Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

PETITION FOR WAIVER OF CISCO SYSTEMS, INC.

Jeffrey A. Campbell
Senior Vice President, Government Affairs
and Public Policy
Cisco Systems, Inc.
601 Pennsylvania Ave., NW
North Building, Ninth Floor
Washington, DC 20004
(202) 354-2920

August 20, 2020

TABLE OF CONTENTS

FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

PETITION FOR WAIVER OF CISCO SYSTEMS, INC.

Cisco Systems, Inc. ("Cisco") submits this request that the Commission exercise its waiver authority to allow schools to use E-rate Category 2 funding to cover the costs of network security software in the 2020 and 2021 funding years.[1]

I.   INTRODUCTION AND SUMMARY

The sudden and widespread shift to remote learning due to the COVID-19 pandemic has vastly increased the vulnerability of schools' and libraries' networks to cyberattacks.[2] According to a security tracking firm, educational networks currently face more cyberattacks than any type of network, receiving five *times* more attacks than the next most-attacked category

---

[1] *See* 47 C.F.R. § 1.3 (Commission may waive its rules for good cause shown); *see also id.* at § 0.91(b) (Wireline Competition Bureau may "[a]ct on requests for interpretation or waiver of rules").

[2] *See, e.g.,* Lily Hay Newman, "Schools Already Struggled With Cybersecurity. Then Came COVID-19," WIRED (July 1, 2020) ("Newman"), https://www.wired.com/story/schools-already-struggled-cybersecurity-then-came-covid-19/; Jake Maher, "Coronavirus Compounds K-12 Cybersecurity Problems: 5 Areas of Watch," EDUCATION WEEK (March 17, 2020) ("Maher"), https://www.edweek.org/ew/articles/2020/03/18/coronavirus-compounds-k-12-cybersecurity-problems-5-areas.html; Micah Castelo, "Cyberattacks Increasingly Threaten Schools – Here's What to Know," EDTECH MAGAZINE (June 17, 2020) ("Castelo"), https://edtechmagazine.com/k12/article/2020/06/cyberattacks-increasingly-threaten-schools-heres-what-know-perfcon; Bradley Barth, "Rush to Adopt Online Learning Under COVID-19 Exposes Schools to Cyberattacks," SC NEWS (April 6, 2020) ("Barth"), https://www.scmagazine.com/home/security-news/news-archive/coronavirus/race-to-adopt-online-learning-under-covid-19-exposes-schools-to-cyberattacks/.

of users.[3] Although the Commission has previously declined to provide support for network

security software, the exigency of the COVID-19 response makes such support critical now.[4]

Moreover, there is no reason not to do so. The Category 2 budget caps create firm discipline on

spending, and there is over $1.5 billion in unused funding available under the overall E-rate

budget cap.[5] Using waiver authority to support network security software in the 2020 and 2021

funding years will provide schools and libraries with an important tool to address new demands

placed on them by the response to COVID-19, consistent with other pandemic-related waivers

that the Commission has granted, and will help protect the Commission's existing investments in

Category 2 networks.

II.   PRESSED BY THE NEW EXIGENCIES OF COVID-RELATED DISTANCE LEARNING, SCHOOLS AND LIBRARIES FACE AN UNPRECEDENTED SIEGE OF CYBERATTACKS

School and library network, which were already struggling to stay ahead of cybersecurity

threats, are facing unprecedented security challenges as they attempt to respond to the new

demands of the COVID-19 pandemic. "With the increased use of technology for teaching,

learning, and continuing school operations in today's remote environment, schools have also

become more vulnerable to cyberattacks."[6] For example, in June, the Federal Bureau of

Investigations ("FBI") issued a security alert to K-12 schools regarding a spike in ransomware

---

[3] *See* Newman at 1.

[4] Although the deployment of technologies for remote learning has created the circumstances necessitating a waiver, *this petition does not seek support for off-campus services*. Rather, it simply seeks support for network security measures to protect existing E-rate-supported local area networks ("LANs") and wireless local area networks ("WLANs").

[5] *Wireline Competition Bureau Directs USAC to Fully Fund Eligible Category One and Category Two E-rate Requests,* Public Notice, 35 FCC Rcd 6756 (WCB 2020) ("*2020 E-rate Funding Public Notice*") (estimating total demand for funding year 2020 at $2.91 billion out of the overall $4.23 billion budget cap, plus $500 million in rollover funds from previous years).

