Before the

FEDERAL COMMUNICATIONS COMMISSION

Washington, DC 20554

In the Matter of

THE EMERGENCY CONNECTIVITY FUND FOR EDUCATIONAL CONNECTIONS AND DEVICES TO ADDRESS THE HOMEWORK GAP DURING THE PANDEMIC

WC Docket No. 21-93

COMMENTS REGARDING THE ELIGIBILITY OF EQUIPMENT AND SERVICES NECESSARY TO SUPPORT AND FACILITATE THE CONNECTIVITY REQUIRED TO MEET REMOTE LEARNING NEEDS

ADT CYBERSECURITY
Michael Hiatt, Director

ADT Cybersecurity, headquartered in Greensboro, North Carolina as a division of ADT, LLC, (Boca Raton Florida) manages firewalls for over 6,000 locations, including K-12. We offer comments in response to the FCC's communication DA 21-317, released March 16, 2021.

SUMMARY:

ADT Cybersecurity agrees with previous petitioners and commenters that have recommended updating the Eligible Service List to define a wider range of Firewall and Related Services as "Basic," and adopt a new broadband definition that intrinsically includes the basic tenets of network security "best practices" that are relevant to off-campus distance learning as put forward by NIST and promulgated through other governmental agencies on the national and state level..

We recommend that, monitoring services, such as represented by the term "SIEM" or Security Information and Event Management be included in the Eligible Services List as fully or partially eligible as an adjunct service under Managed Internal Broadband Connections.

We believe the time to augment the Eligible Services list with services and related equipment is now, in time for the rollout of Emergency Connectivity Fund, and well in advance of the upcoming E-rate FY 2022.

Redefining "Support"

Considering the expanding threat landscape, which according to the GAO in their December 2020 report is targeting k-12 environments to a great extent than ever[1], we urge the Commission to consider redefining the forementioned "support" to focus on the goal of "continuous service" as conceived by the Consortium For School Networking[2]. This approach would include a special focus on the products and services currently ineligible that would address specific vulnerabilities introduced by distance learning whose successful exploitation would result in significant downtime and disruption in the learning process.[3]

We maintain that ensuring that critical infrastructure is secure and resilient is as important a goal as facilitating the acquisition of the infrastructure itself. Without sustainability in the face of service outages and external attacks, the value of that infrastructure is substantially negated.

---

[1] *Data Security: Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm* https://www.gao.gov/products/gao-20-644 https://www.securitymagazine.com/articles/94140-cyber-actors-target-k-12-distance-learning-education-to-cause-disruptions-and-steal-data

[2] *Smart Education Networks by Design*: https://cosn.org/network-design-considerations

[3] https://www.absolute.com/media/5737/abt-2021-distance-learning-impact-education.pdf - https://managedmethods.com/blog/k12-remote-learning-cybersecurity/

These include:

- Multiple paths to the Internet. E-rate eligible entities should be afforded a discount on a redundant internet connection as an emergency back-up to their primary network connection. With an increasing reliance on cloud-based programs and data, extended downtimes have the effect of suspending the learning process, interrupting testing schedules, and disabling critical software programs not only for instruction, but also for school operations, including attendance, grades, performance, access and visitor management, and premise security.

- Reducing or eliminating single points of failure. Firewall high availability should be included as eligible equipment, as well as the ancillary licensing for seamless roll-over should the primary unit suffer failure.

- Endpoint Detection and Response. The roll-out of 1:1 devices for student use in distance learning creates multiple order of magnitude increases in the attack surface. Eligibility for endpoint detection combined with a "rollback" or restoration feature in the case of infection preserves the investment in the device and forestalls replacement.

Additional recommendations to consider:

- Extend eligibility to individual VPN licenses tied to the firewall to secure remote connections, as well as "VPN concentrator" equipment or cloud-based services that provide a similar function.

- Make firewall software features that enable cloud-sandboxing eligible. Currently, certain advanced features contained with firewall software bundles are cost-allocated out of the discount request. These features can have a substantial positive effect in maintaining continuous operations by blocking Zero-day threats in hybrid-cloud environments.[4]

- 24/7/ Network monitoring - Allow SIEM (Security Information and Event Management) services to be an eligible part of network management under MIBS if bundled with new or ongoing management of eligible equipment. School and library IT personnel are challenged as never before with the many complexities of procuring, installing and maintaining the digital classroom, even before the new challenges brought on by the pandemic. The introduction of SIEM-type services into MIBS allows technologies incorporating AI and Machine Learning to identify and eliminate known and unknown threats within the network. Third parties contracting through MIBS can mitigate these threats before they have the opportunity to disrupt network operations

[4] *Recent testimony before congress on Solarwinds Attacks*: https://techcrunch.com/2021/03/22/the-frankencloud-model-is-our-biggest-security-risk/amp/