WILKINSON BARKER KNAUER LLP

1800 M STREET, NW
SUITE 800N
WASHINGTON, DC 20036
TEL 202.783.4141
FAX 202.783.5851
WWW.WBKLAW.COM
L. CHARLES KELLER
202.383.3414
CKELLER@WBKLAW.COM

November 6, 2019

VIA ECFS

Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Re: *Notice of Ex Parte Presentation*
E-rate Category 2 Budgets and Security (WC Docket No. 13-184)

Dear Ms. Dortch:

On November 4, 2019, Cisco Systems, Inc. ("Cisco") met in separate meetings with Nirali Patel of the Office of Chairman Ajit Pai; Joel Miller of the Office of Commissioner Michael O'Rielly; and Joseph Calascione of the Office of Commissioner Brendan Carr. The purpose of the meetings was to discuss issues related to E-rated Category Two support raised in the Commission's July 2019 Notice of Proposed Rulemaking.[1] Cisco was represented by Jeff Campbell, Vice President, Government Affairs and Technology Policy, and undersigned counsel. In addition, in the meetings with Ms. Patel and Mr. Miller, we were joined by Peter Kaplan, National K12 E-rate Channel Manager, Aruba, A Hewlett Packard Enterprise Company.

In the meetings, Cisco's presentation was consistent with Cisco's comments in response to the NPRM and followed the attached talking points, which were distributed to the meeting attendees. In the meetings with Ms. Patel and Mr. Miller, Mr. Kaplan also reiterated the importance of including advanced network security solutions in the eligible services list for 2020 and provided the attached Aruba handout to Ms. Patel and Mr. Miller.

This letter is filed consistent with the Commission's ex parte rules.

Sincerely,

/s/
L. Charles Keller
Counsel to Cisco Systems, Inc.

[1] *Modernizing the E-rate Program for Schools and Libraries*, Notice of Proposed Rulemaking, 34 FCC Rcd 5406 (2019) ("NPRM").

Attachments

cc: Nirali Patel, FCC (email)
Joel Miller, FCC (email)
Joseph Calascione, FCC (email)
Peter Kaplan, Aruba (email)

Cisco Systems, Inc.
E-rate Category 2 Support and Network Security
November 2019

- **The Commission should restore the five-year budgets for E-rate Category 2 services.**
  - Support in the record was effectively universal.
  - Fixed budget approach ensures equitable distribution of C2 support among schools, including rural schools.
  - Fixed budget approach controls spending.
- **The Commission should recognize that network security capabilities are a necessary and integral part of today's internal networks.**
  - The record is clear that cybersecurity is a major challenge for educational networks today.
    - The Attachment provides a sampling of the evidence in the record of cybersecurity incidents that have negatively affected schools and libraries in recent years, and shows that such incidents are increasing in frequency and severity.
  - Record support is unanimous for allowing E-rate C2 support to be used for network security capabilities.
  - The record also shows that network security functions are being integrated into internal network equipment or bundled into internal connections equipment.
    - As a result, in many instances, allowing C2 support to be used for security functionality will simply avoid the need for burdensome cost-allocation.
  - The Commission's public interest obligations under Section 254 include a responsibility to protect against cyber attacks.
    - In the draft USF Supply Chain Order and NPRM, the Commission will hold:
      - "In today's increasingly connected world, safeguarding the security and integrity of America's communications infrastructure has never been more important." (¶ 1)
      - "[T]he promotion of national security is consistent with the public interest, and USF funds should be used to deploy infrastructure and provide services that do not undermine our national security." (¶ 28) "Or, to put it another way, providing a secure service is part of providing a quality service." (¶ 29)
      - "The action we take today also implements section 105 of CALEA [requiring telecommunications carriers to prevent unlawful interceptions of communications]." (¶ 35)
      - "Ensuring the safety, reliability, and security of the nation's communications networks is vital not only to fulfilling the purpose of the Act but to furthering the public interest and the provision of quality services nationwide." (¶ 114)

- The Commission has the authority to provide USF support for network security functionality.
  - Section 254(h)(2) explicitly gives the Commission authority to "enhance…access to advanced telecommunications and information services" for E-rate recipients.
  - The Commission has used this authority over the years to support a range of information services through E-rate, including Internet access.
  - Since 1997, the Commission has held that it has particular authority to support networks and services in order to connect "classrooms" as required by Section 254(b)(6), and this was upheld by the 5th Circuit in *TOPUC*, 183 F.3d 393, 440-443 (5th Cir. 1999).
  - As noted above, network security functionality is now often integrated with internal connections equipment.
  - In light of all of this, the Commission has the authority to allow C2 E-rate support to be used for network security products to promote "access to advanced telecommunications and information services for all public and nonprofit elementary and secondary school *classrooms* … and libraries." 47 U.S.C. § 254(h)(2).
- Supporting network security functionality through E-rate C2 support will have no impact on the size of the fund.
  - The per-applicant five-year budgets impose a strict limit on spending.
  - The overall E-rate fund is capped (and has had carryover funds in recent years).

