1. **How should Congress evaluate the effectiveness of each USF program in achieving their respective missions to uphold universal service?**

We write specifically about the need to consider cybersecurity in evaluating the effectiveness of the E-Rate and Rural Healthcare programs.

There are three elements of the goals outlined in Section 254 of the Communications Act of 1996 that are pertinent to cybersecurity:

- 254(b)(1) states that "*quality* services should be available…" [emphasis added];
- 254(b)(6) requires that "Elementary and secondary schools and classrooms, health care providers, and libraries should have *access* to advanced telecommunications services" [emphasis added]; and
- 254(b)(7) allows the Joint Board and Commission to determine "[s]uch other principles… [that] are necessary and appropriate for the *protection of the public interest*, convenience, and necessity and are consistent with this chapter" [emphasis added].

We address each in turn. In the context of broadband services, quality often refers to latency, bandwidth, and uptime. However, Congress should also evaluate quality through the lens of the "CIA Triad" of confidentiality, integrity, and availability of information stored on or transiting an information system. If an offering subsidized by universal service funds is unable to reliably fulfill these three criteria, the impacts on students, doctors, and patients can be significant.

At its base, impacts to the *availability* of services - such as through denial of service attacks - prevent users from accessing them at all. While traditional reliability metrics capture some of the harm caused by malicious activity (e.g., a broad, distributed denial of service attack that affects an internet service provider), they do not adequately account for *targeted* incidents affecting a school, library, or hospital. For instance, an attempted extortion based on traffic flooding a school's network could effectively prevent a school from accessing the Internet altogether. Such an incident would also be most effectively mitigated "upstream" by a service provider. Yet, today, services to prevent such incidents are not reimbursable under either E-Rate or the Rural Healthcare Program, and Congress does not consider them in evaluating program effectiveness.

Impacts to the integrity or confidentiality of services subsidized with universal service funds are more pernicious. If poor quality leads to cybersecurity failures, data may be read while transiting providers' networks, exposing sensitive personal information about students or patients. Those data also have the potential to be modified in transit. Consider the harm that could be caused if details in a patient record, such as blood type or medication dosing, were changed while they were being retrieved over the Internet.

With respect to 254(b)(6), Congress must recognize that access to services can be impaired not only on the provider side, such as through denial of service as discussed above, but on the subscriber side as well. Traditionally, subscriber-side issues are not in the purview of USF programs: a school groundskeeper accidentally cutting fiber is not something that the Commission can easily account for–nor should it. However, with respect to cybersecurity risks, *the service being provided is also the vector by which schools, libraries, and hospitals can be targeted*. This represents a different paradigm and requires that Congress also consider how resilience measures *within subscribers' networks* can be incorporated into these two programs.

Consider ransomware. In a conventional ransomware incident, cyber criminals, leveraging Internet connectivity, deploy malicious agents that lock users out of their data—and potentially out of their computers altogether. This directly affects schools, libraries, and hospitals' ability to access advanced telecommunications services. It is also a threat that *only exists* due to these advanced telecommunications services. However, the mitigations for these risks are often not part of a broadband package. The Commission has already recognized this in enabling universal service funds to be used for "basic firewalls," but that technology is woefully insufficient in the face of even run-of-the-mill cyber criminals today. Congress should evaluate access to services holistically in a way that encompasses risks to access brought about by connectivity.

Finally, with respect to 254(b)(7), Congress should explicitly factor in the harms caused by cyber incidents as integral to the public interest. When students' personal data are compromised in breaches, they suffer, whether directly through identity fraud or indirectly through a lifelong loss of privacy. Similarly, patient care suffers when hospital systems are shut down due to cyber incidents. Protecting the confidentiality, integrity, and availability of school, library, and rural hospital networks is unquestionably in the public interest, and, in keeping with the statutory goals of the E-Rate and Rural Healthcare programs, Congress should evaluate them with respect to the supports they provide for participants' cybersecurity.

2. **How well has each USF program fulfilled Section 254 of the Communications Act of 1996?**

With respect to cybersecurity, neither the E-Rate Program nor the Rural Health Care Program have fully fulfilled the goals of Section 254 of the Communications Act of 1996.

<u>E-Rate</u>

For E-Rate, Category Two does include basic firewalls on the eligible services list. As described by the Commission, basic firewalls are installed on the edge of a school or library's local area network (LAN) and limit the types of incoming and outgoing connections that can be made from the LAN to the broader Internet. Basic firewalls are an essential element of cybersecurity; however, they are far from sufficient, and they protect against only the most unsophisticated of intrusions.

