Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Modernizing the E-rate Program for Schools and Libraries	)	WC Docket No. 13-184
	)	
	)	
Wireline Competition Bureau Seeks Comment on Proposed Eligible Services List for the E-rate Program	)	
	)	
	)	

COMMENTS OF NCTA – THE INTERNET & TELEVISION ASSOCIATION

NCTA – The Internet & Television Association (NCTA) submits these comments in response to the Wireline Competition Bureau's public notice seeking comment on the proposed eligible services list for the schools and libraries universal service support mechanism, known as the E-rate program, for funding year 2022.[1] NCTA advocates the following changes to the proposed list: (1) allow E-rate to support network security equipment and services; (2) move firewall protection from Category Two to Category One regardless of how it is offered; (3) move Wi-Fi functionality from Category Two to Category One; and (4) clarify that routing and switching equipment that enables Category One broadband service is itself Category One equipment.

1. The Commission Should Provide Support For Network Security

As NCTA and its member companies have advocated previously, E-rate funding should support the provision of network security equipment and services to protect schools and libraries from cyberattacks.[2] Cyberattacks against school networks have grown alarmingly over the past several years, perpetrated by individuals intending to create alarm and chaos, interrupt online

---

[1] *Wireline Competition Bureau Seeks Comment on Proposed Eligible Services List for the E-rate Program*, Public Notice, WC Docket No. 13-184, DA 21-1062 (WCB rel. Aug. 27, 2021).

[2] Reply Comments of NCTA – The Internet & Television Association, WC Docket No. 13-184 (Sept. 18, 2019); Comments of Cox Communications, Inc., WC Docket No. 13-184 (Sept. 9, 2019) (Cox Comments).

testing, or extort money through a ransomware attack.[3] As documented in a recent Joint Cybersecurity Advisory coauthored by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC), ransomware, distributed denial of service (DDOS), and other cyberattacks against K-12 schools have been increasing and schools continue to be especially vulnerable to these types of attacks.[4]

These types of attacks can cripple school and library networks, making their Internet services functionally or actually inaccessible. A DDoS attack is an attempt from an outside individual or group to overload network systems, equipment, and memory resources. DDoS attacks do not simply slow down Internet service; they can cripple systems and effectively result in a temporary loss of Internet service. 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.

When a school is victimized by a DDoS attack or ransomware, the educational goals of the E-rate program obviously are seriously compromised by the complete lack of internet access. Cyberattacks can also result in additional harms, such as threatening disclosure of sensitive information regarding students. The cost of recovering from these types of attacks can be extremely expensive.

For all these reasons, it is no longer a luxury for schools to invest in cyberattack prevention equipment and services. It is time for the Commission to enable schools to make the

---

[3] *See* Cox Comments at 1 n.4 (listing examples of cybercrimes against schools in Louisiana, New York, Connecticut, Oklahoma, Rhode Island, and multistate services).

[4] *See* Joint Cybersecurity Advisory, *Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data* (Dec. 10, 2020), https://us-cert.cisa.gov/sites/default/files/publications/AA20-345A_Joint_Cybersecurity_Advisory_Distance_Learning_S508C.pdf. *See also*, Dan Patterson, *Schools have become the leading targets of ransomware attacks*, CBS News (Mar. 11, 2021), https://www.cbsnews.com/news/schools-popular-ransomware-targets/; Nic Querolo and Shruti Singh, *Schools Brace for More Cyberattacks After Record in 2020*, Bloomberg CityLab (Aug. 9, 2021), https://www.bloomberg.com/news/features/2021-08-09/schools-brace-for-more-cyberattacks-after-record-2020.

necessary investments by providing E-rate support for the purchase of products and services such as intrusion protection, malware detection, content filtering, and firewall protection that will help prevent such attacks. The network equipment and services that protect against cyberattacks may be offered through hardware-based solutions or through virtual cloud-based solutions. Because many types of services are transferring to software-based services, the Commission should make clear that, so long as the underlying function is eligible for E-rate support, virtualized services that perform the same function as a traditional hardware-based solution are eligible as well. Accordingly, E-rate support should be available for all forms of network security service. [5]

2. The Commission Should Treat Firewall Protection As A Category One Function

The Commission has stated that a bundled Internet access service that includes firewall protection, domain name service, dynamic host configuration, or similar features is fully eligible for Category One support where those "features are provided as a standard component of a vendor's Internet access service."[6] By contrast, "[f]irewall protection that is provided by a vendor other than the Internet access service provider or priced out separately will be considered a Category Two internal connections component."[7] This guidance presents operational and compliance challenges because the question of whether a feature like firewall protection is considered a "standard component" or "priced out separately" is often unclear.