Attachment

The K-12 Cybersecurity Resource Center, Cyber Incident Map, https://k12cybersecure.com/map/.

Public Service Announcement, Fed. Bureau of Investigation, Education Techologies: Data Collection and Unsecured Systems Could Pose Risks to Students (Sept. 13, 2018), https://www.ic3.gov/media/2018/180913.aspx.

Doug Olenick, Cyberattack Forces Houston County Schools to Postpone Opening Day, SC Media, July 31, 2019, https://www.scmagazine.com/home/security-news/malware/cyberattack-forces-houston-county-schools-to-postpone-opening-day/ (reporting that the Houston County (Ala.) School District was forced to delay the start of school by 11 days).

FUSD Schools Closed Thursday Due to Cybersecurity Intrusion, Ariz. Daily Sun, Sept. 4, 2019, https://azdailysun.com/news/local/fusd-schools-closed-thursday-due-to-cybersecurity-intrusion/article_eee18f30-03b4-5114-84ee-24f986e03215.html (reporting that schools in Flagstaff, Arizona were closed due to cyberattack).

Bob Keeler, Souderton Area School District Hit by Cyber Attack, Souderton Indep., Sept. 4, 2019, http://www.montgomerynews.com/soudertonindependent/news/souderton-area-school-district-hit-by-cyber-attack/article_c191fcce-cf1c-11e9-bbe5-2730cc5d33c3.html (reporting that internet and network services, including school-issued devices, in Pennsylvania school district were unavailable due to cyberattack).

Tiina Rodrigue, ALERT! – CyberAdvisory – New Type of Cyber Extortion/Threat, U.S. Dept. of Educ., Fed. Student Aid (Oct. 16, 2017), https://ifap.ed.gov/eannouncements/101617ALERTCyberAdvisoryNewTypeCyberExtortionThreat.html.

Initial Comments of the New Mexico Public School Facilities Authority at 12-14, WC Docket No. 13-184 (filed Aug. 16, 2019) (explaining that cyberattacks compromise personally identifiable information, waste money, and stymie productivity).

Comments of the Nebraska Department of Education at 6-9, WC Docket No. 13-184 (filed Aug. 29, 2019) ("Nebraska schools have had several instances of ransomware and malware that have stopped teaching and learning from happening, costing districts extreme amounts of time and money to rectify.").

Reply Comments by the Iowa Department of Education at 4, WC Docket No. 13-184 (filed Sept. 3, 2019).

Reply Comments of the Ohio Information Technology Centers at 8-10, WC Docket No. 13-184 (filed Sept. 3, 2019).

Comments of the State of South Carolina on the Proposed Rulemaking for the Category 2 Program at 3, WC Docket No. 13-184 (filed Aug. 16, 2019).

Comments of the Kentucky Department of Education at 3, WC Docket No. 13-184 (filed Aug. 16, 2019).

Reply Comments of the Florida State E-rate Coordinator Team in Response to FCC Public Notice DA 19-58 at 13-14, WC Docket No. 13-184 (filed Aug. 22, 2019).

Reply Comments of the Illinois Department of Innovation and Technology at 5, WC Docket No. 13-184 (filed Sept. 3, 2019) (explaining that network security services enhance network performance and improve repair times).

Reply Comments of the American Library Association at 3-4, WC Docket No. 13-184 (filed Sept. 3, 2019) ("[I]t is time to urgently address this serious issue.").

Initial Comments of the State E-rate Coordinators' Alliance in Response to DA 19-738 at 6-7, WC Docket No. 13-184 (filed Sept. 3. 2019).

Reply Comments of the State Educational Technology Directors Association Regarding E-rate Category Two at 4, WC Docket No. 13-184 (filed Sept. 3, 2019).

Reply Comments of CoSN, AASA and ASBO Regarding E-rate Category Two at 2-5, WC Docket No. 13-184 (filed Sept. 3, 2019).

Comments of EducationSuperHighway at 6-7, WC Docket No. 13-184 (filed Aug. 16, 2019); Joint Initial Comments to Notice of Proposed Rulemaking (FCC 19-58) Submitted by State E-rate Coordinators' Alliance and Schools, Health & Libraries Broadband Coalition at 26, WC Docket No. 13-184 (filed Aug. 16, 2019).

