BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of Schools and Libraries Cybersecurity Pilot Program	WC Docket No. 23-234

REPLY COMMENTS OF INTERNET2

Belinda Nixon
Internet2
1150 18th Street, NW
Suite 750
Washington, DC 20036

Adam D. Bowser
ArentFox Schiff LLP
1717 K Street NW
Washington, DC 20006
Counsel for Internet2

Date: February 27, 2024

SUMMARY

At its core, Internet2 is a non-profit organization dedicated to providing advanced technologies to securely connect educational institutions to their educators and students. Internet2 therefore fully supports the Commission's proposal to fund cybersecurity and advanced firewall services for eligible schools and libraries through the Pilot Program.

As further detailed below, the Commission should focus funding on commonly-faced cybersecurity threats for schools and libraries – such as distributed denial-of-service (DDoS) attacks. And just as importantly, Internet2 strongly supports the Commission's proposal to make these solutions available through cloud-based services that will, in Internet2's experience and as detailed in the initial comments, provide the most cost-effective solutions. In this way, the Commission's Pilot Program will be able to benefit the greatest number of schools and libraries from the most common cybersecurity threats.

BACKGROUND ON INTERNET2

Internet2 is a non-profit, member-driven advanced technology community founded in 1996 by the nation's leading higher education institutions that provides a secure high-speed network, cloud solutions, research support, and identity and access management services tailored for research and education ("R&E"). Internet2 helps U.S. R&E organizations to solve shared technology challenges and develop innovative solutions in support of their educational, research, and community service missions. Internet2 also operates the nation's largest and fastest coast-to-coast national research and education network ("NREN"), which now serves 323 U.S. universities, 59 government agencies, and 45 regional and state education networks.

Internet2 has helped the R&E community solve many of the same cybersecurity challenges that schools and libraries currently face, and which are the subject of this proceeding

and related Pilot Program. Internet2 operates the InCommon Federation, which facilitates secure, unified, and seamless single sign-on access to local and global research and academic collaboration resources for more than 10 million users and 800 educational institutions, research organizations, and commercial resource providers in the U.S. InCommon makes possible trustworthy academic collaboration that reaches far beyond what a single organization can do on its own, through identity and access management technologies and services that are integrated across the globe. Internet2 also offers its eduroam service in the U.S to enable seamless roaming Wi-Fi at nearly 1,000 colleges, universities, schools, museums, libraries, and research facilities across the country. Additionally, Internet2 offers a cloud-based DDoS Mitigation Service to protect subscribers at the institution level from external threats.

Further, Internet2 plays a key role as a convener and facilitator of the R&E community. Internet2 regularly brings together representatives from academia, federal agencies, and private industry to foster collaboration and find solutions to common challenges related to R&E cyberinfrastructure and security that no single institution or organization could accomplish independently. In fact, Internet2 collaborates with a multitude of NREN partners across the globe that represent more than 100 countries. Finally, Internet2 supports the R&E community through the Internet2 NET+ Cloud Services Program, which enables R&E institutions in adopting cloud solutions through a streamlined process that minimizes the business, legal, financial, and other challenges associated with migrating from on-campus to cloud-based solutions, which can be extended to the K-12 environment.

DISCUSSION

I. Funding Should Focus On Preventing Common Threats Through Cloud-Based Solutions

Internet2 strongly agrees with the conclusions contained in the CISA K-12 Cybersecurity Report that schools and libraries should focus on implementing a "small number of the highest priority steps," such as minimizing exposure to common cybersecurity attacks.[1] In Internet2's experience, DDoS attacks have unfortunately become commonplace today. To help the greatest number of schools and libraries address these challenges through the Pilot Program, Internet2 encourages the Commission to follow through on its proposals to provide schools the ability to tackle these cybersecurity challenges through the use of cloud-based solutions.[2] Indeed, as school districts themselves noted in their initial comments, cloud-based cybersecurity services are a practical necessity in today's networking environment.[3] Students will be constantly accessing a school's network remotely from their homes, and cloud-based services will "allow students off campus to have the same cyber protections as if they were on campus."[4] And as others have noted, cloud-based services are easier to scale, and thus more cost effective[5] – allowing the Pilot Program's limited funds to go farther to protect more school districts from common cybersecurity threats.

---

[1] NPRM, ¶ 22; *see also* ¶ 35 (seeking comment on "certain types of cyber threats or attacks that schools and libraries most commonly face").
[2] NPRM, ¶ 43.
[3] *See, e.g.*, Comments on Proposed Schools and Libraries Cybersecurity Pilot Program of Clark County School District, at 2, *available at* https://www.fcc.gov/ecfs/document/101292815129568/1 ("Clark County Schools Comments").
[4] *Id.*
[5] *See, e.g.*, Comments of the Cybersecurity Coalition, at 5, *available at* https://www.fcc.gov/ecfs/document/10127205116784/1.

A. DDoS Mitigation Through Cloud-Based Solutions

DDoS attacks occur when a hacker gains control of a number of hosts on the network and directs large volumes of traffic from those hosts to one or more target hosts. Hackers often use "botnets" in such attacks. Botnets are large collections of computers infected by worms or trojans that are taken over and remotely controlled by hackers to send spam, propagate viruses, or launch denial of service attacks. The number of compromised hosts on the Internet can be staggering – in the hundreds of thousands. When DDoS attacks occur across a network, the results can be devastating. A DDoS attack focused at a single machine on a campus can easily saturate a gigabit connection.

By some estimates, DDoS attacks against K-12 institutions jumped by an alarming 350% in the last few years. In some cases, school districts' networks were down for days, not only making E-Rate funded services essentially useless during these periods, but also bringing student instruction to a halt. It is also important to note that while disruption to the target network is often the purpose of these attacks, the DDoS attacks may also serve as a smoke screen for more sophisticated attacks. That is, while school IT departments are focused on restoring the network, cybercriminals could be working in the background to obtain unauthorized access to other school systems and data. A cloud-based solution designed to identify and mitigate DDoS attacks would be extremely useful to ensure the security of school and library networks. Indeed, as school districts rightly note, "leaving one device exposed compromises an entire network."[6] Simply put, exposing student devices while they are off-campus is an invitation for bad actors to exploit

[6] Clark County Schools Comments at 2.

those devices when they are back on campus, leaving the school's entire network more exposed to attack. At bottom, cloud-based solutions are not only more cost effective, but they are also a practical necessity to counter common cybersecurity threats facing schools and libraries today. Internet2, along with the other commenters in this proceeding, therefore fully supports the Commission's proposal to fund such cloud-based cybersecurity solutions.

CONCLUSION

As the Commission itself recognized, schools and libraries should be provided "the flexibility to cost-effectively procure remotely-located equipment and services obviating the need to install, maintain, and troubleshoot solutions on-site."[7] Such "cloud-based, centralized resource[s] accessible via the Internet" are indeed the cybersecurity solutions offered in the market currently in the most cost-effective manner to address cybersecurity vulnerabilities such as DDoS attacks. Accordingly, Internet2 fully supports the Commission's proposal to make cloud-based cybersecurity services eligible under the Pilot Program, and Internet2 encourages the Commission to establish the Pilot Program consistent with these recommendations.

Respectfully submitted,

/s/ Belinda Nixon
Belinda Nixon
Vice President and General Counsel
Internet2
1150 18th Street, NW
Suite 750
Washington, DC 20036

[7] NPRM, ¶ 43.