To address this concern, the Commission should clarify that firewall protection will be considered a "standard component" of a vendor's Internet access service when offered as a standard part of a bundle to E-rate participants, irrespective of how the vendor offers similar

---

[5] Adding network security equipment and services to the ESL will also even the playing field by making it clear that all providers may offer them, whereas currently only a few who provide service exclusively to schools and libraries offer them as "standard components" under the ancillary services rule.

[6] *Modernizing the E-Rate Program for Schools and Libraries*, Order, 35 FCC Rcd. 13793, 13804 App. B at 12 (WCB 2020).

[7] *Id*.

services to other customers outside the E-rate program. Clarifying the rules in this manner will avoid the problems that result from the fact that service providers seem to take varying approaches in determining whether firewall protection and similar features qualify as "standard components" of the Internet access services they offer to E-rate applicants. For example, some providers may inform customers that Category One funding will be available based on the inclusion of firewall protection as a standard component of the Internet access service they tailor for E-rate customers, even if they simultaneously offer other, non-E-rate customers firewall protection as an optional, separately priced, add-on feature. But other providers may conclude that the existence of a separately priced option for non-E-rate customers prevents treating firewall protection as a "standard" included element of Internet access uniquely for E-rate customers.

The lack of specific guidance from the Commission on this issue is causing significant public interest harms. To the extent that the Commission's intent is to allow firewall protection to be treated as a Category One service only when a service provider offers it as a standard element of Internet access to all customers in a geographic area, then program integrity is being undermined by numerous providers that rely on a more permissive reading of the eligibility rules. But if the Commission does intend to allow providers to treat firewall protection or other features as eligible under Category One when offered as a standard part of unique E-rate offerings, even if they also offer such features on an optional, separately priced basis to other customers, then providers that have construed the rules more conservatively and their customers are being needlessly deprived of available support. Such divergent interpretations of the eligibility rules distort competition and may result in schools and libraries selecting less qualified providers based on artificial differences in available support.

The Commission should resolve this situation by clarifying that providers need only offer firewall protection or similar features as a standard component of their specific E-rate service offerings, irrespective of how such features may be offered to other customers. That approach will ensure that Category One funding is available for much-needed features such as firewall protection. As noted above, network security is imperative for E-rate applicants, as the Commission recognized in allowing firewall protection and other security features to be included in Category One bundles in the first place. To the extent that uncertainty about E-rate policies deters service providers from including critical security functions in products, it harms schools and libraries and the communities they serve. Providing this clarification also will eliminate the uncertainty and competitive distortions flowing from the divergent practices that providers take in the marketplace.

3. The Commission Should Treat Wi-Fi As A Category One Function

Achieving the educational goals of the E-rate program requires that students have access to the Internet in the places where they learn and on the devices they use. With the prevalence of wireless devices such as laptops and tablets and the diminishing use of wired desktop computers, Wi-Fi should now be considered an essential functionality. If Wi-Fi is not adequately funded, it may materially harm a school's ability to use the Internet for educational purposes.

Given the undeniable importance of Wi-Fi, continuing to treat it as a Category Two service no longer makes sense from a policy perspective. The E-rate program has enabled significant investment over the years in dramatically enhanced capacity to school buildings, but the promise of that investment will go unfulfilled unless the Commission now takes the steps necessary to facilitate getting high-capacity bandwidth to the devices students are using in the classroom by treating Wi-Fi as a Category One function.

4. The Commission Should Clarify That Routing and Switching Equipment Is Category One When It Supports Category One Broadband

The Commission should clarify that network equipment necessary to make a Category One broadband service functional that also enables Category Two cloud-based functionalities can be treated entirely as Category One costs without any cost allocation. The current approach of requiring a cost allocation when equipment that enables a Category One broadband service also contains routing and switching functions or other Category Two capabilities creates significant uncertainty as to whether and how costs should be allocated. For example, cloud-based functionalities typically will not have components that can be isolated for cost-allocation purposes and any mandate to allocate costs necessarily will produce arbitrary results.

As with the issues identified above in connection with firewall services provided as a standard component of a Category One service, the uncertainty surrounding mixed eligibility network equipment that facilitates other Category Two services could distort competition based on differing interpretations by providers of the existing guidance. Accordingly, the Commission should make the requested clarification.

Respectfully submitted,

/s/ Steven F. Morris

Steven F. Morris
NCTA – The Internet & Television Association
25 Massachusetts Avenue, NW – Suite 100
Washington, D.C. 20001-1431

September 27, 2021