[6] Castelo at 1.

attacks that exploit educational remote desktop protocol connections during the pandemic.[7] This

followed an FBI warning to schools in March about security threats to video conferencing and

virtual classroom software deployed in response to the COVID crisis.[8] As Funds For Learning

recently stated, "[w]e know that attacks on school and library networks are occurring, that they

are growing in frequency, and that they account for a significant amount of network downtime."[9]

Experts studying the school cybersecurity crisis identify a lack of resources as one of the

primary challenges that prevents schools from adequately addressing these threats to their

networks.[10] Thus, E-rate support can make a significant difference in helping to avoid harm to

schools' and libraries' networks. Significantly, the waiver requested herein would allow E-rate

funding to be used to protect the same internal networks that E-rate currently funds. As such,

funding network security measures will protect the Commission's investment in schools' internal

networks and advance E-rate goals. "Today, broadband networks cannot function without

security, monitoring, and related services."[11] Stated another way, a high-quality, high-speed

internal network funded by E-rate is of no value to a school or library if it is taken offline by a

cyberattack.

---

[7] Catalin Cimpanu, "FBI Warns K-12 Schools of Ransomware Attacks via RDP," ZDNET (June 25, 2020) ("Cimpanu"), https://www.zdnet.com/article/fbi-warns-k12-schools-of-ransomware-attacks-via-rdp/.

[8] FBI, "FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic," Press Release (March 30, 2020), https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.

[9] Comments of Funds for Learning, LLC on Proposed Eligible Services List for Schools and Libraries Universal Service Program Funding for Funding Year 2021, WC Docket No. 13-184, at 3 (filed Aug. 14, 2020) ("FFL 2021 ESL Comments").

[10] *See, e.g.,* Castelo at 1-2.

[11] FFL 2021 ESL Comments at i.

While there were early hopes that these problems might subside if students and staff returned to full-time in-person instruction for the fall 2020 term, it has become clear that many school districts and libraries will need to continue online instruction and telework to minimize the spread of the coronavirus. It is therefore appropriate for the Commission to issue a waiver to allow schools to deploy advance network protection technology in the near term, and through the next funding year.

III. THE COMMISSION'S RATIONALE FOR NOT SUPPORTING NETWORK SECURITY NO LONGER HOLDS

In 2014, in connection with the establishment of the new Category 2 per-school budget rules, the Commission "decline[d] at this time to designate further network security services and other proposed services in order to ensure internal connections support is targeted efficiently at the equipment that is necessary for LANs/WLANs" to "help ensure available funds are targeted and therefore available to more applicants."[12] The Commission "le[ft] the record open," however, to evaluate changes as circumstances warrant.[13] The Commission affirmed this approach in 2019 when it last considered the issue.[14]

Schools' and libraries' response to COVID-19, however, has definitively changed the landscape such that a new approach is urgently needed for the duration of the pandemic response. As discussed above, schools' and libraries' need to deploy new technology quickly to

---

[12] *Modernizing the E-rate Program for Schools and Libraries,* Report and Order and Further Notice of Proposed Rulemaking, 29 FCC Rcd 8870, 8919 ¶ 121 (2014) ("*2014 E-rate Order*").

[13] *Id.*

[14] *Modernizing the E-rate Program for Schools and Libraries,* Report and Order, 34 FCC Rcd 11219, 11237 ¶ 46 (2019) ("*2019 E-rate Order*").

permit online learning and staff telework has made networks more vulnerable, and the incidence of cyberattacks against educational institutions has skyrocketed.[15]

Moreover, the Commission's rationale for declining to support network security – the desire to focus support on basic networking services to make more support available to more applicants – no longer applies. The Commission has made permanent the fixed Category 2 budgets for each school district and library system and has concluded that these budget rules have "enabled all applicants, regardless of their place on the E-rate discount matrix, to receive funding for broadband equipment and services inside their school and library buildings."[16] These budgets cap the amount that each school district or library system can request for Category 2 services, thereby eliminating the impact of adding an additional eligible service. Instead, they merely give schools and libraries greater flexibility to spend their budgeted amounts on much-needed security services if they choose to do so.[17]

Even though the current Category 2 budgets eliminate any concerns about a fiscal impact from the requested waiver, it is important to note that E-rate is operating well below budget. Total demand for all E-rate services for funding year 2020 was only $2.91 billion out of the overall program budget of $4.23 billion.[18] An additional $500 million in rollover funding also is available in the 2020 funding year.[19] There is thus a total of $1.82 billion in available unspent E-rate funding in the 2020 funding year.

