February 16, 2021

Marlene H. Dortch, Secretary

Federal Communications Commission

Office of the Secretary

445 12th Street, SW

Room TW-A325

Washington, DC 20554

Re: Comment on Using E-Rate Funds to Support Remote Learning

The Cybersecurity Coalition ("Coalition") submits this comment in response to the FCC's Public Notice entitled, *FCC Seeks Comment on Using E-Rate Funding to Support Remote Learning*. The Coalition endorses expanding E-Rate reimbursement to support remote learning, however, it is imperative to emphasize that doing so will create new significant cybersecurity risks which will need to be offset through additional cybersecurity support. The Coalition urges the FCC to use the opportunity of expanding E-Rate funding to support remote learning to also open E-Rate reimbursement to more cybersecurity expenses.

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. 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.

Remote learning capabilities have become a lifeline for millions of Americans during the ongoing COVID-19 pandemic. The urgency to support remote learning with additional resources as a response to the pandemic is further justified with the expectation that its uses will extend well beyond the end of the current public health crisis. However, the efficacy of remote learning is ultimately dependent on our educational institutions' ability to remain secure from cyber threats.

Forging ahead with expanded remote learning without addressing how doing so will create new cyber risks and enlarge existing ones would be imprudent. Both the new and enlarged cyber risks not only threaten the reliability of remote learning capabilities, but they also have the potential to cause

significant damage to the entirety of an educational institution's network. Regardless of the size of a cyberattack, recovery often comes at great cost. IBM has reported that schools have already paid out millions in ransoms, while the cost to student learning is incalculable.[1]

The concern that educational institutions are inadequately prepared to secure themselves after remote learning expansion is based on overwhelming evidence. In 2019, it was estimated that over 1,000 educational institutions were hit by ransomware, and IBM reported 1,600 schools were targeted in 2020.[2, 3] Targeting of schools became so widespread that the FBI and CISA felt obligated to issue a joint cybersecurity advisory that warned of threats to K-12 educational institutions.[4] Those two agencies reported that between August and September of last year, 57% of all reported ransomware attacks targeted schools.[5]

Attacks against public schools during this time period include:

- Virginia's Fairfax County Public Schools: Fairfax County Public Schools, the tenth largest school district in the United States, were the victim of a Maze ransomware attack which ultimately led to leaked student and faculty data.[6]
- Mississippi's Yazoo County School District: The district was hit by a ransomware attack forcing it to pull its IT systems offline and pay a reported $300,000 in recovery costs.[7]
- California's Selma Unified School District: Victimized by a ransomware attack, the district's network was taken down and virtual classes were cancelled.[8]
- North Carolina's Burke County Schools: A ransomware incident delayed remote learning for two weeks.[9]

However, the sheer number of ransomware attacks doesn't fully explain why so many schools became victims. Even though many school districts operate the number of computers and other electronic devices that would put them on par with many medium sized businesses, they typically don't have the funding to support IT and security to the same extent. This is reflected in a Morning Consult poll from October which found "60 percent of educators and administrators weren't sure or hadn't received any

---

[1] *FBI urges new approach to cyber protection of U.S. schools*. Gopal Ratnam, CQ, 2/4/2021: https://plus.cq.com/doc/news-6113432?4&srcpage=home&srcsec=ina

[2] *Ransomware 'Crisis' in US Schools: More Than 1,000 Hit So Far in 2019*. Kelly Jackson Higgins, DARKReading, 12/16/2019: https://www.darkreading.com/threat-intelligence/ransomware-crisis-in-us-schools-more-than-1000-hit-so-far-in-2019/d/d-id/1336634

[3] *FBI urges new approach to cyber protection of U.S. schools*. Gopal Ratnam, CQ, 2/4/2021: https://plus.cq.com/doc/news-6113432?4&srcpage=home&srcsec=ina

[4] *Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data*. CISA, 12/10/2020: https://uscert.cisa.gov/sites/default/files/publications/AA20345A_Joint_Cybersecurity_Advisory_Distance_Learning_S508C.pdf

[5] *FBI urges new approach to cyber protection of U.S. schools*. Gopal Ratnam, CQ, 2/4/2021: https://plus.cq.com/doc/news-6113432?4&srcpage=home&srcsec=ina

[6] *Fairfax County Public Schools hit by Maze ransomware*. Security Magazine, 9/15/2020: https://www.securitymagazine.com/articles/93354-fairfax-county-public-schools-hit-by-maze-ransomware

[7] *Cyber-Attack on Mississippi Schools Costs $300,000*. Sarah Coble, 10/19/2020: https://www.infosecurity-magazine.com/news/cyberattack-on-mississippi-schools/

[8] *Classes in Selma canceled Friday after* district *computer systems hit by ransomware*. Gilbert Magallon, 8/29/2020: https://abc30.com/selma-hack-classes-canceled-ransomware-school-district/6394182/

[9] *North Carolina School District Targeted by Ransomware*. Becky Johnson, 8/26/2020: https://www.govtech.com/security/North-Carolina-School-District-Targeted-by-Ransomware.html

new cybersecurity training in light of increased remote learning," and that more than half had not received basic cybersecurity training at all.

With all of this in mind, the cyber threat to the education sector and to remote learning is clear. The inability of educational institutions to adequately secure themselves will be further exacerbated if they attempt to expand remote learning capabilities without also allocating additional resources to improving security.

This issue has been considered by the FCC before. In 2019, Former FCC Commissioner Michael O'Rielly noted his openness to including network security features and products within the Eligible Services List as a means to shore up vulnerable school and library networks. He recognized 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."[10] Since making that statement, the "mischief" he referred to has become an increasing reality that will grow as remote learning expands.

No singular act will solve this issue overnight, but the FCC is positioned to drastically mitigate the cyber threats we have outlined while improving the security and resiliency of our educational institutions. The Coalition urges you to open E-Rate reimbursement to more cybersecurity expenses. The Inclusion of network security features and products within the Eligible Services List would allow educational institutions the flexibility to invest in a broad range of modern security solutions, including end point, network, cloud, and device security solutions, tailored to meet the specific threats each educational institution faces.

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

Sincerely,

/s/

Ari Schwartz

Coordinator

Cybersecurity Coalition

[10] 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.