Today, most enterprises use a range of network, endpoint, and cloud technologies and services to protect themselves from cyber criminals.[1]

- **Network** - Network defenses include basic firewalls, but they also include next-generation or web-application firewalls, which provide stateful protections against intrusions targeting the most common ports used in day-to-day web interactions. Network cybersecurity services also include virtual private networks, which authenticate remote access, and internal firewalls, which help segment different portions of a network and enable defense in depth.
- **Endpoint** - Endpoint tools include software like endpoint detection and response agents, which can monitor processes for suspicious activity. They also include backup services, which can protect against data lockup from ransomware; patch management tools, which can ensure that systems are updated with the latest software; and even encrypted communications platforms, which protect the confidentiality of sensitive data.
- **Cloud** - Increasingly, enterprises rely on cloud services to complement and enhance their cybersecurity. Common examples include distributed denial of service (DDoS) protection services, which protect against floods of unwanted network traffic, and protective domain name service offerings, which block connections to suspicious or known-malicious web addresses.

Enterprises also rely on tools like security incident event managers to collect and present data from other sensors and services. Schools and libraries are also chronically understaffed with cybersecurity professionals who can configure security tools, review logs, and take steps to remediate vulnerabilities.

Recognizing the insufficiency of basic firewalls to combat modern cyber threats, the Commission authorized a Cybersecurity Pilot Program in June 2024. 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.[2] 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

[1] NIST Special Publication 800-215 provides a more detailed treatment of different types of security technologies: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-215.pdf.
[2] The expansive list includes a wide array of network, endpoint, and cloud technologies: https://www.fcc.gov/cybersecurity-pilot/cybersecurity-pilot-eligible-services-list.

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.

The pilot represents an important step forward for the Commission in addressing cybersecurity deficiencies within the E-Rate program. The application process has already demonstrated *significant* demand for expanded cybersecurity offerings through E-Rate; in that sense, it should already be deemed a success. However, as discussed in the response to question 9, the pilot should be dramatically expanded if it is to transition to a program of record, and there are other steps that Congress and the Commission should consider to ensure E-Rate achieves its mission with respect to cybersecurity.

Rural Health Care Program

The Rural Health Care Program also allows for limited cybersecurity services, including firewalls. However, since 2013, the program—which has disbursed more than $4 billion—has provided reimbursements for only $8.24 million worth of firewalls (roughly 0.02 percent of the total allocation). Despite the consistent targeting of health care facilities by cyber criminals,[3] the Commission has not engaged in rulemaking or program changes to more directly encompass cybersecurity tools or services as eligible (or encouraged) expenses. As a result, the Rural Health Care Program is also failing to achieve its mission with respect to cybersecurity.

3. **Has the FCC adequately assessed each USF program against consistent metrics for performance and advancement of universal service?**

No response.

4. **What reforms within the four existing USF programs would most improve their:**
    a. **Transparency;**
    b. **Accountability;**
    c. **Cost-effectiveness;**
    d. **Administration; and**
    e. **Role supporting universal service?**

We have no comments with respect to the transparency, accountability, or administration of the USF programs.

With respect to the cost-effectiveness and role supporting universal service of the E-Rate and Rural Health Care Programs, we urge Congress to update both programs to explicitly include cybersecurity as a goal and to provide guidance to the Commission as to how to achieve that goal. We wrote about the role of cybersecurity in supporting universal service in our answer to question 1, and we have more details about different approaches Congress could take to reform

[3] See https://www.ibm.com/think/insights/when-ransomware-kills-attacks-on-healthcare-facilities.

in our answer to question 9. Here, we briefly address the cost effectiveness of cybersecurity improvements in the context of universal service.

Cyber incidents in schools, libraries, and hospitals can be incredibly expensive, with full remediation at times costing tens of millions of dollars.[4,5] As noted in the response to question 1, these incidents are almost universally *enabled* by access to the Internet. When local education agencies or non-profit hospitals have to pay for recovery from cyber incidents, their service delivery suffers--including the very services that universal service funded connectivity is intended to support. Destructive ransomware attacks can also cause victims to need to replace system architecture, including routers and other internal network devices reimbursed by the Rural Health Care Program and under E-Rate Category Two. In other words, when criminals exploit a school or hospital's poor cybersecurity posture, the aftermath can wipe out investments made using universal service funds—hardly cost-effective.

Congress should also consider the indirect cost savings that can accrue from a better cybersecurity posture. Investments in cybersecurity can reduce insurance premiums--or make an entity insurable in the first place—saving education agencies and healthcare providers money they can put into their core programming. They can also improve resilience, reducing the impact of cyber incidents that do happen. In conducting any cost-benefit analyses related to cybersecurity investments, the Commission should also consider the harms avoided to patients and students, whether due to loss of privacy or poorer educational or health outcomes. While these are not core goals of the USF, they are real benefits for the public interest and should be factored into policymaking. As noted in our answer to question 7, the Commission would do well to coordinate with Sector Risk Management Agencies (SRMAs) on how investments in cybersecurity with universal service funds fit into broader sector risk management planning. Congress may also wish to consider allowing for joint programs across agencies, such as the Department of Health and Human Services, that leverage the USF funding distribution mechanism with alternative funding sources (e.g., appropriated funds or entitlement programs) to achieve broader cybersecurity goals that are nonetheless grounded in ensuring universal access.