---

[15] *See supra* Section I.

[16] *2019 E-rate Order,* 34 FCC Rcd at 11225 ¶ 16 (internal quotations omitted).

[17] *Id.* at 11223 ¶ 10 (noting findings of staff report that Category 2 budgets approach gives "applicants more flexibility to determine how best to upgrade their systems").

[18] *2020 E-rate Funding Public Notice,* 35 FCC Rcd at 6756.

[19] *Id.*

Indeed, the urgent need for support for network security solutions given the pandemic,

combined with the considerable amount of unspent funding available under the E-rate budget,

suggests that the Commission also should consider using its waiver authority to lift the per-

student budget caps by a reasonable amount, such as ten percent, to allow schools and libraries

the opportunity to seek additional funding for this important service in this extraordinary time.

Given the current Category 2 demand of only $1.17 billion for 2020,[20] a temporary boost in the

Category 2 budgets on the order of ten percent could not be expected to come close to exceeding

the E-rate budget.

IV.   USE OF WAIVER AUTHORITY TO MAKE E-RATE CATEGORY 2 SUPPORT AVAILABLE FOR NETWORK SECURITY IN THE 2020 AND 2021 FUNDING YEARS IS CONSISTENT WITH OTHER COVID-RELATED WAIVERS

Over the course of the last six months, the Commission has responded admirably to the

challenges presented by the novel coronavirus, utilizing its authority under section 1.3 to waive

or modify numerous rules, including E-rate rules, to facilitate the national response to the

pandemic.[21] In these orders, the Commission has recognized that "the mass disruptions to daily

life, including the closure of schools and libraries for an extended period of time, the transition to

remote learning and working for students, teachers, and staff, and the adverse impact to service

---

[20] *Id.*

[21] *See, e.g., Rural Health Care Universal Service Support Mechanism; Schools and Libraries Universal Service Support Mechanism,* Order, 35 FCC Rcd 2741 (WCB 2020) ("*Gift Rule Waiver Order*"); *Schools and Libraries Universal Service Support Mechanism,* Order, 35 FCC Rcd 2978 (WCB 2020) (*E-rate Deadline Waiver Order*); *Lifeline and Link Up Reform and Modernization*, Order, 35 FCC Rcd 2729 (WCB Mar. 17, 2020) ("*Lifeline Recertification and Reverification Waiver Order*"); *Lifeline and Link Up Reform and Modernization,* Order, 35 FCC Rcd 2950 (WCB 2020) ("*Lifeline Usage and De-Enrollment Waiver Order*"). *See also* FCC, "Coronavirus" (collecting actions), https://www.fcc.gov/coronavirus.

providers and manufacturers caused by COVID-19 present compelling and unique circumstances that merit a waiver of our rules."[22]

The waiver requested here would be consistent with these prior waivers. Here too, the need for the waiver stems directly from the impact of the transition to remote learning and telework due to the pandemic – in this case, the marked increase in cyberattacks exploiting systems that schools and libraries have deployed or expanded in response to learning and working remotely.[23] Here too, the Commission can modify its existing rules to provide needed flexibility to universal service support recipients to better address the challenges of this new environment. This is an important opportunity for the Commission to have a positive impact on the national response to COVID-19, and it should seize the chance to do so.

V. CONCLUSION

Schools and libraries are expending enormous effort to transition quickly and unexpectedly to distance learning and telework to prevent the spread of COVID-19. Criminals are exploiting their efforts with a surge in cyberattacks. The Commission can provide meaningful relief for this problem by using its authority under section 1.3 to allow Category 2 support to be used for network security software during the 2020 and 2021 funding years. Such relief would be consistent with the Commission's other pandemic-related waivers and should be granted without delay.

---

[22] *E-rate Deadline Waiver Order*, 35 FCC Rcd at 2975 ¶ 5.

[23] As noted above, this waiver does not seek support for any off-campus services or equipment. *See supra* note 4.

Respectfully submitted,

CISCO SYSTEMS, INC.

By: _____/s/_____

Jeffrey A. Campbell
Senior Vice President, Government Affairs
and Public Policy
Cisco Systems, Inc.
601 Pennsylvania Ave., NW
North Building, Ninth Floor
Washington, DC 20004
(202) 354-2920

August 20, 2020