemic, schools and other telecommunications industry stakeholders submitted petitions asking the FCC to consider expanding the E-Rate program to include discounts for advanced firewall and network security services. While schools can currently utilize the E-Rate program to obtain discounts on telecommunications and internet services like cable modems, routers, and antennas, they are currently unable to use E-Rate program funding to purchase essential cybersecurity products and services, including advanced or next-generation firewalls, that would mitigate the impact of cyberattacks.

With technological advancements, hackers are more capable than ever to devastatingly harm school networks; as such, the technological needs for achieving connectivity to schools have changed since the 1996 Act was passed. Advanced or next-generation firewalls and other network security services are now more essential than ever to obtaining safe and efficient connectivity for K-12 schools. This Note proposes that the FCC immediately expand the E-Rate program to include essential cybersecurity products and services in the program's eligible services list. The FCC has the requisite authority under the Telecommunications Act of 1996 to expand the E-Rate program's eligible services list to keep up with changing technological needs. While different sectors of the federal government are working to resolve the cybersecurity problems schools are facing, what schools need most is immediate and accessible funding.

TABLE OF CONTENTS

While students and parents are back-to-school shopping and meeting new teachers, a potential cyberattack shutting down their schools or stealing their valuable student data should not be on their minds. Before the start of the 2023 school year, however, the city of New Haven, Connecticut had already lost more than $6 million across multiple cyberattacks and only recouped about half before classes resumed.[1] A similar data hack in June 2023 impacted tens of thousands of Minnesota students through the release of sensitive personal data including which students were in foster care, who qualified for government programs, and even students' bus routes.[2] With nearly 93 percent of households with school-aged children engaged in some form of distance learning during the COVID-19 pandemic, schools and

[1] *Connecticut School District Lost More Than $6 Million in Cyber Attack, so Far Gotten About Half Back*, AP NEWS (Aug. 10, 2023, 10:52 PM), https://apnews.com/article/connecticutt-school-district-cyber-attack-new-haven-f7fad8a63916a1a80a3885a92d326964 [perma.cc/BVT4-QU4S].

[2] Jordan Schroeer, *95,000 MN Students' Data Breached in Cyber Attack*, VALLEY NEWS LIVE (June 9, 2023), https://www.valleynewslive.com/2023/06/09/95000-mn-students-data-breached-cyber-attack/ [perma.cc/GG2F-M2CZ].

students became increasingly vulnerable to cyberattacks.[3] However, cyberattacks are not a new issue and risks are certainly not limited to remote learning.[4] The K12 Security Information Exchange, a nonprofit focused on helping schools prevent cyberattacks, estimated that there have been more than 1,330 publicly disclosed cyberattacks on K-12 schools since 2016.[5] In the 2022–2023 school year, at least four K-12 school districts in the United States had to cancel classes or close operations completely for several days due to cyberattacks.[6] The US Government Accountability Office (GAO) reported that each school district loses between $50 thousand to $1 million per cyberattack and that each cyberattack typically lasts from three days to three weeks, with a full recovery taking anywhere from two to nine months.[7]

The COVID-19 pandemic compelled schools to look for funding to increase their cybersecurity services as online schooling became imperative amidst stay-at-home mandates.[8] On August 20, 2020,

[3] *See* Kevin McElrath, *Nearly 93% of Households with School-Age Children Report Some Form of Distance Learning During COVID-19*, U.S. CENSUS BUREAU (Aug. 26, 2020), https://www.census.gov/library/stories/2020/08/schooling-during-the-covid-19-pandemic.html [perma.cc/YD7S-LPNH]; *see also* Petition for Waiver of Cisco Systems, Inc., Petition, WC Docket No. 13-184 (37 FCC Rcd. 14615) at 1 (2021) [hereinafter Cisco Petition]

[4] *See* DOUGLAS A. LEVIN, K12 SEC. INFO. EXCH, THE STATE OF K-12 CYBERSECURITY: YEAR IN REVIEW: 2022 ANNUAL REPORT 3 (2022), https://static1.squarespace.com/static/5e441b46adfb340b05008fe7/t/6228bfe3f412c818293e16e1/1646837732368/StateofK12Cybersecurity2022.pdf [perma.cc/KFZ7-XC6Q] (reporting cybersecurity incident trends in US K-12 public schools based on data from the Government Accountability Office).

[5] *Id.* (these incidents included student data breaches, data breaches involving teachers and school community members, ransomware attacks, business email compromise scams, denial of service attacks, website and social media defacement, online class and school meeting invasions, and other incidents).

[6] Lauren Langreo, *Biden Administration Announces Cybersecurity Initiative for K-12 Schools*, EDUC. WEEK (Aug. 7, 2023), https://www.edweek.org/technology/biden-administration-announces-cybersecurity-initiative-for-k-12-schools/2023/08 [perma.cc/8V7E-RN9P].

[7] *As Cyberattacks Increase on K-12 Schools, Here is What's Being Done,* U.S. GOV'T ACCOUNTABILITY OFF. (Dec. 1, 2022), https://www.gao.gov/blog/cyberattacks-increase-k-12-schools-here-whats-being-done [perma.cc/JY7T-NGB8] [hereinafter *As Cyberattacks Increase*].

[8] *See* Cisco Petition, *supra* note 3, at 3; *see also* Petition for Declaratory Relief and Petition for Rulemaking Allowing Additional Use Of E-Rate Funds for K-12 Cybersecurity, Petition, WC Docket No. 13-184 (37 FCC Rcd. 14615) at 2 (2021) [hereinafter CoSN Petition] (asking the FCC to modernize the E-Rate program to protect schools from cyberattacks); *see, e.g.*, Letter from John D. Harrington, Chief Executive Officer, Funds for Learning, to Jessica Rosenworcel, Chairwoman, Brendan Carr, Geoffrey Starks, Nathan Simington, Commissioners, Letter, WC Docket No. 13-184 (2022); Letter from John D. Harrington, Chief Executive Officer, Funds for Learning, to Marlene H. Dortch, Secretary, Letter, WC Docket No. 13-184 (2022); Letter from John D. Harrington, Chief Executive Officer, Funds for Learning, to Marlene H. Dortch, Secretary, Letter, WC Docket No. 13-184 (2022) (urging the FCC to implement the E-Rate program cybersecurity pilot program) [collectively hereinafter FFL Letters]; Letter from AASA, The School Superintendents Association, et al., to Jessica Rosenworcel, Chairwoman, Brendan Carr, Geoffrey

CISCO Systems, Inc. (CISCO), a digital communications technology corporation and E-Rate program stakeholder, sent a petition for waiver to the Federal Communications Commission (FCC or Commission) requesting that the Commission "exercise its waiver authority to permit schools to use E-Rate Category Two funding to cover the costs of network security software in the 2020 and 2021 funding year."[9] This was followed by continued requests from other E-Rate program stakeholders, including the Consortium for School Networking (CoSN), Funds for Learning (FFL), and twenty national educational groups, led by The School Superintendents Association (AASA), seeking the same.[10] Although the FCC denied these waivers, it has since considered expanding the E-Rate program to include cybersecurity services.[11]

This Note analyzes the FCC's authority to provide discounts for cybersecurity services to K-12 schools through the E-Rate program and expounds upon the need for the FCC to provide these discounts for cybersecurity services to fulfill the E-Rate program's goal of providing connectivity to schools.[12] Part I provides an overview of the FCC's E-Rate program and the authority provided to the FCC to expand the program's Eligible Services List (ESL) to include advanced or next-generation firewalls and other network security services. Part II analyzes other proposed solutions to make cybersecurity services accessible to schools and their shortcomings. Part III recommends that, in light of the existing shortcomings for other proposed solutions to fully

Starks, and Nathan Simington, Commissioners, Letter, CC Docket No. 02-6 (2022) [hereinafter AASA Letter].

[9] Cisco Petition, *supra* note 3, at 1.

[10] *See* CoSN Petition, *supra* note 8; FFL Letters, *supra* note 8; AASA Letter, *supra* note 8.

[11] *See* Wireline Competition Bureau Seeks Comment on Requests to Allow the Use of E-Rate Funds for Advanced of Next-Generation Firewalls and Other Network Security Services, 88 Fed. Reg. 1035 (Jan. 6, 2023) (to be codified at 47 C.F.R. pt. 54) ("[S]eek[ing] comment on petitions seeking permission to use E-Rate program funds to support advanced or next-generation firewalls and services"). During the COVID-19 emergency period, the American Rescue Plan established a $7.171 billion Emergency Connectivity Fund (ECF) that helped schools and libraries to purchases eligible services and equipment. PATRICIA MOLONEY FIGLIOLA, CONG. RSCH. SERV., R47621, THE FUTURE OF THE UNIVERSAL SERVICE FUND AND RELATED BROADBAND PROGRAMS 8 (2024). The ECF was intended to supplement the E-Rate program to purchase services not eligible for E-Rate funding, however, cybersecurity tools were listed as an ineligible cost of the ECF. FCC, FCC 21-58 APPENDIX B: ELIGIBLE SERVICES LIST FOR EMERGENCY CONNECTIVITY FUND PROGRAM, https://www.fcc.gov/sites/default/files/ecf_esl.pdf [perma.cc/JUZ3-YGVU] (last visited Feb. 28, 2024).

