January 29, 2023

Comments of the Alliance for Digital Innovation to the Federal Communications Commission, Wireline Competition Bureau

WC Docket No. 23-234

Re: Schools and Libraries Cybersecurity Pilot Program

The Alliance for Digital Innovation (ADI) submits this comment in response to the Federal Communications Commission's (FCC or the Commission) Wireline Competition Bureau's notice of proposed rulemaking (NPRM) on the Schools and Libraries Cybersecurity Pilot Program (Pilot).

We submit these comments on behalf of our members, which include cybersecurity and digital service companies that service public sector entities at the federal, state, and local levels across the United States. Our members represent a cross-section of technology and service providers, all of which are dedicated to meeting and exceeding the needs of our public sector customers.

ADI commends the Commission for its work to bolster schools' and libraries' access to cybersecurity technologies and services and is broadly supportive of the proposed three-year pilot program within the Universal Service Fund (USF) to provide up to $200 million to support cybersecurity and advanced firewall services for eligible schools and libraries.

We strongly believe that schools and libraries should have access to federal funding to strengthen their cybersecurity, particularly as more of these organizations are reliant on connected devices and endpoint devices. We offer comments on five aspects of the Pilot as outlined in the NPRM, including those related to funding, the future of the program, eligible security technologies, reporting requirements, cybersecurity training, and organizational commitment.

1. **The Commission should increase the funding available in the program, as well as permanently establish the Schools and Libraries Cybersecurity Program upon the completion of the Pilot Program and announce plans well in advance.**

There are nearly 150,000 schools and libraries in this nation, and many lack the funding necessary for mature cybersecurity programs. Schools have become particularly attractive targets for cyberattacks and ransomware attacks by malicious actors. While we appreciate that the $200 million budget represents a substantial investment from the Commission over the next three

years, progress needs to be made quickly in ensuring schools and libraries have the tools and technologies necessary to prevent costly attacks.

ADI also recommends that the Pilot be used to evaluate program performance and modify specific aspects of the program, rather than to evaluate whether a full program should be launched in the future. We encourage the Commission to establish the program on a permanent basis upon the completion of the Pilot, and we recommend that the Commission releases a public notice outlining a plan for sustaining cybersecurity services for schools and libraries no less than eighteen months in advance of the end of the Pilot. This will allow eligible organizations to adjust their budgeting and planning accordingly. The NPRM notes that the E-Rate program or the Universal Service Fund are potential funding mechanisms after the Pilot is completed.

2. **The Commission should not prescribe specific eligible security technologies and solutions.**

ADI recommends that the Commission avoid stipulating specific security technologies that are available for pilot funding. Each school or library has a different risk profile depending on several factors, such as size, type of technology currently in place, and type of cyber threats, among others. In particular, schools are using a large number of different applications to address student needs while they are both on-premises and remote. It is important that each organization is empowered to tailor solutions to manage their specific risk.

We encourage the Commission to instead designate broad categories of security services that preserve flexibility while ensuring that the Pilot remains dedicated to security, as opposed to general IT or technology modernization. These categories may include:

- **Endpoint Detection and Response (EDR) tools and service.** Today, school systems often have many endpoint devices such as desktops, laptops, and mobile devices, as well as other connected devices. EDR is a critical tool to defend these devices and particularly important for early prevention of ransomware.

- **Cloud services.** Organizations can reduce attack surfaces by retiring legacy applications and infrastructure and migrating to cloud services. Additionally, native cloud-based security solutions can be leveraged for improved scalability. Network and cloud scanning and monitoring services can also be used to secure remote learning services and records stored by an organization.

- **Vulnerability management, penetration testing, bug bounty solutions and services.** These solutions can be used to proactively identify and prioritize vulnerabilities that can be exploited by adversaries. Additionally, third-party cybersecurity assessments can be used as a measure of the effectiveness of an organization’s cybersecurity strategy when they are again executed, post implementation of cybersecurity measures.

- **Digital Identity.** Digital identity tools, such as single sign-on (SSO), phishing resistant multi-factor authentication (MFA), identity governance, privileged identity management, and related identity technologies are crucial cybersecurity solutions to verify and authenticate the identity and access levels for K-12 workforce users, as well as students and families accessing educational services both remotely and on-premises. It is also important to include solutions that automate these identity processes at scale, in a secure way that allows organizations to extend and integrate with other solutions in their environment, enabling educational institutions to support better academic outcomes. This is particularly important as more schools engage in remote learning, implement Bring-Your-Own-Device policies, and face identity-related cyber-attacks such as password spraying and credential stuffing.