HPE ARUBA

Adding Advanced Network Security to the 2020 Eligible Services List

- There is 100% consensus amongst the education community and industry that it is critical that advanced network security be added to the FY 2020 Eligible Services List

- State E-rate Coordinators Alliance (SECA)
    - Part of network monitoring also should include allowance for network security features and services to protect networks against intrusion and interference. Networks security and intrusion detection services are often bundled together with firewalls, but currently, these features of firewall appliances are not eligible and must be deducted from firewall appliances. Considering how frequently cyber-attacks occur, it is essential that networks be protected against such malicious attacks. Schools and libraries have been forced to equip themselves with such protection measures, but they must separately bear the burden of these network security costs, because they are ineligible for E-rate funding. This restriction leads to more complex application preparation and processing in order to perform cost allocations to quantify associated costs and remove them from funding requests and for the costs to be borne fully from local budget resources.

- American Library Association
    - Our position is that there are sufficient funds in the program and it is time to urgently address this serious issue

- Funds For Learning
    - C2 Eligible Services Should be Expanded. The Commission also asks whether there are any additional services that should be made eligible for C2 funding. Yes, there are. In terms of achieving all the E-rate program's goals and objectives, it makes perfectly good sense to give applicants the flexibility to spend their C2 budgets on whatever network infrastructure they believe is most important for them to spend it on, *including* I.T. security and network monitoring. We cannot think of any good reason why the Commission would not want to do this. That only 33% of schools and 6% of libraries maxed out their budgets in the past five years proves that applicants can be trusted to purchase only those goods and services which they need and can afford.

- EducationSuperhighway
    - Our initial comments provided detailed information on specific network security features, devices and services that should be made eligible for E-rate support.5

Twenty-one other commenters advocated for adding network security products to the Eligible Services List. As cyberattacks continue to threaten school districts nationwide, network security features, "such as caching, advanced firewall features, anti-intrusion, and DDOS prevention and mitigation are critical to the efficient operation of any network

- Nebraska Department of Education
    - Adopt Advanced Firewall Services as an eligible service as well as other Cybersecurity measures.

- Iowa Department of Education

    - As cited by EducationSuperHighway, - *Network security is an ever more critical component of educational technology infrastructure; schools who lack robust, modern network defense systems and filtering endanger the safety and security of their students, staff, and data.* ESH (page 6); The Department supports the recommendations by ESH on page 7 of their initial comments to add the following items to the C2 Eligible Services List:
        - All components of C2 firewalls
        - Content filtering
        - Deep packet inspection (DPI) capabilities, including Intrusion Detection System (IDS) and/or Intrusion Prevention System (IPS)
        - Network Management Systems (NMS)

- Ohio Information Technology Centers
    - Supports CoSN comments to include advanced network security solutions.

- Wisconsin Department of Public Instruction
    - We also call attention to the joint comments filed by the State E-rate Coordinators' Alliance (SECA) and the Schools, Health & Libraries Broadband Coalition (SHLB).7 Their comments provide the legal rationale on why filtering should be eligible. In addition to making filtering E-rate eligible we agree with a number of commenters who said it is equally necessary to make a wide array of security tools Category 2 eligible.

- Illinois Department of Innovation & Technology
    - Similarly, the Commission should take the opportunity in this proceeding finally to address one of the most needed changes in the E-rate eligibility rules, namely that of information technology security hardware and software and network monitoring.

- Council of Chief State School Officers

- Currently, the only security measure eligible for E-rate support is basic firewall service. In addition to this service, we recommend allowing Category 2 funds to be used to protect broadband networks from increasingly prevalent cyberattacks, including but not limited to the costs for equipment or services which provide advanced firewall, intrusion detection, and DDoS attack mitigation. We believe these basic supports and services are necessary to the effective operation of a broadband network.

- FL Department of Education
  - Our respondents made it abundantly clear that the eligibility of security systems is one of their primary concerns.

- State of SC
  - The Commission must consider the Wi-Fi networks funded through the E-Rate program as an investment in America's students. As such, the Commission must realize that in order to protect the investment it has made, the Commission should include products and services on the eligible services list such as advanced threat protection and network security. Today, the Commission requires that applicants who choose products, such as firewalls with advanced threat protection, to cost allocate a portion of the cost attributable to advanced threat protection. Removing this cost allocation requirement will result in more secure and resilient Wi-Fi networks and simplify the Category 2 Program.

- New Mexico Public School Facilities Authority
  - This definition is very broad and PSFA believes cyber-security, network management, and content filtering are required to enhance information services to school classrooms. If a district cannot manage, filter, or secure its network it cannot deliver information services to the classroom. Prior to the E-Rate Modernization Order, the program was oversubscribed almost every year, so allowing these services to be eligible was not economically reasonable. With the implementation of Category 2 budgets, making these services eligible would be economically feasible.

Industry Supports Expanding ESL to Include Advanced Network Security Products

- HPE Aruba
- Cisco Systems
- Fortinet