HWG | HARRIS, WILTSHIRE & GRANNIS LLP

September 6, 2019

Ex Parte

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: *Modernizing the E-rate Program for Schools and Libraries (WC Docket No. 13-184)*

Dear Ms. Dortch:

On September 4, 2019, representatives of Aruba, a Hewlett Packard Enterprise ("HPE") company, met with Commission officials to discuss making advanced network security eligible for E-rate support. In the first meeting, Dan Rivera of Aruba, Bret Wincup of HPE, Peter Kaplan for Aruba, and the undersigned met with Kris Monteith, D'wana Terry, Ryan Palmer, Kate Dumouchel, Gabriela Gross, Bryan Boyle, Gavin Logan, Joe Schlingbaum, and by telephone with Stephanie Minnock, all of the Wireline Competition Bureau. Later the same day, Dan Rivera, Peter Kaplan, Ansley Erdel of The Alpine Group, and the undersigned met with Nirali Patel, Wireline Advisor to Chairman Pai.

We described the cybersecurity crisis schools currently face. In recent years, schools have suffered nearly 600 reported cyberattacks taking the form of ransomware, distributed denial of service attacks, phishing attacks, and theft or disclosure of students' personal information.[1] Schools are particularly attractive targets for bad actors because they store valuable information about their students in their IT systems, and those systems are often not well secured. Schools typically have, for example, medical information about students as well as health insurance credentials, one of the most valuable types of data targeted by bad actors.[2] Just recently, several school systems have had to

---

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

2 Kate O'Flaherty, *Why Cyber-Criminals Are Attacking Healthcare – And How to Stop Them*, FORBES, Oct. 5, 2018, https://www.forbes.com/sites/kateoflahertyuk/2018/10/05/why-cyber-criminals-are-attacking-healthcare-and-how-to-stop-them/#54578f77f69e.

delay or interrupt the start of the school year due to a cyberattack.[3] The FBI and the Department of Education have warned of the increase in cybercrime against schools.[4]

The urgent need for the E-rate program to include advanced network security for schools and libraries is reflected in the record, without opposition. Authorities from states across the country have explained that they need access to network security to protect sensitive student information,[5] reduce network downtime,[6] and prevent the loss of data and functionality that results even after a

---

[3] *See, e.g.*, 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); *see also* 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).

[4] 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; 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.

[5] *See, e.g.*, 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); 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).

[6] *See, e.g.*, 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."); 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).

cyberattack has been resolved.[7] In addition to the individual comments submitted by public education authorities from Florida, Illinois, Iowa, Kentucky, Nebraska, New Mexico, Oregon, South Carolina, and Wisconsin, national organizations representing leaders in education and library services support eligibility for network security. The Council of Chief State School Officers, representing the heads of education agencies of all fifty states in addition to other non-state U.S. jurisdictions, explained that network security services are essential "to maintain online access that is safe, secure, and resilient."[8] Service providers and others likewise urge the Commission to make advanced network security an eligible service.[9] Support is overwhelming and unanimous.

Aruba urges the Commission and Bureau to act quickly. If modern network security remains ineligible for E-rate support until Funding Year 2021, schools and libraries will lack E-rate funding to help prevent cyberattacks for two to three more years. Aruba encourages the Commission and Bureau to update the Funding Year 2020 Eligible Services List ("ESL") to include modern network security.[10]

---

[7] *See, e.g.*, 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); Category 2 Reply Comments of the Wisconsin Department of Public Instruction at 2, WC Docket No. 13-184 (filed Sept. 3, 2019) (citing Comments of Cisco Systems, Inc. at 7, WC No. 13-184 (filed Aug. 16, 2019)); Reply Comments of Oregon Department of Education at 3-4, WC Docket No. 13-184 (filed Aug. 30, 2019).

[8] Reply Comments of the Council of Chief State School Officers at 1, WC Docket No. 13-184 (filed Sept. 3, 2019); *see also* 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).