[12] Section 254 of the Telecommunications Act of 1996 authorizes the FCC to create the E-Rate program and lays out the guidelines for schools, libraries, and health care providers to obtain telecommunications services at a discounted rate. *See* 47 U.S.C. § 254. This Note only analyzes the E-Rate program's application to K-12 schools and does not address the E-Rate program's application to libraries or health care providers.

address this issue, the FCC should immediately expand the E-Rate program ESL to include advanced or next-generation firewalls and other network security services. Furthermore, this Note suggests that the FCC provide guidance to schools on how they can appropriately use cybersecurity E-Rate discounts to achieve the program's goal of connectivity. Finally, Part III advocates for a partnership between the FCC, the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Emergency Management Agency (FEMA) to combine grant programming through a joint application to ensure there are enough funds for schools to purchase necessary cybersecurity services.

I. OVERVIEW OF THE FCC E-RATE PROGRAM

The FCC's Schools and Libraries Program, more commonly known as the E-Rate program, provides discounts to schools to purchase telecommunications and internet services at an affordable rate.[13] In 1997, the E-Rate program was created by the FCC through a report and order after President Clinton signed the Telecommunications Act of 1996 (the Act) into law, which authorized the FCC to create the E-Rate program as an expansion of the Communications Act of 1934's universal service principle—that all Americans have access to communications services.[14] The E-Rate program, funded by the Universal Service Fund (USF), is primarily intended to provide affordable connectivity to schools.[15] While provisions for standard telecommunications and internet services like telephone dial-up, cable modems, and ethernet used to be enough, with thousands of harmful cyberattacks targeting schools every year, now more than ever, the E-Rate program lacks coverage for advanced cybersecurity services that would help achieve

[13] Services eligible for discounts under the E-Rate program include telecommunications and internet services like cable modems, routers, and antennas. *see* Modernizing the E-Rate Program for Schools and Libraries, Order, WC Docket No. 13-184 (37 FCC Rcd. 14615) (2021) [hereinafter Modernizing the E-Rate Program]. E-Rate discounts on these services range from 20 to 90 percent based on the needs of the school. *E-Rate: Universal Service Program for Schools and Libraries*, FCC, https://www.fcc.gov/consumers/guides/universal-service-program-schools-and-libraries-e-rate [perma.cc/4C3X-EP9C] (last visited Feb. 4, 2024) [hereinafter E-Rate: Universal Service]; *E-Rate – Schools & Libraries USF Program*, FCC, https://www.fcc.gov/general/e-rate-schools-libraries-usf-program [perma.cc/NT9V-29Y9] (last visited Feb. 9, 2024) [hereinafter *Schools & Libraries USF Program*].

[14] *See E-Rate and Education (A History)*, FCC, https://www.fcc.gov/general/e-rate-and-education-history [perma.cc/6TV9-KWBB] (last visited Feb. 29, 2024) [hereinafter *E-Rate and Education*].

[15] *See E-Rate Program - Discounted Telecommunications Services*, U.S. DEP'T EDUC. (Sept. 9, 2019), https://www2.ed.gov/about/inits/ed/non-public-education/other-federal-programs/fcc.html [perma.cc/JNV8-22U4] [hereinafter *Discounted Telecommunications Services*].

its intended purpose in an advancing technological era.[16] The E-Rate program, however, has available funds through the USF for the FCC to expand the E-Rate program ESL to include advanced cybersecurity services.[17] Accordingly, the FCC should exercise its authority under the Act and expand the E-Rate program ESL to include advance cybersecurity services immediately.

A. Universal Service Fund

The universal service is a principle in the Communications Act of 1934 that "all the people of the United States [have access to] rapid, efficient, Nation-wide and world-wide [telecommunications services] with adequate facilities at a reasonable [rate]."[18] In the same clause of the 1934 Act that establishes this universal service principle, the 1934 Act also established the FCC as a federal agency to "execute and enforce the provisions of this Act."[19] The Telecommunications Act of 1996 subsequently expanded on the 1934 Act's original principle of universal service by increasing access to more advanced telecommunications services like high-speed internet.[20] To help achieve universal service's modernized purpose, the Act also authorized the Commission to create the Universal Service Administrative Company (USAC), an independent, not-for-profit corporation, to collect universal service contributions from telecommunications carriers and administer the USF.[21]

[16] *See* Modernizing the E-Rate Program, *supra* note 13.

[17] *See* 47 U.S.C. § 254 (the Telecommunications Act of 1996 provides broad discretion to the FCC to expand the E-Rate program to keep up with advancements in technology); *Schools & Libraries USF Program*, *supra* note 13; Alyson Klein, *Newly Proposed Grants Could Help Districts Extinguish a Cybersecurity '4-Alarm Fire'*, EDUC. WEEK (July 12, 2023), https://www.edweek.org/technology/newly-proposed-grants-could-help-districts-extinguish-a-cybersecurity-4-alarm-fire/2023/07 [perma.cc/WK2Y-VL4P]. The E-Rate program has an annual cap of up to $4.456 billion, however, it has distributed only around $2 or 2.5 billion in the past few years. *See* Alyson Klein, *Newly Proposed Grants Could Help Districts Extinguish a Cybersecurity '4-Alarm Fire'*, EDUC. WEEK (July 12, 2023), https://www.edweek.org/technology/newly-proposed-grants-could-help-districts-extinguish-a-cybersecurity-4-alarm-fire/2023/07 [perma.cc/WK2Y-VL4P]; *Schools & Libraries USF Program*, supra note 13.

[18] Communications Act of 1934, Pub. L. No. 73-416, §1 (1934) (amended 1996).

[19] *Id.*

[20] *Universal Service*, FCC, https://www.fcc.gov/general/universal-service#:~:text=The%20Telecommunications%20Act%20of%201996,just%2C%20reasonable%20and%20affordable%20rates [perma.cc/T2CD-CZAS] (last visited Feb. 10, 2024) [hereinafter *Universal Service*].

[21] *Discounted Telecommunications Services*, *supra* note 15. In lawsuits from Consumers' Research, the constitutionality of the FCC's Universal Service Fund has been questioned. *See* Christopher Cole, *Full 5th Circ. Skeptical of FCC's Universal Service Regime,* LAW360, https://www.law360.com/articles/1723089/full-5th-circ-skeptical-of-fcc-s-universal-

The USF is funded by money collected from telecommunications carriers based on an assessment of their interstate and inter-nation end-user revenues and is used to provide the discounts to schools for eligible telecommunications services within the E-Rate program.[22] Section 254(d) of the Act requires all telecommunications carriers that provide interstate telecommunications services to contribute monetarily on an equitable and nondiscriminatory basis to the USF.[23] Each quarter, the contribution factor changes based on the demand for universal service support.[24] The estimate from USAC of how much money will be needed each quarter is filed with the FCC and is called the "demand filing."[25]

The USF contains almost $10 billion of available funds and is dispersed through four programs, including the E-Rate program.[26] The Commission has allocated up to $4.456 billion specifically to the E-Rate program every year,[27] however, the program has used far less than its allocation in recent years.[28] In 2022, the E-Rate program only used $2.5 billion and in 2021 the program used a little less than $2.1 billion, leaving room for more services like cybersecurity to be added to the program.[29] Given historical usage, almost $2 billion on average may be

service-regime [perma.cc/J2GL-HLMZ] (last visited March 19, 2024). Both the Fifth and Sixth Circuits have ruled the universal fund as constitutional. Consumers' Rsch. v. FCC, 72 F.4th 107, 108 (5th Cir. 2023); Consumers' Rsch. v. FCC, 67 F.4th 773, 778 (6th Cir. 2023). The Eleventh Circuit has also held that the Universal Service Fund is within the FCC's constitutional authority to delegate to a private entity and does not violate the nondelegation doctrine. Consumers' Rsch. v. FCC, 88 F.4th 917, 920–21 (11th Cir. 2023).

[22] *Universal Service*, *supra* note 20.

[23] *See* 47 U.S.C. § 254(d); *Universal Service*, *supra* note 20. Providers include telecommunications carriers, wireline and wireless companies, and interconnected Voice over Internet Protocol (VoIP) providers. *Universal Service*, *supra* note 20.

[24] *Universal Service*, *supra* note 20.

[25] *See id.* Occasionally, telecommunications carriers pass their obligations onto their customers by charging a small fee to cover the carrier's contribution factor amount. *Id.* The Telecommunications Act is neutral on this fee-shifting practice and neither encourages nor condones it. *Id.*

[26] The four programs the funds support are Lifeline, E-Rate, High Cost, and Rural Health Care. *See About USAC,* UNIVERSAL SERV. ADMIN. CO., https://www.usac.org/about/ [perma.cc/4EAH-H2AK] (last visited Feb. 29, 2024) [hereinafter *About USAC*].

[27] *Schools & Libraries USF Program*, *supra* note 13.

[28] Klein, *supra* note 17.

