



September 4, 2020

Marlene H. Dortch, Secretary
Federal Communications Commission
Office of the Secretary
445 12th Street, SW
Room TW-A325
Washington, DC 20554

Re: Comment in Support of Cisco Systems Inc.'s Petition for Waiver, WC Docket No. 13-184

The Cybersecurity Coalition (“Coalition”) submits this comment in support of Cisco Systems, Inc.’s (“Cisco’s”) petition for waiver to permit schools to use E-rate Category Two funding to cover the costs of network security software in the 2020 and 2021 funding years, which was submitted to the Federal Communications Commission (“FCC”) on August 20, 2020.¹ We believe this is an example of the approach the FCC should take. School districts should be provided the flexibility to select a variety of solutions, including end point, network, cloud, and device security solutions, as they tailor their cyber security protections to meet their unique risk profiles. The Coalition appreciates the opportunity to provide these comments and engage in this important discussion.

The Coalition is composed of leading companies with a specialty in cybersecurity products and services dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies.² We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management. We are supportive of efforts to identify and promote the adoption of cybersecurity best practices, information sharing, and voluntary standards throughout the global community.

The unprecedented shift to remote learning during the COVID-19 pandemic has left schools and libraries struggling to ensure user connectivity and the security of their newly expanded networks. Prior to the pandemic, Commissioner O’Reily recognized the vulnerability of school and library networks to cybersecurity attacks, explaining that “without proper diligence, these systems could be extremely vulnerable to mischief, causing extensive harm to users and others while wasting our investments in the process.”³ After the shift to remote

¹ See Petition for Waiver of Cisco Systems, Inc., WC Docket No. 13-184 (filed Aug. 20, 2020) (“Cisco Petition”).

² The views expressed in this comment reflect the consensus views of the Coalition and do not necessarily reflect the views of any individual Coalition member. For more information on the Coalition, see www.cybersecuritycoalition.org.

³ *Modernizing the E-rate Program for Schools and Libraries*, Report and Order, WC Docket 13-0184, FCC 19-117, at 44 (Dec. 3, 2019). Commissioner Rosenworcel also emphasized the need to “keep a close watch on emerging cyber vulnerabilities affecting schools and libraries.” *Id.* at 45.

learning, the cybersecurity threats to school networks, in particular, has increased.⁴ The Federal Bureau of Investigation (“FBI”) issued a security alert warning K-12 schools about an increase in ransomware attacks in June.⁵ Given the broad recognition that schools and library networks are uniquely vulnerable to cyberattacks and the increased demand for security services, the Coalition urges the Commission to provide access to reasonably priced security products through the E-rate program.

The Coalition believes that cyber security is essential to the safety and reliability of school and library networks. Currently, the only security option listed on the ESL is firewall services and components.⁶ Although firewalls are a good first step, alone, a firewall is not enough to protect against today’s cyber threats. While there is no one-size-fits all approach to security, a strong cyber security system must include a variety of security features beyond what is currently offered under the E-rate program. Given the range of available cyber security solutions, schools and libraries should have the flexibility to choose those security products that are most suitable to their needs, including such solutions as network, cloud, end point, and device security solutions. The Commission has recognized the importance of granting schools and libraries the flexibility to purchase other services that “meets their needs” and should apply that reasoning to security products as well.⁷

The Commission’s prior reasons for declining to include network security products on the ESL do not make sense in light of changing technology use during the pandemic. The Commission previously explained that it would not include network security products on the ESL because it wished to “ensure available funds are targeted and therefore available to more applicants.”⁸ However, any financial concerns related to the expansion of the ESL to cover network security services no longer makes sense. As Cisco noted in its petition for waiver, the fixed Category Two budgets for school districts and library systems eliminate “the impact of adding an additional eligible service” because entities must operate within a set budget range when choosing which service to purchase.⁹ This rationale should no longer serve as a barrier to offering schools and libraries the option to purchase security services, particularly in light of the increased security concerns during the pandemic.

⁴ See e.g., Jake Maher, *Coronavirus Compounds K-12 Security Problems: 5 Areas to Watch*, EDUCATION WEEK (Mar. 17, 2020) <https://www.edweek.org/ew/articles/2020/03/18/coronavirus-compounds-k-12-cybersecurity-problems-5-areas.html> (explaining how the move to remote learning increases the risk of cyberattacks); Micah Castelo, *Cybersecurity Attacks Increasingly Threaten Schools – Here’s What to Know*, EDTECH MAGAZINE (June 17, 2020) <https://edtechmagazine.com/k12/article/2020/06/cyberattacks-increasingly-threaten-schools-heres-what-know-perfcon> (explaining that cyberthreats at schools have increased because “cyber attackers view schools and districts as easy targets” due to the lack of security resources).

⁵ FBI, *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic*, (Mar. 30, 2020), <https://www.fbi.gov/contact-us/fieldoffices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroomhijacking-during-covid-19-pandemic>.

⁶ *Id.*

⁷ *Modernizing the E-rate Program for Schools and Libraries*, Report and Order and Further Notice of Proposed Rulemaking, WC Docket 13-184, FCC 14-99 at ¶¶ 42, 123 (July 23, 2014) (recognizing the importance of granting schools the flexibility to purchase the “bandwidth that meets their needs” and to have a choice “among managed Wi-Fi options”).

⁸ *Id.* at ¶ 121.

⁹ Cisco Petition at 5.

Finally, the Commission itself has granted several waivers, including one related to the E-rate program, in recognition of the unique strain that the COVID-19 pandemic has placed on the resources of schools, libraries, and other organizations.¹⁰ It would be consistent with these decisions for the Commission to grant Cisco's waiver request.

The Coalition thanks the Commission for its continued efforts to provide support for schools and libraries impacted by the COVID-19 pandemic and appreciates the opportunity to comment on this important issue.

Sincerely,

/s/ Ari Schwartz
Coordinator
Cybersecurity Coalition

¹⁰ For a full list of the Commission's coronavirus related actions, see FCC, *Coronavirus*, <https://www.fcc.gov/coronavirus>.