IST POLICY MEMO | JULY 2025

Cybersecurity Considerations for Universal Service Fund Reform

By Nicholas Leiserson

Following the decision in FCC v. Consumers' Research,[1] Congress has expressed a clear desire to reinvigorate the Universal Service Fund (USF) through legislation.[2]

Historically, USF funding has had only limited applicability to cybersecurity tools and services. However, with requests for the FCC's recent cybersecurity pilot exceeding 18 times the allocated budget, the education community has demonstrated clear demand for broadband access that brings opportunity without also leaving schools more vulnerable. Should policymakers wish to take action to address cybersecurity gaps at "target rich, cyber poor" educational institutions, there are several means they could use to do so, including codifying a cybersecurity program similar to the pilot, expanding the list of eligible services under the E-Rate program to include modern cybersecurity technologies, or creating a cross-sector cybersecurity set-aside.

Background

Cyber Threats to K-12

The speed, scope, and impact of cyber threats to K-12 schools continues to increase. Cyber criminals are increasingly targeting organizations like schools and hospitals—entities that house valuable data but are unable to afford cutting-edge cybersecurity solutions. An average of five cyber incidents occur each week impacting K-12 schools.[3] Ransomware has shut down schools across the country,[4] and one technology vendor's data breach in December 2024 affected more than 60 million students across thousands of school districts.[5]

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 that are integrated into the education system, such as nutrition programs.

School systems face a challenging funding environment, and shared services provided by the U.S. Government have been scaled back since the beginning of 2025.[6]

The E-Rate Program

The Federal Communications Commission administers the E-Rate Program using monies from the Universal Service Fund, a fee-based mechanism that aims to ensure all Americans have access to affordable communications. E-Rate, which was authorized by Congress in 1996, helps schools and libraries obtain affordable broadband Internet service.[7] The program allocates funding based on demonstrated need, up to a limit set by the FCC (currently $4.456 billion). While E-Rate funding can be used for basic firewalls,[8] core network security features, such as Protective Domain Name System (PDNS) resolution services, are not reimbursable through the program.[9] The E-Rate program also does not cover other cybersecurity technologies central to mitigating the risks that come with Internet access, such as endpoint protection or identity and access management.[10]

info@securityandtechnology.org · 195 41st St, #11045, Oakland, CA 94611 · securityandtechnology.org

The Cybersecurity Pilot

In June 2024, the FCC adopted an order creating the "Schools and Libraries Cybersecurity Pilot Program." Based on the 2020 Connected Care Pilot, it provides a specific allocation of $200 million from the USF for an expanded list of cybersecurity services.[11] The stated goal of the program is to determine whether using USF monies "advances the key universal service principles of providing quality Internet and broadband services to K-12 schools and libraries at just, reasonable, and affordable rates; and ensuring schools' and libraries' access to advanced telecommunications." The pilot runs over a three-year term. All E-Rate eligible entities are able to participate.

Applications for the funds closed on November 1, 2024. The FCC received over $3.7 billion in requests, more than 18 times the funding allocated for the pilot. Of the 2,734 applicants, 707 were selected to participate, based on a combination of factors including number of students eligible for the National School Lunch Program and geographic diversity. Participating schools are now in the process of bidding for services and preparing requests for reimbursement.

Policy Approaches

The FCC's cybersecurity pilot has clearly demonstrated significant unmet need for security tools and services among E-Rate-eligible schools. This gap is consistent with findings from other Federal agencies,[12] the Government Accountability Office,[13] and private sector analysis.[14, 15]

USF reform presents a unique opportunity for legislators to determine whether measures to ensure the safety of students in the face of Internet-based threats should fall within the remit of USF-funded programs.[16] Should Congress wish to codify an explicit cybersecurity mission into the USF, there are several approaches it could take.[17]

Codify the Pilot

Policymakers could codify the cybersecurity pilot, transitioning it into a full USF program.[18] The unmet need for cybersecurity services is significant, and the pilot has existing infrastructure that could easily transition to a permanent program. Doing so would provide a targeted intervention for K-12 entities whose cybersecurity posture cannot keep up with the current threat environment. Congress could scope the program with a specific dollar cap per year, ensuring that expanding and sustaining Internet access—the primary purpose of the USF—is not subsumed by cybersecurity investments. At the same time, a dedicated program ensures that cybersecurity is not ignored entirely, a challenge that has been observed in the context of other Federal grant programs.