[29] *See id.* There has been a lower demand for E-Rate funds due to changes made to the E-Rate program in 2014 and declining data costs. *Id.* Changes to the program in 2014 included a cap on the per-pupil amount a single applicant could request. *See* Benjamin Herold, *The E-Rate Overhaul in 4 Easy Charts*, EDUC. WEEKLY, https://www.edweek.org/technology/the-e-rate-overhaul-in-4-easy-charts [perma.cc/7QWT-QNDQ] (last visited Feb. 10, 2024). This prevented large urban school districts from using all available E-Rate funds and provided a more even distribution and cut the program's costs. *See id.*

available to expand the E-Rate programs ESL to include services like advance firewalls and network security.[30]

B. The Telecommunications Act of 1996

On February 8, 1996, President Bill Clinton signed the Telecommunications Act of 1996 into law.[31] The Act was the first major overhaul of telecommunications law in almost sixty-two years.[32] With developments to the internet and changes to the telephone and television, the Act addressed newly emergent needs, but the President emphasized at the signing ceremony that a primary goal of the Act was "to connect America's classrooms and libraries to the [i]nternet by the year 2002."[33]

The E-Rate program—a mechanism to facilitate this connection—was created by Section 254(h)(1)(B) of the Act.[34] It states that:

> All telecommunications carriers . . . shall upon a bona fide request for any of its services that are within the definition of universal service . . . provide such services to elementary schools, secondary schools, and libraries for education purposes at rates less than the amounts charged for similar services to other parties.[35]

The Act authorizes the creation of the E-Rate program by expanding on the universal service principle to ensure schools and libraries have access to telecommunications services by offering discounts through the USF and giving the Commission the discretion to decide how the USF will be used.[36] Outside of the requirement that the services be for educational purposes and for connectivity, the Act is vague on what services qualify for E-Rate funds and gives discretion to the Commission.[37]

[30] *See generally* Klein, *supra* note 17.

[31] *President Clinton Signs the Telecommunications Act of 1996*, WHITE HOUSE (Feb. 8, 1996), https://clintonwhitehouse4.archives.gov/WH/EOP/OP/telecom/signing.html [perma.cc/LG5U-4DQJ] [hereinafter *President Clinton*].

[32] *The Telecommunications Act of 1996*, FCC (June 20, 2013), https://www.fcc.gov/general/telecommunications-act-1996 [perma.cc/9SRW-7TGW].

[33] *President Clinton*, *supra* note 31 (connecting America's classrooms and libraries to the Internet was an objective in President Clinton's State of the Union address).

[34] *See* 47 U.S.C. § 254(h)(1)(B).

[35] *Id.*

[36] *See* 47 U.S.C. § 254(a)(2); 47 U.S.C. § 254(h)(2)(A) (also requiring that the supported service be primarily used to support connectivity).

[37] *See* 47 U.S.C. § 254(c)(1)–(3); 47 U.S.C. § 254(a)(2); 47 U.S.C. § 254(h)(2)(A). The Act does not specify services by name. *See* § 254(c)(1)–(3). In the definitions section, the Act defines the Universal Service as "an evolving level of telecommunications services that the Commission shall establish periodically under this section, taking into account advances in telecommunications and information technologies and services." § 254(c)(1).

Additionally, Section 254(a)(1) of the Act requires the creation of a Federal-State Joint Board on Universal Service (the Joint Board) to make recommendations on implementing the universal service provisions of the Act.[38] Pursuant to the Section's mandate, the Joint Board was established in March 1996 and is comprised of FCC Commissioners, State Utility Commissioners, and a consumer advocate representative.[39] Section 254(a)(2) authorizes the Commission to initiate a single proceeding to implement the recommendations from the Joint Board.[40] It also instructs the Commission to include a definition of the services that are supported by the universal service support mechanisms and when they will be implemented.[41]

The Act includes guiding principles for the Commission's consideration when assigning the universal service's support mechanism including quality and rates, access to telecommunications services for schools, and other principles determined by the Joint Board.[42] These principles collectively demonstrate that the Act grants the Commission authority to decide what services qualify for the E-Rate program, and therefore also grants authority to the Commission to expand the E-Rate program to include advanced firewall and cybersecurity services, if it so chooses.[43] The Act further instructs that the Commission should take "into account advances in telecommunications and information technologies and services," and offers additional guidance to the Joint Board and the Commission in defining the supported services.[44] Sections 254(c)(1)(A)–(D) advise both

[38] *Federal-State Joint Board on Universal Service*, FCC, https://www.fcc.gov/general/federal-state-joint-board-universal-service [perma.cc/44ZL-9Z3N] (last visited Feb. 29, 2024) [hereinafter *Joint Board on Universal Service*]; 47 U.S.C. § 254(a)(1) ("Within one month after the date of enactment of the Telecommunications Act of 1996, the Commission shall institute and refer to a Federal-State Joint Board . . . to recommend changes to any of its regulations").

[39] *Joint Board on Universal Service*, *supra* note 38.

[40] 47 U.S.C. § 254(a)(2) ("The Commission shall initiate a single proceeding to implement the recommendations from the Joint Board required by paragraph (1) and shall complete such proceeding within 15 months after the date of enactment of the Telecommunications Act of 1996.").

[41] 47 U.S.C. § 254(a)(2) ("The rules established by such proceeding shall include a definition of the services that are supported by Federal universal service support mechanisms and a specific timetable for implementation.").

[42] *See* 47 U.S.C. § 254(b) ("(1) Quality and rates—ensuring services are "available at just, reasonable, and affordable rates"; (2) access to advanced telecommunications services; (3) access in rural and high cost areas; (4) equitable and nondiscriminatory contribution; (5) specific and predictable support mechanisms; (6) access to advanced telecommunications services for schools, health care, and libraries—elementary and secondary schools should have access to advanced telecommunications services; and (7) additional principals determined necessary by the Joint Board and the Commission for the protection of the public interest, convenience, and necessity.").

[43] *See* 47 U.S.C. § 254(b)(1), (2), (6), (7).

[44] 47 U.S.C. § 254(c)(1).

the Joint Board and the Commission to consider the extent to which the telecommunications services "(1) are essential to education, public health, or public safety; (2) have been subscribed to by a substantial majority of residential customers; (3) are being deployed in public telecommunications networks by telecommunications carriers; and (4) are consistent with public interest, convenience, and necessity."[45] Moreover, Section 254(c)(3) of the Act states that the "Commission may designate additional services for such support mechanisms for schools, libraries, and health care providers for the purpose of subsection (h)," the E-Rate program.[46] This vague language, omitting a definition for what these additional services include, gives the Commission broad discretion to determine additional services for the E-Rate program with the minimal requirement that they are essential to education and connectivity.[47]

Beyond the textual evidence, the Clinton administration's clear goal in signing the Act was to connect students to the internet.[48] At the Act's signing ceremony, Vice President Al Gore joined students virtually from Calvin Coolidge High School in Washington, D.C., to ask them how they thought the bill would impact their lives, and students had positive responses.[49] One student told the Vice President that "thanks to the telecommunications bill, [the student] believe[d] that it [would] open up new horizons for international access for cultures all over the world."[50] Another student replied that it would "make advances in technology readily available to a diverse group of people."[51] Since 1996, however, the internet and digital technologies have continued to advance, but the means to assure connectivity have remained relatively the same; without advanced cybersecurity services, schools are susceptible to

[45] *Id.*

[46] 47 U.S.C. § 254(c)(3).

[47] *See* 47 U.S.C. § 254(c); 47 U.S.C. § 254(a)(2); 47 U.S.C. § 254(h)(2)(A).

[48] *See* Guy Lamolinara, *Wired for the Future: President Clinton Signs the Telecom Act at LC*, LIBR. CONG. (Feb. 19, 1996), https://www.loc.gov/loc/lcib/9603/telecom.html [perma.cc/XU9K-Z33K]. Connecting classrooms and libraries to the internet was part of President Clinton's State of the Union address and was highlighted at the Telecommunications Act's signing. *Id.* The Act was the first bill to be signed in the Library of Congress, the first bill signed in cyberspace, and the event was available in real time over the internet. *Id.* The signing ceremony also included a virtual conversation between Vice President Al Gore and high school students about how the bill will help their lives. *See id.*

[49] *See id.*

[50] *Id.*

[51] *Id.*

harmful cyberattacks that thwart their ability to provide the intended connectivity to students nationwide.[52]

C. Joint Board Report of 1996 and the Report and Order of 1997

Vested with the authority to do so, the 1996 Joint Board Report helped the FCC create the first list of eligible services to be included in the E-Rate program.[53] In compliance with Section 254(a)(1) of the Act, on March 8, 1996, the FCC adopted a Notice of Proposed Rulemaking (NPRM) to "(1) define the services that will be supported by Federal universal service support mechanisms; (2) define those support mechanism; and (3) otherwise recommend changes to our regulations to implement the universal service directives of the 1996 Act."[54] After comments were received in April 1996, two additional Public Notices were released asking seventy-two questions about the universal service system and seeking comment in regard to proxy cost models.[55] The Joint Board reviewed the public responses to these questions and then issued recommendations on November 7, 1996.[56] In making their recommendations, the Joint Board advocated for schools to receive maximum flexibility to "purchase the packages of services they believe will meet their communications needs most effectively."[57] On May 8, 1997, the Commission released a Report and Order that implemented the Act's universal service provisions.[58]

The Report and Order agreed with the Joint Board that schools and libraries should have "maximum flexibility to purchase the package

[52] See Adam Stone, *E-Rate Funds Can Boost K-12 Cybersecurity*, EDTECH (March 15, 2023), https://edtechmagazine.com/k12/article/2023/03/e-rate-funds-can-boost-k-12-cybersecurity [perma.cc/2965-J56A] (explaining how schools can use cybersecurity solutions to strengthen their networks).