5. **What reforms would ensure that the USF contribution factor is sufficient to preserve universal service?**

No response.

6. **What reforms would reduce waste, fraud, and abuse in each of the four USF programs?**

[4] See https://www.k12dive.com/news/school-ransomware-attacks-cybersecurity-funding/730333/, noting the mean cost to a district to restore from backups was $3.76 million and the median ransom payment was $7.5 million.
[5] See https://insurica.com/blog/uvm-health-network-ransomware-attack/.

We have no comments with respect to reforms that would reduce fraud and abuse within USF programs. Regarding waste—and with respect to the E-Rate and Rural Health Care Programs—we note that our answer to question 4 addresses the cost of cybersecurity incidents. By taking steps to better protect schools, libraries, and health care facilities, the Commission will reduce waste in the form of subsidies for services that are unable to be realized due to outages caused by cyber incidents.

7. **What actions would improve coordination and efficiency among USF programs and other FCC programs, as well as broadband programs housed at other federal agencies?**

In its order creating the K-12 Cybersecurity Pilot, the Commission noted its reliance on the expertise of the Cybersecurity and Infrastructure Security Agency (CISA) in developing the program. This kind of interagency collaboration will be essential to the more thorough integration of cybersecurity into USF programming. Congress should ensure that, as part of USF Reform, the Commission continues to engage with:

- CISA - In its role as National Coordinator for Critical Infrastructure Risk and Resilience, CISA helps lead the whole-of-nation effort to reduce risk to our critical infrastructure from all hazards, including cyber threats. CISA's technical expertise and reach into states are key resources the Commission should draw upon in developing cybersecurity requirements and service eligibility lists for USF programs.
- SRMAs - As codified in Section 9002 of the Fiscal Year 2021 National Defense Authorization Act, each Sector Risk Management Agency is responsible for assessing sector risk and supporting sector risk management within its particular critical infrastructure sector. Schools and libraries are part of the Government Facilities and Services Sector, and rural health care facilities are part of the Healthcare and Public Health Sector. The Commission should coordinate with the SRMAs (CISA and GSA for E-Rate and the Department of Health and Human Services for the Rural Health Care Program) as well as the Department of Education, which serves as the SRMA for the Education Sub-sector of the Government Services and Facilities Sector. As part of its work, the Commission should consider how cybersecurity and resilience awards fit into broader, whole-of-government plans, and SRMAs are the key locus for ensuring such coordination takes place.
- NIST - The National Institute for Standards and Technology provides guidance for Federal agencies and private sector partners regarding cybersecurity risk management. The Commission should consider how to use tools like the Cybersecurity Framework to help schools, libraries, and health care facilities assess and manage their risk. To the greatest extent practical, Congress should also require that the Commission use common terminology defined by NIST for cybersecurity tools and services.
- ONCD - The White House Office of the National Cyber Director coordinates national cybersecurity policy, strategy, and implementation on behalf of the President. By working closely with ONCD, the Commission will have a clear understanding of how its

cybersecurity efforts fit into the national strategy, and Congress can be assured that resource allocations are being made cognizant of other programs intended to improve the nation's cybersecurity posture.

Several other agencies have roles and responsibilities for cybersecurity, including the Federal Bureau of Investigation, the National Security Agency, and the National Telecommunications and Information Agency. Congress should encourage the Commission to consult with such agencies as appropriate but should not require engagement.

8. **For any recommendations on reforms, does the Commission currently have the feasibility and authority to make such changes?**

Under Section 254(c)(3), the Commission has the authority to designate "additional services" for the support of schools, libraries, and rural health care providers. Between this authority and the broad authority under Section 254(c)(1)(D) to consider the extent to which services are "consistent with the public interest", the Commission can—and has, through the K-12 cybersecurity pilot—authorized specific funding for cybersecurity tools and services.

However, we strongly urge Congress to *codify* cybersecurity as a specific goal for universal service funds flowing to schools, libraries, and hospitals as part of USF Reform activities. While the Commission does possess the authority to subsidize cybersecurity—and while, as noted in the answer to question 1, *supra*, the Communications Act of 1996 should be read to incorporate mitigation of cybersecurity risk—it is unclear whether the Commission will exercise this authority absent action from Congress.

In particular, while the cybersecurity pilot is proving successful, it is wildly insufficient given demonstrated need. Schools and libraries identified $3.7 billion in necessary support as part of their applications for the three-year pilot (which is likely significantly under actual need, given the Commission's stated limitations on the scale of the program and the limited number of eligible entities that applied), yet the pilot only provided $200 million. The Rural Healthcare Program has not even run such a pilot.

