C1 GOVERNMENT SOLUTIONS

Cybersecurity Protection for K-12 Schools & Libraries

Protect your future with C1: Your trusted partner for the FCC Cybersecurity Pilot Program

The FCC Cybersecurity Pilot Program is an initiative by the Federal Communications Commission (FCC) aimed at enhancing the cybersecurity posture of K-12 schools and libraries across the United States. It is part of a broader effort to protect critical educational infrastructure from increasing cyber threats, such as ransomware attacks, data breaches, and other malicious activities targeting the educational sector.

The purpose of the three-year, $200 million pilot is to provide foundational cybersecurity protection for institutions with minimal current security measures. This C1 solution is designed to help schools and libraries optimize their cybersecurity spending by prioritizing solutions that address the most significant gaps in their cybersecurity posture. It helps these institutions achieve the minimum acceptable baseline security goals as established by CISA, increasing the likelihood of receiving funding from the FCC Cybersecurity Fund pilot program.

Key objectives

Strengthen cybersecurity protection: Provide schools and libraries with the necessary resources and guidance to improve their cybersecurity defenses.

Funding allocation: Distribute financial support to high-risk institutions to implement and upgrade cybersecurity measures.

Achieve baseline security goals: Ensure that participating institutions achieve a minimum acceptable level of cybersecurity, aligned with guidelines from agencies such as the Cybersecurity and Infrastructure Security Agency (CISA).

Conduct comprehensive assessments: Conduct thorough assessments to identify vulnerabilities and gaps in existing cybersecurity frameworks.

Capacity building: Enhance the overall capacity of educational institutions to prevent, detect, respond to, and recover from cyber incidents.

The C1 advantage: Assessment. Detection. Response. Recovery.

C1's Cybersecurity Protection for K-12 Schools and Libraries solution addresses the needs of these institutions regardless of their cybersecurity maturity level and provides straightforward ways to help implement the baseline security standards established by CISA. By strengthening their cybersecurity protection, their ability to prevent, detect, respond to, and recover from cyber incidents is enhanced.

Protection for all

C1 will maximize the cybersecurity of your educational institution by targeting the FCC's $200 million Cybersecurity Funding pilot program designed to support high-risk schools and libraries, including those in urban, rural, large, small, or Tribal environments.

Expert guidance

C1 will help navigate the FCC application process to maximize your chances of program selection. A large number of schools and educational partners have trusted C1 for their E-Rate funding process.

Proven track record

C1 will leverage their extensive experience with federal, state, and local programs such as E-Rate to assist in solution identification and delivery. C1's strong security experience provides strong synergies with our industry leading Communications and Infrastructure Experience solutions.

Unparalleled risk assessments

C1 provides a comprehensive security risk assessment that aligns closely with CISA recommendations. For more mature institutions, the CISA CPG framework and the NIST CSF are leveraged to identify potential gaps and improve your cybersecurity posture.

Tailored cybersecurity solutions

C1's robust portfolio of best-in-class SX (Security Experience) solutions are tailored to safeguard the unique cybersecurity needs of K-12 schools and libraries. Our unmatched partner ecosystem ensures that we always provide best-in-class solutions to our customers.

Scalable solutions

C1 provides scalable solutions to meet the unique needs of small schools through large districts at all cybersecurity maturity levels.

Reduced costs

The increasing cost of cyber insurance is significantly impacting K-12 schools and libraries' ability to manage the financial risks associated with a cyber-incident. Given the financial burden this places on these institutions, these funds can be better allocated towards detection, prevention, and recovery from cyber-attacks.

Tailored to your specific needs

Cybersecurity Protection for K-12 Schools and Libraries - Basic

- **Penetration Test, Vulnerability Scan** – C1 (CISA has basic Penetration Testing Service – wait times very long)

- **Security Risk Assessment** – C1 (input for incident response plan)

    - Complimentary nationally recognized Cybersecurity security assessment for Education

- **MDR Service** – Arctic Wolf

- **Integrate existing platforms to unified environment**; email security (#1 vector for bad actors)

- **Email Security** – Proof Point, Microsoft (Educational Favorable SKUs), Cisco

- **Cybersecurity Awareness Training** – C1 provides a comprehensive security awareness training that aligns closely with CISA recommendations through Arctic Wolf or CISA's training for higher education

Cybersecurity Protection for K-12 Schools and Libraries - Advanced

- **Basic Solutions** plus:

- **Cyber Recovery Solution** – Dell/Cisco

- **Multi-factor Authentication** – Multiple vendors (Cisco Duo; Microsoft 2 Factor Solution)

- **Security Risk Assessment** – C1 leverages the CISA CPG (Cybersecurity Performance Goals) framework and the NIST CSF (Cybersecurity Framework) to identify potential gaps and improve the cybersecurity posture of your organization

Why you should participate

Increasing cyber threats

- Educational institutions are increasingly becoming targets for cyberattacks. The rapid evolution of these attacks are outpacing the defenses and skillsets of even the most prepared educational institutions.
- Cyber threats can disrupt educational operations, compromise sensitive data, and incur significant financial costs.

Financial support

- The program offers crucial funding to schools and libraries that may lack the financial resources to implement robust cybersecurity measures on their own.
- It aims to alleviate the financial burden of cybersecurity enhancements, making it feasible for even the most resource-constrained institutions to protect themselves.

Regulatory compliance

- By participating in the program, schools and libraries can ensure compliance with federal and state cybersecurity regulations and standards, thereby avoiding potential legal and financial repercussions.

Capacity building and awareness

- The program not only provides financial resources but also educates and empowers institutions to maintain and improve their cybersecurity posture.
- Training and awareness initiatives under the program help staff and students understand and implement best practices in cybersecurity.

Protecting educational integrity

- Safeguarding digital infrastructure is critical to maintaining the integrity and continuity of educational services.
- Optimizing cybersecurity helps protect the academic environment, thereby supporting the educational mission and preserving trust in these institutions.

Enhanced preparedness

- Schools and libraries that participate in the program will be better prepared to handle cyber incidents, ensuring quicker recovery and minimizing disruptions to educational activities.

Prepare for the Fall 2025 funding announcement.
Contact C1 to assess your eligibility and develop a winning cybersecurity strategy.

Contact us to learn more.