[53] *See E-Rate and Education*, *supra* note 14.

[54] Notice of Proposed Rulemaking and Order Establishing Joint Board, Order, CC Docket No. 96-45 (11 FCC Rcd. 18092) (1996) [hereinafter Order Establishing Joint Board].

[55] *E-Rate and Education*, *supra* note 14; Order Establishing Joint Board, *supra* note 54; Common Carrier Bureau Seeks Further Comment on Specific Questions in Universal Service Notice of Proposed Rulemaking, Public Notice, CC Docket No. 96-45 (11 FCC Rcd. 7750) (1996). These questions included definition issues; application to schools, libraries, and health care providers; the high-cost support system; proxy models; competitive bidding; the benchmark cost model; the cost proxy model; low-income consumers; and administration of universal service support. Common Carrier Bureau Seeks Further Comment on Specific Questions in Universal Service Notice of Proposed Rulemaking, Public Notice, CC Docket No. 96-45 (11 FCC Rcd. 7750) (1996).

[56] *E-Rate and Education*, *supra* note 14.

[57] Federal-State Bd. on Universal Serv., Recommended Decision, CC Docket No. 96-45 (12 FCC Rcd. 87) (1996).

[58] Federal-State Joint Bd. on Universal Serv., Report and Order, CC Docket No. 96-45 (12 FCC Rcd. 8776) (1997) [hereinafter Joint Board Report and Order].

of services they believe will meet their communications needs most effectively."[59] The Commission also reiterated that Section 254(c)(3) of the Act allowed the Commission to designate "additional services for such support mechanisms for schools," and explained that "given the varying needs and preferences of different schools and libraries and the relative advantages and disadvantages of different technologies, [they] agree[d] with the Joint Board that individual schools and libraries are in the best position to evaluate the relative costs and benefits of different services and technologies."[60] As the Joint Board observed, "permitting schools and libraries full flexibility to choose among telecommunications services also eliminates the potential risk that new technologies will remain unavailable to schools and libraries until the Commission has completed a subsequent proceeding to review evolving technological needs."[61] The FCC emphasized the Clinton administration's goal for passing the law—connecting students to the internet—stating that "the legislative history indicated that Congress intended to ensure that eligible schools and libraries have affordable access to modern telecommunications and information services that will enable them to provide educational services to all parts of the nation."[62]

Additionally, the Report and Order addressed a perceived limitation laid out in Section 254(h)(1)(B) of the Act, which specifically names telecommunications carriers as the entities to provide additional services as part of the E-Rate program.[63] The Commission clarified, however, that if "Congress intended to so limit the 254(c)(3) additional services . . . it would have used the phrase 'additional telecommunications services' rather than then broader term 'additional services' that it chose to use."[64] Against this backdrop, therefore, non-telecommunications carriers, like cybersecurity companies, can provide 254(c)(3) services through the E-Rate program by creating partnerships with telecommunications carriers.[65]

[59] *Id.*

[60] *Id.* at 228, 231.

[61] *Id.* at 232.

[62] *Id.* at 227.

[63] *See id.* at 235; 47 U.S.C. § 254(h)(1)(B) ("All telecommunications carriers serving a geographic area shall, upon a bona fide request for any of its services that are within the definition of universal service under subsection (c)(3), provide such services to elementary schools, secondary schools, and libraries for educational purposes at rates less than the amounts charged for similar services to other parties.").

[64] Joint Board Report and Order, *supra* note 58; *see* 57 U.S.C. § 254(c)(3) ("In addition to the services included in the definition of universal service under paragraph (1), the Commission may designate additional services for such support mechanisms for schools, libraries, and health care providers for the purposes of subsection (h).").

[65] Joint Board Report and Order, *supra* note 58; *see* 57 U.S.C. § 254(c)(3).

II. Alternative Solutions that Fail to Hit the Funding Mark

With more cyberattacks targeting K-12 schools occurring every day,[66] the FCC, other government agencies, Congress, and the Biden administration have all proposed solutions to help K-12 schools combat these devastating attacks.[67] While these solutions are a step in the right direction, they fail to fully resolve the immediate funding issue schools are facing.

A. E-Rate Pilot Program

On December 14, 2022, the FCC's Wireline Competition Bureau (WCB), the lead Bureau in ensuring "that all Americans have access to robust, affordable broadband and voice services,"[68] released a Public Notice seeking "comment[s] on requests to allow the use of E-Rate funds for advanced or next-generation firewalls and other network security services."[69] This Public Notice was part of FCC Chairwoman Jessica Rosenworcel's "Learn Without Limits" initiative to modernize the E-Rate program.[70] In a speech on June 26, 2023 Rosenworcel called on her fellow Commissioners to support the expansion of E-Rate funding in three phases.[71] The first phase was to expand the E-Rate program to support WiFi on school buses.[72] The second phase was to expand the E-Rate ESL to include WiFi hotspots in libraries and schools.[73] Lastly, the third phase was a proposed pilot program supporting the expansion of

[66] *See* Levin, *supra* note 4, at 3 (averaging the number of cyberattacks over the last six years, there is more than one cyberattack in K-12 schools per day).

[67] *See id.* at 20.

[68] *Wireline Competition*, FCC, https://www.fcc.gov/wireline-competition [perma.cc/B7LB-WL6S] (last visited Feb. 10, 2024).

[69] Wireline Competition Bureau Seeks Comment on Requests to Allow the Use of E-Rate Funds for Advanced or Next-Generation Firewalls and Other Network Security Services, Public Notice, WC Docket No. 13-184 (37 FCC Rcd. 14633) (2022) [hereinafter Wireline Competition Bureau].

[70] *See FCC Chairwoman Rosenworcel Takes Steps to Protect Schools Against Cyber Attacks*, FCC News (July 12, 2023), https://docs.fcc.gov/public/attachments/DOC-395069A1.pdf [perma.cc/D6NH-T7C6] [hereinafter *Rosenworcel Takes Steps*].

[71] *See id.*

[72] *See id.*; *FCC Announces E-Rate Funding Can Support Wi-Fi on School Buses*, FCC News (Oct. 19, 2023), https://docs.fcc.gov/public/attachments/DOC-397825A1.pdf [perma.cc/DR9A-VKS5]. The Commission voted on and approved this measure on October 19, 2023, enabling the expansion of the E-Rate program ESL to include WiFi on school buses starting in funding year 2024. *See generally* Jessica Rosenworcel, *Addressing the Homework Gap*, FCC (Feb. 1, 2021), https://www.fcc.gov/news-events/notes/2021/02/01/addressing-homework-gap [perma.cc/XH7H-7BLS].

[73] *Rosenworcel Takes Steps*, *supra* note 70.

the E-Rate program ESL to include cybersecurity and advanced firewall-related services to eligible K-12 schools.[74]

The WCB reports the ESL every funding year pursuant to Section 54.502(e) of the Commission's rules and provides guidance to schools on the eligibility of products and services under the E-Rate program.[75] Eligible services are divided into two categories:[76] Category One services include telecommunications services, telecommunications, and internet access,[77] and Category Two services include internal connections, basic maintenance, and managed internal broadband services.[78] Currently the E-Rate program only funds basic firewall services within both of these categories.[79] According to the funding year 2022 data, $230 million E-Rate program funds were used for Category One requests that included basic firewalls as part of the overarching services and over $16 million of funds was used for Category Two requests for basic firewall services and components.[80]

The comments responding to the 2022 WCB Public Notice addressed the definition of "advanced or next-generation firewalls and services," the specific cybersecurity equipment and services needed, and the impact that funding would have on the E-Rate program's goal of basic connectivity among other things.[81] With daily cyberattacks harming schools across the country, K-12 schools are increasingly interested in expanding E-Rate funding to include more advanced cybersecurity costs.[82] While the E-Rate program currently provides funds for basic firewall services, it has declined to extend the definition of basic firewall services to include "anti-virus and anti-spam software, intrusion protection and intrusion protection devices that monitor,

[74] This proposal also includes libraries. *Id.*

[75] *Eligible Service List*, UNIVERSAL SERV. ADMIN. CO., https://www.usac.org/e-rate/applicant-process/before-you-begin/eligible-services-list/ [perma.cc/DX4P-RKRP] (last visited Feb. 29, 2024); 47 C.F.R. § 54.502(e) ("The Administrator shall submit by March 30 of each year a draft list of services eligible for support, based on the Commission's rules for the following funding year.").

[76] Wireline Competition Bureau, *supra* note 69, at 4.

[77] *Id.*

[78] *Id.*

[79] Schools and Libraries Cybersecurity Pilot Program, Notice of Proposed Rulemaking, WC Docket No. 23-234 (FCC Rcd. 23-92) at 5 (2023) [hereinafter Pilot Program NPRM].

