

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

|   |   |                      |
|---|---|----------------------|
| In the Matter of  | ) |                      |
|   | ) |                      |
| Modernizing the E-Rate Program for Schools<br>and Libraries   | ) | WC Docket No. 13-184 |
|   | ) |                      |
| Wireline Competition Bureau Seeks Comment<br>On Proposed Eligible Services List for<br>The E-Rate Program | ) |                      |
|   | ) |                      |

**REPLY COMMENTS OF COX COMMUNICATIONS, INC.**

Cox Communications, Inc., (“Cox”) hereby submits these reply comments in response to the Wireline Competition Bureau’s (“Bureau”) public notice regarding the proposed Eligible Services List (“ESL”) for funding year 2021.<sup>1</sup> Cox agrees with commenters who argue advanced network security services should be eligible for E-rate support.<sup>2</sup> As Cox has previously stated, since the Commission declined to include E-Rate support for “further network security services,”<sup>3</sup> schools across the country have seen marked increases in ransomware and Distributed Denial of Service (“DDoS”) attacks, which warrant the Commission taking a fresh look at including these needed services. Last year, Commissioners O’Rielly and Rosenworcel indicated a willingness to revisit the eligibility of advanced network security services,<sup>4</sup> and given the increased importance

---

<sup>1</sup> Wireline Competition Bureau Seeks Comment on Proposed Eligible Services List for the E-Rate Program, DA 20-767 (WCB. rel. July 21, 2020).

<sup>2</sup> See Funds for Learning Comments at 2-7; State E-Rate Coordinators Alliance at 10-11; and Cisco Systems, Inc. Petition for Waiver in WC Docket No. 13-184.

<sup>3</sup> See *Modernizing the E-Rate Program for Schools and Libraries*, Report and Order and Further Notice of Proposed Rulemaking, 29 FCC Rcd 8870, 8918, para 121 & n. 275 (“*Modernization Order*”) (declining to designate services suggested by commenters, including intrusion protection and detection, malware protection, application control, content filters, DDoS mitigation, and cybersecurity services, as eligible in three sentences).

<sup>4</sup> In separate statements, Commissioner O’Rielly stated: I am open to discussing the possibility of including such services [network security features and services] in the future; while Commissioner Rosenworcel stated: As these problems grow more common, it is appropriate to consider what practices can help prevent school and library networks avoid the inconvenience and harm that follows in the wake of these attacks. So I am pleased that my colleagues agree that the agency should be open to learning more about these challenges. I hope this will help inform policies that across the board will ensure that school and library networks remain strong and secure in the future. *Modernizing the E-Rate Program for Schools and Libraries*, WC Docket 13-184, Report and Order, 34 FCC Rcd 11219 (2019).

of distance learning services during the Covid-19 pandemic, the Bureau or Commission should take action now to ensure schools' vital Internet services are protected.

Schools are increasingly becoming the targets of DDoS,<sup>5</sup> ransomware,<sup>6</sup> and other network cyberattacks. Cox is aware of at least two school systems in Arizona who were subject to DDoS attacks in 2017 and six others in Arizona, Florida, Nevada, Oklahoma, and Virginia in 2020. At least two school systems in Rhode Island were infected with malware in 2019. On July 24, 2019, the Governor of Louisiana issued an emergency declaration after school systems in Monroe, Morehouse Parish, and Sabine Parish were impacted by ransomware attacks.<sup>7</sup> On March 30, 2020, the Federal Bureau of Investigation (FBI) warned schools of online video classroom hijacking, after two schools in Massachusetts reported zoom conferences being infiltrated or hijacked by unidentified individuals.<sup>8</sup> On June 23, 2020, the FBI issued a Private Industry Notification or security alert warning K-12 schools and others about ransomware attacks on U.S. and foreign government organizations, education entities, private companies, and health agencies by unidentified cyber actors.<sup>9</sup>

Because DDoS and ransomware attacks can render Internet service effectively unusable, support for DDoS and ransomware prevention and restoration services and equipment is necessary to protect the E-Rate funds invested in Internet access, internal connections, and the integrity of educational networks. This is particularly important while many school systems are operating virtually in whole or in part in response to the Covid 19 pandemic. If school systems' access to

---

<sup>5</sup> A DDoS attack is an attempt from an outside individual or group to overload network systems, equipment and memory resources. DDoS attacks are unique from other types of malware or viruses, because they do not simply slow down Internet service; they can cripple systems and effectively result in a temporary loss of Internet service. In addition, certain types of reflective DDoS attacks, attacks which may involve sending forged requests to a large number of computers that will reply to the requests and send those replies to the targeted victim, can saturate Internet broadband circuits, leaving local firewall appliances helpless to restrict unwanted traffic.

<sup>6</sup> Ransomware is a type of malware that locks a target's files, data, or the PC itself and extorts money in order to provide access.

<sup>7</sup> See <https://cyware.com/news/louisiana-governor-declares-emergency-after-ransomware-attack-hits-three-schools-50569756?ref=readmore>. In January 2020, the St Landry Parish school system went offline after staff discovered a ransomware attack. <https://www.klfy.com/local/cyber-attack-on-st-landry-parish-school-system-under-investigation/>.

<sup>8</sup> See <https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic>.

<sup>9</sup> See <https://securityaffairs.co/wordpress/106671/cyber-crime/fbi-warns-netwalker-ransomware-attacks.html>; <https://www.zdnet.com/article/fbi-warns-k12-schools-of-ransomware-attacks-via-rdp/>.

their distance learning platforms is compromised, students lose actual instructional classroom time, not just their ability to utilize supplemental educational materials.<sup>10</sup>

Unfortunately, the need for advanced network security solutions comes at a time of increased financial pressures for school systems. Several of Cox's customers who have purchased DDoS mitigation services have only been able to afford coverage for a portion of their traffic, so they are unable to operate at full capacity. In addition, at a Cox roundtable held in June 2020, school systems stated that attempted network breaches are an everyday occurrence, citing ransomware, spyware, and malware as the usual suspects. When asked what they would most want on the E-rate Category Two list, the school systems resoundingly pointed to cybersecurity solutions and, more specifically, comprehensive security audits/vulnerability assessments, layered perimeter security, intrusion detection systems (IDS), 24/7 security operation center (SOC), DDoS mitigation, and multi-factor authentication (MFA). However, the school systems also noted the extreme pressures on finite IT budgets, and the need for IT departments to determine how much security risks they can accept. This is a difficult and untenable position that could be made sufficiently more tolerable with a decision to provide E-Rate funding for advanced network security solutions.

Based on the reasons outlined herein, Cox respectfully requests that the Bureau include advanced network security solutions on the ESL to prevent and mitigate ransomware and DDoS attacks for funding year 2021. Alternatively, the Commission should open a rulemaking proceeding to consider making advanced network security solutions eligible for E-Rate support.

Respectfully submitted.

By: \_\_\_\_\_ /s/

Joiava Philpott  
Vice President, Regulatory Affairs  
Cox Communications, Inc.  
6205 Peachtree Dunwoody Road  
Atlanta, GA 30328

September 4, 2020

---

<sup>10</sup> See <https://www.nbcnews.com/news/us-news/miami-dade-public-schools-remote-learning-platform-endures-days-cyberattacks-n1239129>.