STRATEGY GUIDE

TriVigil

WE PROTECT EDUCATION

CYBERSECURITY SOLUTIONS ARE NOW ELIGIBLE FOR E-RATE

HERE'S HOW TO USE THE NEW FUNDS TO SECURE YOUR DISTRICT.

What is E-Rate, and what is the new Schools and Libraries Cybersecurity Pilot Program?

The **FCC's Universal Service Program for Schools and Libraries**, commonly called E-Rate, is a federal initiative that helps schools and libraries in the U.S. obtain affordable broadband and telecommunications services. Historically, it has focused on providing funding for internet access and network infrastructure.

In 2024, the FCC launched a new **Schools and Libraries Cybersecurity Pilot Program** aimed at bolstering cybersecurity for K-12 schools and libraries. This pilot program provides $200 million over three years, with $100 million available in the first year. The funds are intended to help schools and libraries strengthen their cybersecurity defenses, including firewalls, network monitoring, and incident response systems.

This initiative marks a significant expansion of the E-Rate program to address the growing cybersecurity needs of schools and districts, ensuring they can protect sensitive data and maintain secure digital learning environments.

What is eligible for these new funds?

The **Cybersecurity Pilot Program** has designated four specific categories of eligibility to guide schools and libraries in securing funding for various types of cybersecurity services and equipment:

1. **Advanced/Next–Generation Firewalls**
   Equipment and services that implement advanced/next–generation firewalls, including software–defined firewalls and Firewall as a Service, are eligible. Specifically, equipment, services, or a combination of equipment and services that limit access between networks—excluding basic firewalls already funded through the E–Rate program—are eligible.

2. **Endpoint Protection**
   Equipment and services that implement endpoint protection are eligible. Specifically, equipment, services, or a combination of equipment and services that implement safeguards to protect devices owned by schools, libraries or end users—including desktops, laptops, and mobile devices—against cyber threats and attacks are eligible.

3. **Identity Protection and Authentication**
   Equipment and services that implement identity protection and authentication are eligible. Specifically, equipment, services, or a combination of equipment and services that implement safeguards to protect a user's network identity from theft or misuse, and/or provide assurance about the network identity of an entity interacting with a system are eligible.

4. **Monitoring, Detection, and Response**
   Equipment and services that implement monitoring, detection and response are eligible. Specifically, equipment, services, or a combination of equipment and services that monitor and/or detect threats to a network and that take responsive action to remediate or otherwise address those threats are eligible.

What are the steps in the process of applying for funds, and what are the deadlines?

1. **September 17, 2024:** Start of Filing Window
   This is the date when schools and libraries can begin submitting their applications for the Cybersecurity Pilot Program. Applicants will need to ensure they are prepared to meet the program's requirements and gather necessary documentation for eligibility.

2. **November 1, 2024:** Closing of Filing Window
   The filing window for the Cybersecurity Pilot Program will close on this date. Schools and libraries must submit FCC Form 471 by this deadline to be considered for funding under the program. Form 470 should be filed at least 28 days prior to this to allow time for service providers to bid.

3. **Form 470 Deadline:** Mid–October 2024 (Exact Date TBD)
   To ensure compliance with the 28–day competitive bidding process, schools and libraries must file FCC Form 470 no later than mid–October 2024 (the exact date depends on when institutions wish to file their Form 471). This form allows service providers to submit bids for eligible services.

4. **Funding Commitment Decision Letters (FCDL):** Early 2025
   After the filing window closes, the FCC will review applications and issue Funding Commitment Decision Letters (FCDLs), likely in early 2025. This will notify applicants whether they have been approved for funding.

5. **Implementation Deadline:** June 30, 2026
   Approved cybersecurity solutions must be implemented by June 30, 2026. Schools and libraries will need to deploy the funded solutions within this timeframe to remain compliant with the program's requirements.

How can TriVigil help?

It is critical for any school district to hire a trusted partner to guide them through this process, to quickly assess current needs and provide a comprehensive plan for improvement.

Trivigil Inc. is a premier cybersecurity firm with a specialized focus on education, providing technical expertise, risk assessment, policy development, security training, ongoing monitoring and support to school districts.

Trivigil is an approved FCC E–Rate and USAC partner and offers services and solutions in all four cybersecurity pilot categories: Monitoring, Detection, and Response, Endpoint Protection, Identity Protection and Authentication, and Advanced/Next–Gen Firewalls.

In addition, Trivigil's Quick Start program is perfectly designed to help school systems identify needs, and apply for the new E–Rate cybersecurity funding. In just 4 hours, TriVigil can deliver a detailed roadmap based on NIST 800 standards, giving you clear insights into your district's current needs and providing actionable steps to close any gaps.

"This exciting initiative holds the potential to significantly bridge the digital divide—especially for underserved communities—while enhancing access to critical communication infrastructures," says Avni Trivedi, founder and CEO of TriVigil.

"At Trivigil, we understand the complexities involved in such large–scale projects. Our team is here to provide expert guidance, cybersecurity solutions, and a clear roadmap to help you effectively secure, manage, and implement these funds. Together, we can ensure that this pilot program leads to meaningful change—strengthening our networks, safeguarding data, and ensuring equitable access for all. Let's embrace this opportunity to lead with innovation and security."

To learn more, go to: www.trivigil.com/e–rate–program