[80] *Id.*

[81] Wireline Competition Bureau, *supra* note 69. The public notice also sought comment on the categorization of firewall services and components, how to ensure applicants are making cost-effective choices; and comment on legal issues regarding the Commission's statutory authority to "extend E-Rate eligibility to advanced or next-generation firewalls and services." *Id.*

[82] *See id.* at 2–3 ("During the COVID-19 pandemic, several E-Rate stakeholders submitted petitions asking the Commission to reconsider the eligibility of advanced firewall and network security services given the increased use of schools' broadband networks to provide remote learning to their students.").

detect, and deter threats to a network from external and internal attacks, and other services to protect networks."[83] With an increase in broadband demand in schools, the Commission has attempted to refocus the E-Rate program from supporting legacy telecommunications services to supporting broadband services.[84] However, the Commission is still exploring how to handle cyberattacks as a result of the increase in broadband access.[85]

In response to the 2022 WCB Public Notice, the Commission received many comments, reply comments, and ex parte notices from schools, teachers, and school administrators across the country in addition to other E-Rate program stakeholders, like telecommunications and cybersecurity companies.[86] A majority of the responses were in favor of expanding the E-Rate program ESL to include next-generation firewalls and other, more advanced cybersecurity services.[87] Among the commentors was E-Rate Provider Services, LLC, a consulting firm serving service providers in the E-Rate program.[88] In favor of expansion, the firm justified its position as necessary because "networks can only help schoolchildren learn if they are functional . . . [b]asic firewalls, uninterruptible power supplies (UPSs) and redundant power supplies . . . met the criteria of devices which do not directly enable communication, but instead protect the equipment that does from mishap or attack."[89] Another commentor, the Deerfield Community School District in Wisconsin, stated that they are currently "unable to provide technology related services without adequate security tools."[90] Similar themes appeared from other commentors, like Pike County Schools in Troy, Alabama, which commented on how "cyberattacks pose a serious threat to the continuous delivery of the broadband connectivity E-Rate is designed to provide for schools."[91]

[83] *Id.*

[84] Pilot Program NPRM, *supra* note 79, at 3

[85] *See id.*

[86] *See Commission Documents*, FCC, WC Docket No. 13-184 (2022).

[87] *See id.* Commentors expressed that adding next-generation firewall and other cybersecurity services to the ESL would help schools combat cyberattacks and keep their networks safe. *Id.*

[88] *Id.*; E-Rate Provider Services, LLC, Reply Comment, WC Docket No. 13-184 (2023).

[89] E-Rate Provider Services, LLC, Reply Comment, WC Docket No. 13-184 (2023).

[90] Deerfield Community School District, Comment, WC Docket No. 13-184 (2023) ("Adequate security tools are expensive, so we fully support the modernizing of the E-Rate program.").

[91] Pike County Schools, Reply Comment, WC Docket No. 13-184 (2023). The Pike County Schools also noted that in 2021, their school network was attacked by a high school student who

The Learn Without Limits initiative is a huge step in the right direction—increasing accessibility to achieve the ultimate goal of widespread student connectivity.[92] The expansion of the E-Rate program ESL to include WiFi for school buses, for example, is the Commission's exercise of its discretionary authority under the Telecommunications Act of 1996 to expand the ESL in line with the underlying goals of the Act.[93] WiFi on school buses will enable students who do not have WiFi at home to complete their homework assignments on the bus ride home from school.[94] Although this need was not present in 1996 when the first ESL was written, the expansion of the ESL to add WiFi on school buses shows that the ESL can—and should—evolve with advancing technological needs.[95] Consistent with this adaptive line of thinking, adding advanced cybersecurity services to the ESL has become necessary for the FCC to keep up with advancing technology and continue supporting students connectivity to the internet.[96]

Schools need E-Rate funding for advanced cybersecurity services to combat growing cybersecurity needs.[97] Although the latest NPRM from the Commission proposes that the E-Rate pilot program provide up to $200 million over three years for schools to strengthen their cybersecurity systems, this is not enough money to solve the problem.[98] While some schools would receive immediate E-Rate program discounts to use for cybersecurity services,[99] $200 million over three years would not nearly be enough to make an effective impact on solving the current cybersecurity problem schools are facing. Schools need a more

did not want to participate in Spring testing. *Id.* The student brought down the county's entire network including phones by purchasing a Denial of Service attack for only thirty dollars. *Id.*

[92] *See Rosenworcel Takes Steps*, *supra* note 70.

[93] *See* FCC, *Fact Sheet Clarifying the Use of Wi-Fi on School Buses is Eligible for E-Rate Funding*, FCC (Sept. 28, 2023), https://docs.fcc.gov/public/attachments/DOC-397311A1.pdf [perma.cc/M56K-8SAW] [hereinafter *FCC Fact Sheet*].

[94] *See* Zachary Schermele, *Wi-Fi on the Way to School: How FCC Vote Could Impact Your Kid's Ride on the School Bus*, USA TODAY (Oct. 20, 2023, 9:14 AM), https://www.usatoday.com/story/news/education/2023/10/19/fcc-funding-wifi-school-buses/71240028007/ [perma.cc/8EHP-VSXL].

[95] *See FCC Fact Sheet*, *supra* note 93, at 2, 6. The Commission decided that WiFi on school buses fits within Section 254(h)(1)(B) of the act's requirement that telecommunications carrier to provide services to schools for educational purposes. *Id.* In 1996, students were less likely to need to access the internet to do their homework, but today the FCC has found WiFi essential for students to complete most of their homework. *Id.*

[96] *Id.* at 6. Similar to how the FCC expanded the ESL to include WiFi on school buses, the FCC must also add cybersecurity services to the ESL because it is essential for education purposes. *See id.*

[97] *See* Stone, *supra* note 52 (arguing that cybersecurity services are needed to protect student data and school networks).

[98] *See* Pilot Program NPRM, *supra* note 79, at 1–2, 8, 14, 16.

[99] *See* Pilot Program NPRM, *supra* note 79, at 8, 14.

permanent solution that will enable all eligible schools to utilize discounts to purchase necessary services before it is too late.

B. Federal Agency Recommendations

Beyond expansion of the FCC's E-Rate program, other government agencies have recommended alternative solutions to help schools receive necessary cybersecurity services to ensure a safe internet connection.[100] In a 2022 GAO report, GAO named the Department of Education as the lead agency, or sector risk management agency, for the education sector.[101] GAO called on the Department of Education and CISA to coordinate K-12 cybersecurity efforts and made four recommendations for how the Department of Education and the Department of Homeland Security could minimize cybersecurity risks in K-12 schools.[102]

GAO first recommended that the Department of Education and CISA establish a collaborative mechanism to coordinate cybersecurity efforts between agencies, including the FCC.[103] The second recommendation was that the Secretary of Education should "develop metrics for obtaining feedback to measure the effectiveness of [the Department of] Education's K-12 cybersecurity-related products and services."[104] The third recommendation was that the Department of Education "help school districts overcome the identified challenges and consider the identified opportunities for addressing cyber threats."[105] The last recommendation was for the Secretary of Homeland Security to ensure that CISA "develops metrics for measuring the effectiveness of its K-12 cybersecurity-related products and services."[106] Separate from the GAO report, the Department of Education also recently released recommendations in three K-12 Digital Infrastructure Briefs suggesting immediate steps that K-12 school districts can take to prevent cyber threats and attacks.[107]

[100] *See* W. WILLIAM RUSSELL, U.S. GOV'T ACCOUNTABILITY OFF., GAO-23-105380, CRITICAL INFRASTRUCTURE PROTECTION: ADDITIONAL FEDERAL COORDINATION IS NEEDED TO ENHANCE K-12 CYBERSECURITY 1 (2022).

[101] *Id.* ("The objectives of this report are to (1) determine what is known about the impact of cyber incidents, and (2) determine the extent to which key federal agencies coordinate with other federal and nonfederal entities to help K-12 schools combat cyber threats.").

[102] *Id.* at 31–32.

[103] *Id.* at 32.

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *See* U.S. DEP'T EDUC., K-12 DIGITAL INFRASTRUCTURE BRIEF: ADEQUATE AND FUTURE PROOF (2023); U.S. DEP'T EDUC., K-12 DIGITAL INFRASTRUCTURE BRIEF: PRIVACY ENHANCING,

While these recommendations rightfully put the Department of Education in charge of leading the solution to cyberattacks in schools,[108] the FCC should not wait for the Department of Education to coordinate with the other agencies or to receive feedback on products and services. For years, the Department of Education and CISA have failed to meet the expectations of a National Infrastructure Protection Plan and to create metrics to track the effectiveness of their services.[109] The Department of Education has also failed to update its K-12 cybersecurity guidance for over a decade.[110] Therefore, it is unlikely that the Department of Education will create a coordinated plan to address cyberattacks any time soon. By waiting for the Department of Education to find a solution first, schools remain vulnerable to devastating attacks and funds already available through the E-Rate program remain indefinitely unused.[111]

A separate report from the CoSN addressed the funding issues schools have in obtaining necessary cybersecurity products and services.[112] The report found that K-12 schools would need $2.389 billion from the E-Rate program to fund essential advanced security

INTEROPERABLE, AND USEFUL (2023); DEP'T. EDUC., K-12 INFRASTRUCTURE BRIEF: DEFENSIBLE & RESILIENT (2023). These briefs are a part of a series "on the key considerations facing educational leaders as they work to build and sustain core digital infrastructure for learning." DEP'T. EDUC., K-12 INFRASTRUCTURE BRIEF: DEFENSIBLE & RESILIENT (2023).

