Cybersecurity Pilot Program Eligible Services List

Equipment and services that constitute a protection designed to improve or enhance the cybersecurity of a K-12 school, library, or consortia are eligible. A non-exhaustive list of four eligible technological categories and, for each category, a non-exhaustive list of eligible equipment and services, follows.

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 limits access between networks, excluding basic firewalls that are funded through the Commission's E-Rate program, are eligible.

Eligible equipment and services may include the following features, substantially similar features, or their equivalents:

- Advanced Threat Detection and Prevention
- AI/ML Threat Detection and Response
- Application Awareness & Control
- Cloud-Delivered Threat Intelligence
- Comprehensive Network Visibility Software-defined Firewalls
- Deep Packet Inspection (DPI)
- Distributed-Denial-of-Service (DDoS) Protection
- Firewall as a Service (FWaaS)
- Integrated Intrusion Prevention Systems (IPS)
- Internet of Things (IoT) Security
- Intrusion Prevention/Detection
- Malware Detection
- Network Segmentation
- Patch Management Systems
- VPN

Endpoint Protection

Equipment and services that implement endpoint protection are eligible. Specifically, equipment, services, or a combination of equipment and services that implements safeguards to protect school- and library-owned end-user devices, including desktops, laptops, and mobile devices, against cyber threats and attacks are eligible.

Eligible equipment and services may include the following features, substantially similar features or their equivalents:

- Anti-Malware
- Anti-Ransomware
- Anti-Spam
- Anti-Virus
- Endpoint Detection & Response (EDR)
- Extended Detection & Response (XDR)
- Insider and Privilege Misuse
- Privileged Access Management
- Secure Sockets Layer (SSL) Inspections
- Target Intrusions
- Web Application Hacking

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 implements 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.

Eligible equipment and services may include the following features, substantially similar features, or their equivalents:

- Active Countermeasure Tools
- Cloud Application Protection
- Cloud Services
- Credential Stuffing
- Content Blocking and Filtering/URL Filtering
- Content Caching Systems and Service
- Customer Portal Services
- Digital Identity Tools
- Distributed-Denial-of-Service (DDoS) Protection
- DNS/DNS-Layer Security, Blocking, and Filtering
- Email and Web Security
- Identity Governance & Technologies
- Intrusion Detection Systems (IDS)
- Logging Practices / Event Logging
- Network Access Control
- Offsite/Immutable back-ups
- MFA/Phishing-Resistant MFA

- Patching
- Password Spraying
- Privileged Identity Management
- Products with TPM Chips
- Secure Access Service Edge (SASE)
- Secure-By-Design Equipment and Services
- Security Information and Event Management (SIEM)
- Security Updates
- Single Sign-On (SSO)
- Trusted Platform Module (TPM)
- Web Content Controls
- Wireless Access Controllers
- Zero Trust Architecture

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 is eligible.

Eligible equipment and services may include the following features, substantially similar features, or their equivalents:

- Advanced Attack Surface Management and Asset Management Solutions
- Bug Bounty Solutions & Services
- Compliance Assessment
- Dark Web Scanning
- Data Loss Prevention
- Internal/External Vulnerability Scanning
- Network/Device Monitoring & Response
- Network Security Audit
- Network Traffic Analysis
- Managed Detection & Response (MDR)
- Managed Service Providers
- Maturity Models
- Network Detection Response (NDR)
- Penetration Testing
- Security Operations Center (SOC) for Around the Clock (24/7/365) Monitoring, Detection, and Response
- Threat Hunting/Updates and Threat Intelligence
- Vulnerability Management

Notes:

- Certain technologies (e.g., DDoS protection) are listed in multiple categories above, reflecting the multiple ways they are categorized in the marketplace.
- Eligible costs include maintenance, operation and support charges, monthly charges, special construction, installation and activation charges, software, modulating electronics, and other equipment necessary to make eligible equipment and services functional. All eligible equipment and services and related costs, including maintenance and operation, must be competitively bid.
- A manufacturer's multi-year warranty for a period up to three years that is provided as an integral part of an eligible component, without a separately identifiable cost, may be included in the cost of the component.
- Eligibility is limited to equipment that is network-based (i.e., that excludes end-user devices, including, for example, tablets, smartphones, and laptops) and services that are network-based and/or locally installed on end-user devices, where the devices are owned or leased by the school or library, and where equipment and services are designed to identify and/or remediate threats that could otherwise directly impair or disrupt a school's or library's network, including to threats from users accessing the network remotely.
- Ineligible costs include:
    - Any equipment, service, or other related cost that is eligible in the Commission's E-Rate eligible services list program in the funding year for which Pilot reimbursement is sought.
    - Any equipment, service, or other related cost for which a participant has already received reimbursement, or plans to apply for reimbursement, through any other USF or federal, state, or local program in the funding year for which Pilot reimbursement is sought.
    - Staff salaries and labor costs for personnel of the participant or underlying beneficiary are not eligible.
    - Consulting services that are not related to the installation and configuration of the eligible equipment and services are not eligible. These include services related to application assistance, Program advice, and other activities not tied directly to actual installation and initial configuration of eligible equipment and services.
    - Long-term planning and risk assessment surveys, including threat intelligence analysis and costs associated with incident response plans
    - Security cameras, asset tracking tags, insurance costs, threat responses exercises, training, and any costs associated with responding to specific ransom demands are ineligible.
    - Any equipment or services prohibited by the Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609) (Secure Networks Act) or the Commission's rules, including Commission rules 54.9 and 54.10, that implement the Secure Networks Act.

Training

Training is eligible as a part of installation of the equipment and services only if it is basic instruction on the use of eligible equipment and services, directly associated with equipment and services installation, and is part of the contract or agreement for the equipment and services. Training must occur coincidently or within a reasonable time after installation.