[9] *See, e.g.*, Comments of Cisco Systems, Inc. at 7; Reply Comments of Fortinet at 2, WC Docket No. 13-184 (filed Sept. 3, 2019); Reply Comments of Education Networks of America, Inc. at 3-4, WC Docket No. 13-184 (filed Sept. 3, 2019); Reply Comments of Kellogg & Sovereign Consulting, LLC at 5-6, WC Docket No. 13-184 (filed Sept. 3, 2019); Comments of Funds For Learning, LLC on Making the Category Two Budget Approach Permanent and Other Modifications to the Category Two Budget Approach at 12-13, WC Docket No. 13-184 (filed Aug. 16, 2019).

[10] Ideally the Commission or Bureau would release the ESL at least 60 days before the opening of the Funding Year 2020 application window as required by 47 C.F.R. § 54.502(d). For good cause, the Commission has previously waived the requirement that the ESL be released 60 days

Please be in touch if you have any questions.

Sincerely,

Julie A. Veach
Counsel to Aruba, a Hewlett Packard Enterprise Company

Attachment

cc: Nirali Patel
Kris Monteith
D'wana Terry
Ryan Palmer
Kate Dumouchel
Gabriela Gross
Bryan Boyle
Gavin Logan
Stephanie Minnock
Joe Schlingbaum

---

before the opening of the application filing window. For example, in 2009, the Commission included the ESL within a Report and Order making additional services eligible for E-rate funding. Due to the timing of the Report and Order, on its own motion the Commission waived the rule requiring the ESL to be released 60 days before the application filing window. *Schools and Libraries Universal Service Support Mechanism*, Report and Order and Further Notice of Proposed Rulemaking, 25 FCC Rcd. 6562, 6566 ¶ 10, 6583 ¶ 45 & n.161 (2009) (waiving the 60-day rule and citing three prior instances of waiving the rule).

The Commission should update network security options in the E-rate program

September 4, 2019

The Problem:

Schools and libraries are increasingly subject to cyberattacks—distributed denial of service attacks, ransomware attacks, phishing attacks, and data theft or unauthorized disclosure.

- There are nearly 600 reported cyber incidents involving schools since January 2016.[1]
- Last year, the FBI released an alert regarding exploitation of schools' IT systems to obtain student information, including biometric data and medical information.[2]
- The Department of Education has warned against attackers who demand money by threatening to release sensitive student data.[3]
- In July 2019, Louisiana declared a state emergency after attacks on several school systems in the state.[4]

The Record:

- There is widespread support, no opposition, and a demonstrated need:
  - Education authorities in Florida, Kentucky, Nebraska, New Mexico, Oregon, and South Carolina support updated network security, as well as the Council of Chief State School Officers, the State Educational Technology Directors Association, SECA, SHLB, Funds for Learning, EducationSuperHighway and others.
  - The annual Funds for Learning survey of E-rate applicants found that 96% want network security and management funded in Category 2.[5]
- No additional funds are needed, and network security may lead to E-rate savings:
  - Network security will ensure that only authorized users and devices can use the school's or library's E-rate-supported broadband network, limiting the burden on the network and allowing the beneficiary to purchase less capacity.

The Solution:

Starting with Funding Year 2020, include advanced network security—not just firewalls—as a Category 2 service.

- Add advanced network security to the FY2020 Eligible Services List.
- Act quickly to ensure that schools and libraries do not have to wait until 2021-2022 to secure their networks.

---

[1] The K-12 Cybersecurity Resource Center, Cyber Incident Map, https://k12cybersecure.com/map/.
[2] Federal Bureau of Investigation, Public Service Announcement, https://www.ic3.gov/media/2018/180913.aspx.
[3] U.S. Department of Education, Federal Student Aid, https://ifap.ed.gov/eannouncements/101617ALERTCyberAdvisoryNewTypeCyberExtortionThreat.html.
[4] https://www.govtech.com/security/Louisiana-Declares-State-Emergency-After-Malware-Attack-on-Multiple-School-Systems.html.
[5] *See* Letter from John D. Harrington, CEO, Funds for Learning, LLC, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 13-184 & CC Docket No. 02-6.