**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]](#footnote-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]](#footnote-2)
* The Department of Education has warned against attackers who demand money by threatening to release sensitive student data.[[3]](#footnote-3)
* In July 2019, Louisiana declared a state emergency after attacks on several school systems in the state.[[4]](#footnote-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]](#footnote-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/. [↑](#footnote-ref-1)
2. Federal Bureau of Investigation, Public Service Announcement, <https://www.ic3.gov/media/2018/180913.aspx>. [↑](#footnote-ref-2)
3. U.S. Department of Education, Federal Student Aid, <https://ifap.ed.gov/eannouncements/101617ALERTCyberAdvisoryNewTypeCyberExtortionThreat.html>. [↑](#footnote-ref-3)
4. <https://www.govtech.com/security/Louisiana-Declares-State-Emergency-After-Malware-Attack-on-Multiple-School-Systems.html>. [↑](#footnote-ref-4)
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. [↑](#footnote-ref-5)