[108] *See* RUSSELL, *supra* note 100; *see also About ED: Overview and Mission Statement*, U.S. DEPT. EDUC., https://www2.ed.gov/about/landing.jhtml [perma.cc/ET84-TYSE] (last visited Feb. 10, 2024) (putting the Department of Education in charge of the solution to cyberattacks in schools is in line with the Department of Educations self-described mission "to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access.").

[109] *See* Benjamin Freed, *Feds Still Behind on K-12 Cybersecurity, Audit Finds*, STATESCOOP (Oct. 24, 2022), https://statescoop.com/feds-behind-k12-cybersecurity-audit/ [perma.cc/76GQ-G7CB].

[110] *Id.* Doug Levin, executive director of the K12 Security Information Exchange, has described the response from the Department of Education as if they have "been asleep at the wheel." *Id.*

[111] *See* Klein, *supra* note 17. The E-Rate program has an annual spending cap of $4.4 billion, however, it has used only around $2–2.5 billion in the past couple years. *Id.*; *Schools & Libraries USF Program*, *supra* note 13; *see also* 47 U.S.C. § 254. The Telecommunications Act of 1996 provides broad discretion to the FCC to expand the E-Rate program to keep up with advancements in technology. *See* 47 U.S.C. § 254.

[112] *See* COSN & FUNDS FOR LEARNING, E-RATE CYBERSECURITY COST ESTIMATE 3 (2021) [hereinafter COSN & FUNDS FOR LEARNING]; *CoSN, SETDA, SECA, All4Ed, SHLB and CGCS Submit E-Rate Cybersecurity Cost Estimate to FCC*, COSN, https://www.cosn.org/cosn-news/cosn-setda-seca-all4ed-shlb-and-cgcs-submit-e-rate-cybersecurity-cost-estimate-to-fcc/ [perma.cc/PM9D-UD9H] (last visited Feb. 10, 2024) [hereinafter *CoSN: Rate Cybersecurity Cost Estimate to FCC*] ("The cost estimates are based on an analysis of five-year price models for third-party hardware, software and cloud-based services used to guard schools from online attacks.").

services—services that they currently lack access to.[113] CISA released a similar report in January 2023 recommending that K-12 schools leverage the State and Local Cybersecurity Grant Program (SLCGP).[114] This grant is managed by CISA and the Federal Emergency Management Agency (FEMA) and will provide grants totaling $1 billion over the next four years.[115] The SLCGP is available to state, local, territorial, and tribal governments broadly to reduce cyber risk, and K-12 public schools are eligible for the grant money because they are a government service.[116] K-12 schools are also eligible to leverage the Homeland Security Grant Program (HSGP).[117] The HSGP includes "grants to assist state, local, tribal, and territorial efforts in preventing, protecting against, mitigating, responding to and recovering from acts of terrorism and other threats," and dedicates 7.5 percent of its funds to support cybersecurity infrastructure.[118] While the CISA report makes recommendation to help schools obtain grant funding to purchase cybersecurity services and products, directing schools toward multiple grant programs to obtain sufficient funds is a complicated solution that may lead to more unnecessary complexities for schools to obtain adequate funding for their cybersecurity services.

C. Congressional Legislation

Members of the US Congress have also introduced legislation to address the increase of cyber risks in K-12 schools.[119] In April 2023, a bipartisan group of lawmakers in both the House of Representatives

[113] *See* COSN & FUNDS FOR LEARNING, *supra* note 112, at 4, 16. This report makes recommendations to handle the funding issue. *Id.* The recommendations included: (1) that the FCC should adopt a broadband definition that includes minimum cybersecurity protections; (2) the USAC should treat all firewalls as "basic"; and (3) the FCC should increase the five-year Category 2 budget cap by $81 per student to cover basic firewalls. *Id.*

[114] U.S. DEP'T HOMELAND SEC. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, PROTECTING OUR FUTURE: PARTNERING TO SAFEGUARD K-12 ORGANIZATIONS FROM CYBERSECURITY THREATS 2, 16 (2023) [hereinafter PROTECTING OUR FUTURE] (analyzing and making recommendations on the state of K-12 cybersecurity measures).

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] *Homeland Security Grant Program*, FEMA, https://www.fema.gov/grants/preparedness/homeland-security#funding-totals [perma.cc/NAV7-ULQ4] (last visited Mar. 1, 2024); *see* PROTECTING OUR FUTURE, *supra* note 114, at 16.

[119] *See* Enhancing K-12 Cybersecurity Act, H.R. 2845, 118th Cong. (2023). This bill did not make it past introduction in the US House of Representatives. *See id.*; *see also* Enhancing K-12 Cybersecurity Act, S. 1191, 118th Cong. (2023). This bill did not make it past introduction in the US Senate. *See* S. 1191.

and the Senate reintroduced the Enhancing K-12 Cybersecurity Act.[120] The legislation directs CISA to establish a school cybersecurity information exchange, as well as a cybersecurity incident registry, and creates a K-12 cybersecurity technology improvement program.[121] The cybersecurity information exchange would create a website that disseminates information, cybersecurity best practices, training, and lessons learned for schools to access and the cybersecurity incident registry would serve as a universal place for schools to report cyberattacks. [122] The data collected from this registry would then be used to help CISA improve its cybersecurity response.[123] The K-12 cybersecurity technology improvement program would deploy cybersecurity capabilities to address cybersecurity risks and threats to information systems of K-12 schools.[124]

Some have expressed concern that "[i]f there is not a direct return to the organization who is submitting that information, it just feels like an unfunded mandate. If the data goes into a black hole and if they're not seeing a benefit, it can be difficult to convince people to do that work."[125] These concerns are legitimate; while there is good reason to track cyberattacks at schools, creating a reporting requirement will not immediately solve the current cyber threats schools are facing.[126] Additionally, while the legislation may be funded up to $20 million to address cyber risks and threats broadly, the legislation provides no explicit guidance or limits on how this money should be allocated.[127] With schools losing between $50,000 to $1 million per cyberattack, however, $20 million will not come close to covering the needs of all schools nationwide.[128]

[120] *See* H.R. 2845; S. 1191; Lauraine Langreo, *Lawmakers Reintroduce K-12 Cybersecurity Bill*, GOV'T TECH. (Apr. 24, 2023), https://www.govtech.com/education/k-12/lawmakers-reintroduce-k-12-cybersecurity-bill [perma.cc/ZVS7-AY3P]. This bill was reintroduced in response to the increase in cyberattacks targeting schools. *Id.*

[121] *See* H.R. 2845 § 2(a)–(b); S. 1191 § 3(a)–(b).

[122] *See* H.R. 2845 § 2(a); S. 1191 § 3(a).

[123] *See* H.R. 2845 § 3(b); S. 1191 § 4(b).

[124] *See* S. 1191 § 5(a); H.R. 2845 § 4(a). This would be accomplished through "(1) developing cybersecurity strategies and installation of effective cybersecurity tools tailored for K-12 schools; (2) making available services that enhance the ability of K-12 schools to protect themselves from ransomware and other cybersecurity threats; and (3) continuing training opportunities on cybersecurity threats, best practices, and relevant technologies for K-12 schools." H.R. 2845 § 4(a).

[125] Langreo, *supra* note 120.

[126] *See id.*

[127] *See id.*

[128] *See As Cyberattacks Increase*, *supra* note 7.

In 2021, Congress passed the Cybersecurity Act of 2021.[129] This legislation, which became law on October 8, 2021, instructs the Director of CISA to

> (1) conduct a study to analyze how certain cybersecurity risks specifically impacted K-12 educational institutions; (2) evaluate the cybersecurity challenges K-12 educational institutions faced when implementing cybersecurity protocols and securing information systems and data; (3) identify cybersecurity challenges related to remote learning; and (4) evaluate the most accessible ways to communicate cybersecurity recommendations and tools.[130]

As a result, CISA published a report in January 2023 recommending that K-12 schools make investments in cybersecurity measures, address cybersecurity resource limitation, and collaborate through information sharing.[131] While the Cybersecurity Act of 2021 produced positive impacts on schools, neither the law nor the resulting CISA report solved the funding problem that schools have when looking to purchase cybersecurity equipment and services.[132] The CISA report instead recommended steps schools can take to maximize their cybersecurity budgets by

> (1) working with the state planning committee to leverage the State and Local Cybersecurity Grant Program (SLCGP); (2) utilize free or low-cost services to make near-term improvements in resource-constrained environments; (3) expect and call for technology providers to enable strong security controls by default for no additional charge; and (4) minimize the burden of security by migrating IT services to more secure cloud versions.[133]

In addition to these recommendations, CISA also provided an online tool kit with resources and materials to help achieve CISA's recommendations.[134] While these recommendations and the tool kit are helpful, it is unlikely that schools will know how to utilize all of these resources to the fullest effect and will still require additional funding to purchase equipment and services needed to combat their cybersecurity risks.

[129] K-12 Cybersecurity Act of 2021, Pub. L. No. 117-47, 135 Stat. 397 (2021) (codified as amended at 6 U.S.C. § 652).

[130] K-12 Cybersecurity Act of 2021 § 3(b)(1).

[131] PROTECTING OUR FUTURE, *supra* note 114, at 11–12; *see also CISA Releases Protecting Our Future: Partnering to Safeguard K-12 Organizations From Cybersecurity Threats*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Jan. 24, 2023), https://www.cisa.gov/news-events/alerts/2023/01/24/cisa-releases-protecting-our-future-partnering-safeguard-k-12 [perma.cc/KTW7-QCXH] [hereinafter *CISA: Partnering to Safeguard*].