- **Zero Trust Architecture.** In addition to identity authentication, other Zero Trust cybersecurity tools can be implemented to reduce or prevent lateral movements by adversaries if they do gain access to a network.

- **Logging Practices.** Organizations can utilize tools and systems to collect and maintain security-relevant log information to improve proactive security measures and incident assessments.

- **Managed solutions or cybersecurity as a service.** These services are beneficial for organizations lacking the cybersecurity maturity or workforce to run sufficient internal security programs. They also allow organizations to scale cybersecurity programs more easily without requiring significant technical expertise. As the Consortium for School Networking (CoSN) reported last year in their annual State of EdTech Leadership Survey, hiring and retaining skilled personnel is the second leading IT challenge among school systems, trailing only budget constraints.[1]

Many of these solutions, tools, and services may include on-going, recurring costs due to service contracts or updates, for example. The Commission should avoid limiting participants to one-time purchases, as it will create artificial barriers on the type of technologies that Pilot participants are able to use—or possibly even lead to the use of outdated technologies.

3. **The Commission should avoid overly onerous incident reporting requirements, both before and during the Pilot Program.**

ADI recommends that the Commission does not require applicants to the Pilot Program to report previous cyber threats or incidents as part of the application. We also recommend that the Commission does not use previous cyber incidents as a metric to allocate funding. Organizations that have not experienced cyber incidents may still have immature or inadequate cybersecurity programs; such organizations may be unaware of the full extent of prior or ongoing cyber

[1] State of EdTech Leadership Survey: https://www.cosn.org/edtech-topics/state-of-edtech-leadership/

incidents, or even of the occurrence of a cyber incident altogether. We urge the Commission to evaluate applicants based on a holistic risk profile and application.

The Commission should avoid requiring participants to provide an excessive amount of information during the Pilot. Collecting and reporting information may result in additional strains on participants that are already lacking sufficient resources. Additionally, information such as the number of intrusion attempts and estimated cost of each attack may be difficult to measure or subjective based on the reporting organization; therefore, it is unlikely that this information will provide beneficial or measurable insights for the Commission. If the Commission must collect information to measure the efficacy of the program, it should consider metrics like the mean time to detection and response.

Additionally, it is critical that any reporting requirements include a guarantee that data will be anonymized and kept confidential. Eligible organizations may be reluctant to participate in the Pilot due to concerns that sensitive information may become public.

4. **The Commission should make cybersecurity awareness training a requirement for acceptance into the Pilot Program.**

Cybersecurity awareness training is a necessary component of any effective Cybersecurity Strategy to help minimize risks stemming from the human element. The first major line of defense is the awareness and good practices of users. Cybersecurity awareness training should be a factor when selecting Pilot schools or libraries. There are several free resources to consider for organizations that do not have sufficient resources or funding to support this training: Nationwide Cybersecurity Review (NCSR), CISA K-12 Cybersecurity Toolkit, Cybersecurity Rubric, and CoSN's Trusted Learning Environment (TLE) Seal Program.[2] Selected pilot organizations should pledge to use these or other cybersecurity training resources as a baseline commitment to acceptance into the program.

5. **The Commission should make leadership commitment a requirement for Pilot Program consideration.**

Senior leadership commitment plays a pivotal role in prioritizing cybersecurity within organizations. Leaders at the executive level set the tone for security culture, demonstrating that cybersecurity is a top priority. Their commitment ensures the allocation of essential resources, compliance with regulations, protection of reputation, and alignment with strategic goals. Senior leadership involvement also sets the priority for cybersecurity awareness training among staff, which was identified above as a necessary component of a successful cybersecurity strategy. In

[2] NCSR: https://www.cisecurity.org/ms-isac/services/ncsr;
CISA K-12 Cybersecurity Toolkit: https://www.cisa.gov/online-toolkit-partnering-safeguard-k-12-organizations-cybersecurity-threats;
Cybersecurity Rubric: https://www.cybersecurityrubric.org/resources;
CoSN's TLE Seal Program: https://www.cosn.org/edtech-topics/trusted-learning-environment/

today's digital age, having senior leaders that prioritize and champion cybersecurity is not just a best practice – it is a fundamental necessity for organizational cybersecurity and resilience.

The Alliance for Digital Innovation appreciates the opportunity to submit these comments for the Commission's consideration, and we hope our input will be helpful. If ADI can offer further assistance as the Commission continues its work to establish the Schools and Libraries Cybersecurity Pilot Program, please contact ADI's Director of State Programs Dan Wolf at dwolf@alliance4digitalinnovation.org.

Respectfully Submitted,

The Alliance for Digital Innovation