Update Eligible Expenses

Policymakers could update the eligible uses for E-Rate funds to more explicitly include cybersecurity services. For instance, licenses for endpoint detection and response capability might be reimbursable at a certain rate for a subset of high value assets. 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. This approach would keep the locus of control with educational entities, which have the best understanding of their own specific needs across access, networking infrastructure, and security. Avoiding a fixed dollar cap for cybersecurity reimbursements would also allow funding to scale to meet demand.

Create a Cyber Set-aside

Rather than addressing programs directly in statute, Congress might consider setting a goal for the FCC that allocates a set proportion of E-Rate funds to apply to cybersecurity needs. While estimates vary, surveys of chief information security officers in industry reflect that approximately 10 percent of IT spending is used for security.[19] Congress could consider a similar target and leave it up to the Commission to design both programs to implement it and evaluation metrics. This approach provides maximal flexibility to evolve over time while still offering clear direction from Congress to the Commissioners on the importance of cybersecurity.

ADDITIONAL CONSIDERATIONS

Combining Approaches

The approaches outlined above are not mutually exclusive. For instance, Congress may consider codifying the cybersecurity pilot as a way to set a "floor" for the annual investment using universal service funds. At the same time, policymakers could also expand eligibility, so that schools with acute cybersecurity needs could get reimbursed through the traditional E-Rate program. Such a hybrid approach might offer the best of both worlds, giving local education agencies more flexibility while ensuring some progress each year toward improving the resilience of the sector.

Smaller Organizations

Smaller education agencies may lack the IT personnel or grant-writing support necessary to successfully navigate a new E-Rate program. Many cybersecurity services can also be deployed at scale, whether through state educational agencies, regional education networks, or blanket purchase agreements.[20] Policymakers may wish to consider approaches that allow for state or regional cooperation on cybersecurity services eligible for reimbursement to minimize duplication and maximize efficacy, particularly services that can support smaller schools and school districts. Policymakers should also consider ways to streamline application processes for small entities to ensure they can take advantage of new cybersecurity programs.,

Healthcare

Beyond education, universal service funds also support broadband access for rural hospitals, through the Rural Health Care Program. Many of the community institutions supported by these programs also are vulnerable to cyber intrusions, and healthcare organizations have also been increasingly targeted by cyber criminals.[21] Policymakers could consider whether the approaches outlined for the E-Rate program might also be applicable in a healthcare context. Alternatively, policymakers might adopt a USF-wide cybersecurity policy or program that is sector agnostic, so as to ensure that funding support for access is always paired with safety and security.

Way Forward

The latter half of 2025 is a critical period for determining the future of the USF. There is a demonstrated need for additional cybersecurity investment in K-12 education, and there are several mechanisms policymakers could use to leverage universal service funds for this purpose. However, it will be up to Congress to decide whether security measures should be baked into broadband offerings or bolted on through other funding mechanisms after the fact.

1 The decision, dated June 27, 2025, affirmed the constitutionality of the Universal Service Fund. "Federal Communications Commission et al. v. Consumers' Research et al.," Supreme Court of the United States, no. 24–354, argued March 26, 2025, decided June 27, 2025, https://www.supremecourt.gov/opinions/24pdf/24-354_0861.pdf.

2 Statement by Chairmen Guthrie and Hudson note that "[t]he Committee on Energy and Commerce can now turn its attention to reforming the USF…" "Chairmen Guthrie and Hudson Issue Statement After the Supreme Court Upheld the Constitutionality of the Universal Service Fund," press release, Energy & Commerce Committee, June 27, 2025, https://energycommerce.house.gov/posts/chairmen-guthrie-and-hudson-issue-statement-after-the-supreme-court-upheld-the-constitutionality-of-the-universal-service-fund.

3 "K12 Security Information eXchange (K12 SIX) Cyber Incident Map," K12 SIX, last updated February 13, 2023, https://www.k12six.org/map.

4 Kara Arundel and Shaun Lucas, "School ransomware attacks are on the rise. What can districts do?" *K-12 Dive,* October 28, 2024, https://www.k12dive.com/news/school-ransomware-attacks-cybersecurity-funding/730333/.