[132] *See* PROTECTING OUR FUTURE, *supra* note 114, at 16.

[133] *Id*. at 16–17.

[134] *Online Toolkit: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/online-toolkit-partnering-safeguard-k-12-organizations-cybersecurity-threats [perma.cc/U7AC-K5YT] (last visited Mar. 1, 2024); *see CISA: Partnering to Safeguard*, *supra* note 131.

D. Biden-Harris Administration

Within the executive branch, on August 7, 2023, President Biden announced new efforts to strengthen cybersecurity in America's K-12 schools.[135] The President highlighted additional action coming from the Department of Education including its establishing of a Government Coordinating Council to coordinate cybersecurity policies amongst education leaders from all levels of government.[136] He also described additional cybersecurity training for K-12 entities from CISA and resource guides updated by the FBI and National Guard Bureau for educators to learn how to report cybersecurity incidents.[137] Additionally, President Biden shared that many education technology providers, including Amazon Web Services, Cloudflare, PowerSchool, Google, and D2L, had committed to provide free and low-cost cybersecurity resources to schools.[138] While all of these programs may prove helpful in combating the cybersecurity issue in schools, they do not provide schools with the immediate funding they need to directly address the current cybersecurity risks they face.[139] Even though these education technology companies are independently offering discounts and cybersecurity training,[140] schools that need funding may not qualify for a specifically tailored program or the program may not offer the essential cybersecurity service that a school needs.[141] Schools are confined to the policies of these companies programs and lack the flexibility to use funds for what they may need the most.[142]

[135] *Biden-Harris Administration Launches New Efforts to Strengthen America's K-12 Schools' Cybersecurity*, WHITE HOUSE (Aug. 7, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/07/biden-harris-administration-launches-new-efforts-to-strengthen-americas-k-12-schools-cybersecurity/ [perma.cc/LC2X-EHKP].

[136] *Id.*

[137] *See id.*

[138] *Id.*

[139] *See id.*

[140] *See id.* These discounts are provided directly from the private companies. *Id.* Amazon Web Services, for example, is committing $20 million for a K-12 cyber grant program while Cloudflare is offering a suite of free Zero Trust cybersecurity solutions to small public school districts. *See id.*

[141] *See id.* For example, a large school may also need funding but does not qualify for Cloudflare's offer. *See id.*

[142] *See id.* A school who wants to utilize Amazon Web Services' program will only be able to use the funds for training and security reviews. *See id.*

III. Solution: Expanding the E-Rate Program ESL, Providing Guidance to Schools, and Combining Grant Programs

A. Expanding the E-Rate Program ESL

The FCC should expand the E-Rate program ESL to include advanced or next-generation firewalls and other network security services because this expansion is the most effective and efficient way for schools to affordably purchase necessary cybersecurity services to protect their schools from cyberattacks. The FCC has proposed a pilot program within the USF to provide up to $200 million over three years for schools to strengthen their cybersecurity systems,[143] and although the current efforts to create a pilot program are a step in the right direction, more must be done. $200 million over three years is not enough for every school requiring funding to purchase the necessary cybersecurity services.[144] The FCC should go a step further and immediately adopt advanced cybersecurity services within its ESL to meaningfully effectuate a resolution for schools.

Schools and other E-Rate program stakeholders have requested that the FCC use its authority under the Telecommunications Act to expand the ESL to include cybersecurity services,[145] however the Commission declined to make this expansion despite the rapid increase in cyberattacks in schools.[146] In the 2023 ESL, the Commission acknowledged the requests to add advanced or next-generation firewalls or other network security services to the ESL but explained that they were not willing to add them at that time.[147] Basic firewall services that are bundled with other internet access services are already included in the 2023 ESL Category One supported services,[148] and other basic firewall services and firewall components are included in the 2023 ESL Category Two supported services;[149] however, what

[143] *See* Pilot Program NPRM, *supra* note 79, at 1–2. This is separate from the E-Rate program for now and requires a full vote from the commission to pass. *See id.* This proposal is the third phase of the Chairwoman's "Learn Without Limits" initiative to modernize the E-Rate programs. *Rosenworcel Takes Steps*, *supra* note 70.

[144] *See* COSN & FUNDS FOR LEARNING, *supra* note 112, at 4. The report found that K-12 schools would need $2.389 billion from the E-Rate program to fund needed advanced security services. *Id.*

[145] *See* Cisco Petition, *supra* note 3, at 1; CoSN Petition, *supra* note 8, at 2; FFL Letters, *supra* note 8; AASA Letter, *supra* note 8.

[146] Modernizing the E-Rate Program, *supra* note 13.

[147] *Id.*

[148] *See id.* at 14620.

[149] *Id.* at 14622.

qualifies for cybersecurity purposes under these categories is insufficient.[150]

"Firewall" is currently defined in the E-Rate program 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."[151] Schools are only able to obtain very basic firewall protections through the existing E-Rate program because of this definition.[152] The Commission has failed to extend the ESL to include "anti-virus and anti-spam software, intrusion protection and prevention devices that monitor, detect, and deter threats to a network from external and internal attacks."[153]

Allowing funding for advanced cybersecurity services—by extending the upcoming ESL to include these important protections—could save schools millions of dollars incurred as a result of cyberattacks.[154] More than 350,000 new malware programs are created every day, increasing opportunities for these attacks to take place while schools remain vulnerable.[155] By expanding the ESL to include services like antivirus and anti-spam software, schools will be able to better detect and prevent dangerous malware from attacking their computer systems.[156] This inclusion would not only save schools millions of dollars but also keep their doors open and protect confidential student data like their home addresses, grades, and classroom assignments from harmful hackers.[157]

If in receipt of adequate funding, schools may obtain additional protections by hiring proper cybersecurity or information technology

[150] *See id.* Currently only basic firewalls are included in the ESL. *Id.* But, schools need more advanced cybersecurity services to keep up with growing cyberattacks. *See* CoSN Petition, *supra* note 8, at 2.

[151] *ESL-Glossary*, UNIVERSAL SERV. ADMIN. CO., https://www.usac.org/wp-content/uploads/e-rate/documents/ESL-Glossary.pdf [perma.cc/ED8J-F52L] (last visited Feb. 21, 2024).

[152] *See* Pilot Program NPRM, *supra* note 79, at 22–23.

[153] *Id.* at 9.

[154] *See As Cyberattacks Increase*, *supra* note 7. The GAO reported that each school district loses between $50,000 to $1 million per cyberattack. *Id.*

[155] Aliza Vigderman & Gabe Turner, *Does Antivirus Stop Hackers?*, SECURITY.ORG (Jan. 2, 2024), https://www.security.org/antivirus/hackers/ [perma.cc/9DD9-F8RA].

[156] *See id.* Antivirus software automatically scans files, directories, and media received from outside sources before being opened to ensure they do not contain harmful viruses that can destroy the school's computer system. *Id.* Some antivirus software systems are even capable of neutralizing and disposing malware once it is detected. *Id.* Anti-spam software can detect malicious emails that could divulge personal and confidential information by opening them. *Id.* Further, anti-spam software can detect malicious e-mails that could divulge personal and confidential information by opening them. *See As Cyberattacks Increase*, *supra* note 7.

[157] *See As Cyberattacks Increase*, *supra* note 7; Vigderman & Turner, *supra* note 155.

(IT) staff.[158] Many cyberattacks happen because of human error, such as falling for phishing attacks or accidentally giving scammers passwords and other credentials.[159] By hiring an IT professional, schools could more easily train students, teachers, and other faculty to take precautions to protect school data like using more complex passwords or using multifactor authentication.[160] With technology constantly evolving, having a dedicated IT professional to continuously train the school community could prevent schools from falling victim to a serious cyberattack and allow school community members to carry such skills forward.[161] Moreover, IT professionals may lower the risk of telecommunications and cybersecurity companies committing fraud by tricking schools into buying more services than needed.[162] These professionals would have the expertise to inform schools on what cybersecurity products are actually needed for their specific school, ultimately saving schools and the E-Rate program money.

B. Providing Guidance to Schools

In addition to expanding the E-Rate program, the FCC would be well-advised to provide guidance to schools on how they can appropriately use cybersecurity E-Rate discounts to achieve protected connectivity. Eligible schools can receive discounts that range from 20 to 90 percent of the costs of eligible services.[163] With cybersecurity needs that vary by school, the Commission should provide individualized guidance to schools on appropriate uses of E-Rate discounts under an expanded ESL. For example, currently only one-third of school districts have a full-time employee dedicated to cybersecurity.[164] It may be appropriate for smaller school districts to share a cybersecurity professional amongst schools, but for larger school districts, a designated cybersecurity professional may be required at each individual school. While the Commission could evaluate these unique needs on a case-by-case basis, the option of using E-Rate funding for cybersecurity products and services, including an IT professional,

[158] *See* Micah Castelo, *Cyber Security in Schools: Attacks Increasingly Threaten Districts*, EDTECH (June 17, 2020), https://edtechmagazine.com/k12/article/2020/06/cyberattacks-increasingly-threaten-schools-heres-what-know-perfcon [perma.cc/56LS-ZX4U].

