Institute for Security and Technology
195 41st Street
#11045
Oakland, CA 94611

securityandtechnology.org

September 12, 2025

Dear Chairs Fischer and Hudson and Ranking Members Lujan and Matsui:

Thank you for the opportunity to comment on potential reforms to the Universal Service Fund (USF). We write as cybersecurity policymakers, who, collectively, have experience in Congress and at the White House as well as administering IT programs in schools and overseeing them at the U.S. Department of Education. We are focused on the critical need to include cybersecurity as a fundable activity for the E-Rate and Rural Healthcare programs as part of any USF reform effort.

Under E-Rate, Congress already requires that schools and libraries have Internet safety policies that address "unauthorized access" and "unauthorized disclosure… of personal identification information regarding minors." However, until the current Schools and Libraries Cybersecurity Pilot Program, the Federal Communications Commission only allowed schools and libraries to use E-Rate funds to purchase "basic firewalls" rather than a more robust set of cybersecurity technologies and services that protect students' safety, security, and privacy from cyber criminals.

The increasing speed, scope, and impact of cyber threats to K-12 schools and hospitals–entities that house valuable data but are unable to afford cutting-edge cybersecurity solutions– demands increased investment and support. Each week, K-12 schools face an average of five cyber incidents. Ransomware has shut down schools across the country, and one technology vendor's data breach in December 2024 affected more than 60 million students across thousands of school districts.

These incidents can have real impacts on children and their education. Stolen personal data can be used to create synthetic identities, leaving kids with damaged credit when they graduate. When schools shut down due to unavailability of their information systems, learning suffers—as does the delivery of other social services like nutrition programs that are integrated into the education system. When E-Rate was passed nearly 30 years ago, Congress could not have intended that access to the Internet enabled through universal service funds would be leveraged to deny students an education or impact their food security.

Thankfully, USF Reform offers an opportunity to clarify eligible expenses under E-Rate–and potentially the Rural Healthcare Program–to include modern cybersecurity tools and services that can meaningfully reduce the risks cyber criminals pose to students (and patients). The FCC took an important first step in

authorizing the Schools and Libraries Cybersecurity Pilot Program (Cybersecurity Pilot) in June 2024. However, the funding for the program has been woefully inadequate: schools and libraries submitted over $3.7 billion in requests for assistance, more than fifteen times the program budget of $200 million.

There are several approaches that Congress and the FCC could take to ensure the safety and security of universal service fund recipients, including:

- **Codifying a cybersecurity program similar to the pilot** that leverages existing E-Rate infrastructure. Congress could set a yearly program cap that more closely meets the demonstrated need from E-Rate-eligible entities or provide guidance to the FCC regarding the appropriate level of support. Congress might also consider directing the FCC to create a "Category Three" for cybersecurity tools and services that mirrors existing E-Rate reimbursement allocations.
- **Expanding the list of eligible services under the E-Rate program to include modern cybersecurity technologies,** rather than the limited "basic firewalls" that are eligible for reimbursement under Category Two today. The current list of allowable expenses (excluding those allowed through the pilot) does not account for most current- or next-generation cybersecurity technologies. To avoid challenges as the market advances, Congress would likely need to provide a mechanism to adjust the list as technology evolves.
- **Creating a cybersecurity set-aside** that provides strategic direction to the FCC about the minimum proportion of E-Rate funding that should go to cybersecurity. This outcome-oriented approach allows the FCC to innovate with different program designs while still providing a clear strategic intent from Congress.

As part of USF Reform, we urge Congress to also consider similar approaches with respect to rural healthcare. Hospitals have cited ransomware incidents as events that helped precipitate closures, and there has been extensive documentation of patient harms due to unavailability of systems due to malicious activity. Healthcare is another sector that is increasingly being targeted by criminals, and USF reform provides a unique opportunity to help rural hospitals address a significant risk they face—one rooted in their enhanced connectivity.

At the Institute for Security and Technology, we are committed to collaborating with technologists and policymakers to advance practical solutions for pressing challenges in national security and public safety. We have provided specific answers to the questions posed in your request for comment below. We would also

welcome the opportunity to discuss our work with you and your staff as you continue to develop USF Reform proposals.

Thank you for your leadership on this issue, and we look forward to continued dialogue on ways to ensure the safety and security of some of our most vulnerable populations, including our students and patients, in this connected world.

Sincerely,

Nicholas Leiserson
Senior Vice President for Policy

Michael Klein
Senior Director for Preparedness and Response