Schools and Libraries Cybersecurity Pilot Program

Department of Education

Overview

The FCC's Schools and Libraries Cybersecurity Pilot Program (CPP) is a three-year pilot funded through the Universal Service Fund (USF) that provides up to **$200 million** to help eligible K–12 schools, libraries, and consortia pay for advanced cybersecurity services and equipment that protect their broadband networks and data. The Pilot is designed to gather real-world cost and effectiveness data to inform whether (and how) USF support could be used for school and library cybersecurity longer term. CPP uses fixed, pre-discount budgets and requires participants to cover a non-discount share (similar to E-Rate). For schools and districts, the annual pre-discount budget is typically **$13.60** per student, with a **$15,000** minimum floor and a **$1.5M** maximum cap. For libraries and library systems, the annual pre-discount budget is **$15,000** per library/site (up to 11 sites), with larger systems capped at up to **$175,000** annually. In the most recent cycle, the Pilot participation application (FCC Form 484 Part 1) ran **Sept 17–Nov 1, 2024**, selected participants were announced **Jan 16, 2025**, and the funding request window (Pilot FCC Form 471) was **Mar 18–Sept 15, 2025.**

CPP Eligible Cybersecurity Solution Areas:

Pillar Priority	Directive	Impact
Pillar I: Advanced / Next-Gen Firewalls	Deploy NGFW/FWaaS and related protections (e.g., IPS, segmentation, DDoS protection) to harden the network edge.	Drives demand enterprise-grade perimeter security, modern firewall services, and implementation support.
Pillar II: Endpoint Protection	Protect school/library-owned devices with EDR/XDR, anti-malware/anti-ransomware, and endpoint safeguards.	Expands adoption of managed endpoint security and incident containment capabilities.
Pillar III: Identify Protection & Authentication	Strengthen identity controls like MFA/phishing-resistant MFA, SSO, PAM, Zero Trust-aligned tools, and identity governance.	Increases demand for identity-first security and access control modernization.
Pillar IV: Monitoring Detection & Response	Implement MDR/SOC services, NDR, vuln scanning/management, threat hunting, and continuous monitoring.	Accelerates purchasing of 24/7 monitoring + response services and operational security tooling.
Pillar V: Compliance + Program Integrity	Follow competitive bidding, document retention, and required certifications; CIPA obligations can be triggered by CPP-supported purchases.	Pushes participants toward procurement-ready, compliant implementations with clear documentation and governance.

carahsoft.
TECHNOLOGY BY POLICY

Timeline: KEY DATES AND MILESTONES

SEPTEMBER 17 – NOVEMBER 1, 2024

FCC opens the CPP application window (**FCC Form 484 Part 1**) for eligible schools, libraries, and consortia.

JANUARY 16, 2025

FCC announces selected **CPP participants**, enabling applications to proceed toward procurement and funding requests.

MARCH 18 – SEPTEMBER 15, 2025

Selected participants submit **Pilot FCC Form 471** funding requests during the CPP funding request window.

What Does This Mean for Vendors?

For cybersecurity vendors and service providers, the **Schools and Libraries Cybersecurity Pilot Program (CPP)** is a clear signal that **K–12 schools and libraries are actively funding "next-level" security** beyond basic tools—using a structured, compliance-driven program that rewards measurable protection and well-documented implementation.

Key take aways for vendors:

- CPP creates near-term, funded demand for eligible cybersecurity categories (advanced firewalls, endpoint protection, identity protection, monitoring/detection/response), plus implementation services tied to making those solutions operational.
- Procurement and documentation matter as much as the product. Winners will be vendors that can support competitive bidding requirements, clear scoping, and clean paperwork (line items, eligibility alignment, invoicing readiness).
- Schools and libraries will favor "deployable + supportable" solutions platforms that integrate with existing environments, can be implemented quickly, and include ongoing management/response options (MDR/SOC-style support is especially attractive for resource-limited IT teams).
- Bundled offerings win. Vendors that pair tools with the services needed to deploy, configure, and maintain them (and help customers stay compliant through invoicing and change requests) will be best positioned.

In short, CPP is a buying signal for multi-year cybersecurity modernization in K–12 and libraries. Vendors that align to eligible CPP categories, bring implementation + operational support, and help applicants stay compliant will be best positioned to win and expand.

Contact Us:

Email: Research@carahsoft.com

See more from the Carahsoft Team:
To explore our catalog of federal, state, and local technology policies, executive orders, and directives shaping public sector modernization scan this QR code.