[159] *Id.*

[160] *See id.*

[161] *See id.*

[162] *See generally id.*

[163] *Schools & Libraries USF Program*, *supra* note 13.

[164] U.S. DEP'T EDUC., OFF. EDUC. TECH., K-12 DIGITAL INFRASTRUCTURE BRIEF: DEFENSIBLE & RESILIENT 8 (2023), https://tech.ed.gov/files/2023/08/DOEd-Report_20230804_-508c.pdf [perma.cc/BYS7-972P].

training for students, teachers, and faculty, as well as cybersecurity equipment, should be included under the umbrella of advance cybersecurity services on the ESL.

Guidance and adequate case-by-case consideration are particularly necessary because of the risk that telecommunications, computer, and cybersecurity companies may take advantage of schools knowing that the schools are able to access E-Rate funds for their services.[165] Historically, some computer and telecommunications companies have convinced poor and technologically unsavvy school districts to buy more equipment or services than they need or simply just overcharge for their services.[166]

Despite the clear stance by the FCC that E-Rate program service providers must provide the lowest price charged to similarly situated customers,[167] and that schools are required to participate in a competitive bidding process when seeking E-Rate funds,[168] fraud is still a risk to both companies offering these services and schools receiving them.[169] Fraud by telecommunications companies has occurred in the past because they failed to offer the lowest price and instead charged schools with the highest price possible.[170] Additionally, schools have also committed fraud by failing to participate in the competitive bidding process when they have a personal interest in using a particular provider.[171] It is thus important for the Commission to keep the risks that may result from expanding the ESL in mind, and it is equally important for the Commission to provide guidance to schools on

[165] *See* Jonathan Meer, *Highway Robbery Online: Is E-Rate Worth the Fraud?*, 2006 BYU EDUC. & L.J. 323, 324 (2006) (explaining types of fraud that occur in the E-Rate program).

[166] *Id.*; *see* U.S. ex rel. Health v. Wis. Bell, Inc., 75 F.4th 778, 782–83 (7th Cir. 2023) (discussing whether Wisconsin Bell committed fraud when its sales representatives followed normal private business protocol and offered schools and libraries the highest prices whenever possible because the E-Rate program requires them to offer the lowest price charged to similarly situated customers).

[167] *See Wis. Bell*, 75 F.4th at 781; 47 C.F.R. § 54.500.

[168] *See Step 1: Competitive Bidding*, UNIVERSAL SERV. ADMIN. CO., https://www.usac.org/e-rate/applicant-process/competitive-bidding [perma.cc/4BHA-MTX6] (last visited Feb. 10, 2024) (describing the competitive bidding process that requires schools to select the most cost-effective provider).

[169] *See Wis. Bell*, 75 F.4th at 782; Basic Servs., Inc. v. Gov't of the Virgin Islands, 2020 VI LEXIS *80 at *1 (Super. Ct. Dec. 10, 2020); SETO J. BAGDOYAN, U.S. GOV'T ACCOUNTABILITY OFF., GAO-20-606, FCC SHOULD TAKE ACTION TO BETTER MANAGE PERSISTENT FRAUD RISKS IN THE SCHOOLS AND LIBRARIES PROGRAM (2020) (responding to a report on the E-Rate program's fraud risks and how the FCC and USAC manage fraud risks).

[170] *Cf. Wis. Bell*, 75 F.4th at 782 (Knowing of the E-Rate program's lowest price rule, Wisconsin Bell did not train its sales representatives on the rule and even instructed the sales representatives to offer the highest prices "whenever possible").

[171] *See also Basic Services*, 2020 VI at *1-3.

appropriate uses of E-Rate discounts under the expansion of allowing advanced firewall services on the ESL.[172]

With the addition of cybersecurity service to the E-Rate program ESL, the FCC should also add cybersecurity services to its E-Rate discount application process. As it stands, to apply for an E-Rate discount, the school must first create an account in the E-Rate Productivity Center to submit their applications.[173] When reviewing the various forms necessary for applying for E-Rate discounts, the USAC already considers each school's request on an individual basis; however, the USAC should add the schools' cybersecurity needs to its review process.[174]

The first step for schools in applying for E-Rate discounts is to enter the competitive bidding process by submitting FCC form 470.[175] Integrating cybersecurity services into the competitive bidding process would ensure that there is minimal fraud in the pricing of the cybersecurity services provided to schools. After the cybersecurity service provider is selected, the applicant must apply for the discount by submitting FCC form 471.[176] On this form, the applicant schools should be able to list their individual cybersecurity needs for the USAC's review.[177] Then, the USAC should approve discount requests on a case-by-case basis, allowing for consideration of a variety of cybersecurity services capable of accommodating advancements in technology.

C. Partnering with CISA and FEMA to Combine Grant Programming

In order to guarantee sufficient funding for schools to purchase necessary cybersecurity services, the FCC should also partner with CISA and FEMA to combine grant programming through a joint application.[178] The 2022 GAO report highlighted that the Department of Education, CISA, the FBI, and the FCC should assist schools in protecting against cyber threats;[179] however, there is currently no

[172] *See* BAGDOYAN, *supra* note 169.

[173] UNIVERSAL SERV. ADMIN. CO., SCHOOLS AND LIBRARIES (E-RATE) PROGRAM OVERVIEW 3, 5 (2019).

[174] *See id.* at 5 ("After the FCC Form 471 is certified, USAC reviews the data on the form to verify all of the funding requests on the form are accurate and compliant with E-Rate Program rules.").

[175] *Id.* at 4.

[176] *Id.* at 5.

[177] *Id.*

[178] This application would be located in one form on the official government website for grant program applications.

[179] RUSSELL, *supra* note 100, at 4.

formal mechanism for coordinating between the agencies.[180] GAO's recommendations for preventing cyberattacks to schools were all based on coordination between the agencies and creating mechanisms to obtain feedback on the effectiveness of cyber-related products and do not address immediate funding for cybersecurity products and services or how these agency's grant programs could be combined.[181] While the report notes there is a need for additional cybersecurity funding for schools and explains the issue that "covering advanced cybersecurity services for school districts [with the E-Rate program] would likely exceed the funding allocation for the whole program," it does not offer a solution for obtaining adequate cybersecurity funds or address a consolidation mechanism for the various agency grant programs that already exist.[182]

Additionally, if the estimates that schools will need $2.389 billion to purchase necessary cybersecurity products and services are correct,[183] creating a joint application so schools can apply for E-Rate, SLCGP, and HSGP funds simultaneously would ensure there are enough funds to support school's cybersecurity needs without schools having to go to multiple places to apply for these programs.[184] Schools may miss out on grant money and other funding opportunities because they do not know they exist or because the applications are too complicated.[185] By streamlining the process, schools are given the best opportunity for receiving the funding they need and specific government programs like E-Rate are less likely to run out of funds.[186]

IV. CONCLUSION

With emergent and advancing technologies that are increasing the connectivity needs of students and threats to schools' cybersecurity, an expansion of the E-Rate program's ESL to include advanced cybersecurity services is long overdue. Cyberattack rates in schools are increasing every day, leaving intimate and valuable data vulnerable to

[180] *Id.* at 22.

[181] *See id.* at 32.

[182] *Id.* at 30.

[183] *See* COSN & FUNDS FOR LEARNING, *supra* note 112, at 4.

[184] *See CoSN: Rate Cybersecurity Cost Estimate to FCC*, *supra* note 112.

[185] *See* Justin Schweitzer, *How to Address the Administrative Burdens of Accessing the Safety Net*, CTR. FOR AM. PROGRESS (May 5, 2022), https://www.americanprogress.org/article/how-to-address-the-administrative-burdens-of-accessing-the-safety-net/ [perma.cc/C92N-CKEH] (explaining how administrative burdens can prevent people from taking advantage of government programs).

[186] *See id.*

attack.[187] Not only do students suffer, but schools have been forced to shut down due to attacks, leaving students out of school for days or even weeks.[188] School districts that cannot afford cybersecurity expansions are left with losses averaging between $50,000 to $1 million per attack that they do not have the funds to mitigate, and current resolutions have not fixed the problem.[189] As such, vested with the authority of the Telecommunications Act of 1996 to expand the ESL, the FCC must include advanced or next-generation firewalls and other network security services to the E-Rate program's ESL immediately.[190] The FCC would be well-advised to also provide guidance to schools on how to appropriately use E-Rate discounts to achieve safe connectivity, and partner with CISA and FEMA to combine cybersecurity grant programming through a joint application. By taking these steps, K-12 schools would be able to better protect their students and themselves from cyberattacks—allowing them to keep their doors open, protect students' private data, and ultimately provide education to their students without a looming threat of cyberattacks.

Madeline Strasser[*]

[187] *See* LEVIN, *supra* note 4, at 3–4.

[188] *See As Cyberattacks Increase, supra* note 7.

[189] *Id.*; LEVIN, *supra* note 4, at 8–9.

[190] *See* 47 U.S.C. § 254.

[*] JD Candidate, Vanderbilt University Law School, 2025; BA, The Pennsylvania State University, 2017. The Author would like to thank the editorial staff of the Vanderbilt Journal of Entertainment & Technology Law for their assistance and guidance throughout writing this note. The Author would also like to thank Coach and her family for their unwavering support and encouragement during law school and beyond.