Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Modernizing the E-Rate Program for Schools	)	WC Docket No. 13-184
and Libraries	)	
	)	

REPLY COMMENTS OF ADTEC, ADMINISTRATIVE AND TECHNICAL CONSULTING, INC. ON THE FY 2020 PROPOSED ELIGIBLE SERVICES LIST FOR THE SCHOOLS AND LIBRARIES UNIVERSAL SERVICE MECHANISM (DA 19-738)

AdTec, Administrative and Technical Consulting, Inc. submits these reply comments in response to the FCC Wireline Competition Bureau's Public Notice, released August 2, 2019 (DA 19-738), regarding the E-rate Eligible Services List ("ESL") for funding year 2020 and the comments submitted by COX COMMUNICATIONS, INC. on 9/9/2019.

In their comments, Cox Communications urged the Bureau to include in the ESL "network security equipment and services to prevent and recover from cyberattacks," and specifically described the issue of Denial of Service ("DoS") attack prevention and mitigation. AdTec concurs with the comments of Cox Communications, and wishes to amplify those with a recent example.

School districts in the state of Indiana avail themselves to an e-mail listserv in which Technology Directors exchange information regarding problems and solutions they face as they manage and protect school district networks. The following exchange from last week merits the Bureau's attention and underscores the importance of this topic. Author's names have been omitted rather than to provide attribution without permission, and posts were paraphrased for brevity.

> --
> *Sent: Wednesday, September 11, 2019*
> *Subject: DDOS*
>
> *We had a student use https://www.stressthem.to/ from his phone to flood our 1GB Internet for 5 minutes. There was no charge from the website for him to do this. He repeated this for 3 hours thus making our Internet crawl/unusable. Luckily he bragged to his friends, we questioned him, he confessed.*
>
> *Any proven defenses against this? I'm told there is almost nothing we can do. It could happen again tomorrow.*
>
> --
> *Sent: Wednesday, September 11, 2019 1:40 PM*
> *Subject: Re: DDOS*
>
> *We had this happen a few years ago and changed our public IP while monitoring the suspected student's screen. As soon as the IP was changed, the student immediately went to a site to see*

> *what our new IP was. We also got the Indiana State Police involved. With witnesses to some of the activities, we were able to press charges.*
>
> *It looks like the price has gone down. Our student paid $30.00.*
>
> *--*
> *Sent: Wednesday, September 11, 2019*
> *Subject: Re: DDOS*
>
> *He could actually do it again. We expelled him. All you need to know is our IP addresses. Anyone could do it. :-(*
> *--*

Consequences for schools can be dire. When DDoS attack occurs, a school district's connection to the outside world is so fully saturated with incoming data that no traffic can pass out. Not only is the business of education disrupted, but for schools depending on their Internet access to remain connected to first responders, public safety is also endangered. There is potential for great harm from such an easy attack: harm to the school and its occupants, and serious and life-changing consequences for a young student who might not know the "prank" they undertake can lead to their expulsion or be prosecuted as a felony.[1]

There are services and tools to mitigate these problems, but without E-rate support, most schools and libraries cannot afford them. It is imperative that the Bureau add such services to the ESL in Category 1 and such tools in Category 2, as it is clear from the evidence that the networks that the Universal Service Mechanism has so carefully assisted in building can be rendered unusable by the actions of almost anyone with the inclination to do so.

Respectfully submitted by

__________/s/____________
Dan Rice
Consultant
AdTec, Administrative and Technical Consulting, Inc.

September 18, 2019

[1] See https://www.abc57.com/news/high-school-hackers-in-elkhart-face-felony-charges, posted Oct 5, 2015.