5 Kevin Collier, "Children's data hacked after school software firm missed basic security step, internal report says," *NBC News*, January 31, 2025, https://www.nbcnews.com/tech/security/%20powerschool-hack-data-breach-protect-student-school-teacher-safe-rcna189029.

6 Zack Quaintance, "With Less Federal Support, States Look to Lead in Cyber," *Government Technology*, July 16, 2025, https://www.govtech.com/security/with-less-federal-support-states-look-to-lead-in-cyber.

7 Almost all K-12 schools, public and private, are eligible to participate, so long as they are not-for-profit and do not have an endowment over $50 million.

8 Under Category Two, which covers internal connections needed for broadband access. "In the Matter of Modernizing the E-Rate Program for Schools and Libraries," Federal Communications Commission, WC Docket no. 13-184, October 25, 2024, https://docs.fcc.gov/public/attachments/DA-24-1104A1.pdf.

9 In fact, the FCC has explicitly declined to add these services. (see Paragraph 6, ibid.)

10 The FCC has considered adding these types of services in the past as well. "In doing so, the Commission explained that it "must balance the benefits of such protections with the cost of augmenting [the] list of supported services" and "[a]lthough [the Commission] agree[s] that protection from unauthorized access is a legitimate concern, the funds available to support the E-Rate program are constrained." "In the Matter of Schools and Cybersecurity Pilot Program," Federal Communications Commission, WC Docket No. 23-234, June 6, 2024, https://docs.fcc.gov/public/attachments/FCC-24-63A1.pdf.

11 The expansive list includes a wide array of network, endpoint, and cloud technologies. "Cybersecurity Pilot Program Eligible Services List," Federal Communications Commission Bureau of Consumer and Governmental Affairs, June 12, 2024, https://www.fcc.gov/cybersecurity-pilot/cybersecurity-pilot-eligible-services-list.

12 "Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats," U.S. Department of Homeland Security, Critical Infrastructure and Security Agency, January 2023, https://www.cisa.gov/sites/default/files/2023-01/K-12report_FINAL_V2_508c_0.pdf.

13 "Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity," Government Accountability Office, GAO-23-105480, October 2022, https://www.gao.gov/assets/gao-23-105480.pdf.

14 "E-Rate Cybersecurity Cost Estimate," CoSN and Funds for Learning, January 2021, https://emma-assets.s3.amazonaws.com/paqab/0d06153c299fd09df713071630f201df/CoSNFFL_Cybersecurity_Review_January_2021.pdf.

15 IST's Ransomware Task Force Report also suggested that policymakers consider financially incentivizing ransomware mitigations (Objective 3.4). "RTF Report: Combating Ransomware," April 2021, Institute for Security and Technology, https://securityandtechnology.org/ransomwaretaskforce/report

16 Some commissioners have suggested that the FCC may have exceeded its mandate under the Telecommunications Act by providing reimbursement for cybersecurity services. Action by Congress would also provide valuable clarity as to the intended scope of the program.

17 Beyond the FCC, the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Education, as Sector Risk Management Agency for the Education Subsector, each have valuable insights about how to protect K-12 schools. Policymakers may wish to require that the FCC consult or coordinate with these agencies in executing the cybersecurity programs outlined in this paper.

18 One option for doing so is the creation of a third category of the E-Rate Eligible Services List that includes services similar to those on offer in the cyber pilot. This new "Category Three" would inherently leverage existing processes for allocation and reimbursement.

19 "New Research from IANS and Artico Search Reveals Cybersecurity Budgets Increased Just 6% for 2022-2023 Cycle," press release, IANS, September 23, 2023, https://www.iansresearch.com/resources/press-releases/detail/new-research-from-ians-and-artico-search-reveals-cybersecurity-budgets-increased-just-6-for-2022-2023-cycle.

20 For instance, schools in a region might consider leveraging a shared security operations center to help triage and respond to cyber incidents. https://www.nascio.org/wp-content/uploads/2023/08/TXCrossBoundaryCollaborationandPartnerships.pdf

21 Heather Landi, "Healthcare remains top target for cybercriminals with an uptick in hacking attacks in 2024," *Fierce Healthcare,* April 24, 2025, https://www.fiercehealthcare.com/health-tech/healthcare-remains-top-target-cybercriminals-uptick-hacking-attacks-2024.