What's more, in the order creating the K-12 cybersecurity pilot, two Commissioners dissented, noting that, despite the importance of cybersecurity, they had concerns that the pilot might go beyond the Commission's mandate to provide additional services (or enhanced services under Section 254(h)(2)). While we believe that the authority clearly exists today, Congressional clarity on this point would remove any ambiguity and allow legislators to guide and scope the Commission's approach to cybersecurity in the context of universal service.

Based on a policy memo published by IST in July 2025, we offer the following suggestions for approaches Congress could take to positively codify cybersecurity into the E-Rate and Rural Healthcare programs.

Codify the Pilot

Policymakers could codify the cybersecurity pilot, transitioning it into a full USF program.[6] The unmet need for cybersecurity services is significant, and the pilot has existing infrastructure that could easily transition to a permanent program. 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 the Commission does not ignore cybersecurity entirely, a challenge that has been observed in the context of other Federal grant programs, such as FEMA's Homeland Security Grant Program.

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 need to provide a mechanism to adjust the list as technology evolves. This approach would ensure educational entities remain the primary decisionmakers, as they may 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 Commission 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 organizations use approximately 10 percent of IT spending for security.[7] Congress could consider a similar target and leave it up to the Commission to design programs to implement it and evaluation metrics to measure impact. This approach provides maximal flexibility to evolve over time while still offering clear direction from Congress to the Commissioners on the importance of cybersecurity.

---

[6] 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.

[7] "New Research from IANS and Artico Search Reveals Cybersecurity Budgets Increased Just 6% for 2022-2023 Cycle," press release, IANS, September 26, 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.

Additional Considerations

Combining Approaches

These approaches 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.

Healthcare

Many of the community institutions supported by the Rural Health Care Program are vulnerable to cyber intrusions, and healthcare organizations have also been increasingly targeted by cyber criminals.[8] 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.

9. **Is the USF administrator, the Universal Service Administrative Company (USAC), sufficiently accountable and transparent? Is USAC's role in need of reform?**

No response.

10. **Additional Comments**

About the authors:

Nicholas Leiserson is the Senior Vice President for Policy at the Institute for Security and Technology (IST). A legislative strategist and technologist, he has spent 15 years addressing cybersecurity risk and resilience and managing multidisciplinary teams of senior professionals at the White House and on Capitol Hill. He was integral in the creation of the Office of the National Cyber Director (ONCD) and served as one of its first employees where he built the infrastructure for an office that grew to over 80 people in two years.

Leiserson previously served as the Assistant National Cyber Director for Cyber Policy and Programs at ONCD. In this role, Leiserson led ONCD's national cybersecurity policy development, including critical infrastructure protection, regulatory harmonization, cyber insurance, and software liability. He earlier served as ONCD's Deputy Chief of Staff. Prior to joining ONCD,

[8] https://www.fiercehealthcare.com/health-tech/healthcare-remains-top-target-cybercriminals-uptick-hacking-attacks-2024.

Leiserson spent more than a decade on the staff of former Congressman James R. Langevin (RI-02) in various roles, most recently as his Chief of Staff.

Michael Klein is Senior Director for Preparedness and Response at IST, where he focuses on improving the resilience of "target rich, cyber poor" critical infrastructure sectors. He comes to the role with nearly 20 years of experience across K-12 education as a teacher, coach, consultant, and district leader as well as federal cyber policy.

Most recently, as the US Department of Education's (ED) Senior Advisor for Cybersecurity, Michael led ED's K-12 cybersecurity work with the National Security Council, Office of the National Cyber Director, CISA, FBI, the Intelligence Community, as well as State, Local, Tribal, and Territorial (SLTT) partners, and the private sector.

Prior to his federal service, Michael was a school district IT Director during the COVID-19 pandemic, where he led a team supporting 2500 students and 550 staff as they navigated in-person, hybrid, and remote learning safely and securely. Michael has also led coaching for a team of educational consultants, helped grow 2 edtech startups, taught elementary school in Brooklyn and Harlem, and served as a founding teacher at a High Tech High school just south of San Diego.

About IST:

Technology has the potential to unlock greater knowledge, enhance our collective capabilities, and create new opportunities for growth and innovation. However, insecure, negligent, or exploitative technological advancements can threaten global security and stability. Anticipating these issues and guiding the development of trustworthy technology is essential to preserve what we all value.

The Institute for Security and Technology (IST), the 501(c)(3) critical action think tank, stands at the forefront of this imperative, uniting policymakers, technology experts, and industry leaders to identify and translate discourse into impact. We take collaborative action to advance national security and global stability through technology built on trust, guiding businesses and governments with hands-on expertise, in-depth analysis, and a global network.