American Rescue Plan for Education: A Reference Guide

The pandemic and the accelerated digital transformation it caused has created a whole new paradigm for education. Distance- and hybrid-learning are new and completely different delivery systems. In addition, as schools and universities reopen, bringing students, faculty, and staff back to campus, they need to address an influx of devices on their networks.

This third round of funding that is part of the American Rescue Plan Act allows educational institutions to fund IT and security projects that will enable educators to move forward with their missions. Educational institutions need to understand how much funding is available and consider the ways in which it can be used to respond to the rapidly changing paradigm shifts in the delivery of educational services. IT departments have a critical opportunity to secure and shore-up their networks, but they must be proactive.

Funding Sources

K–12 Education

- ESSER 1 ($13.29B) and CARES 2 ($54B)
- American Rescue Plan ($130B)
- ESSER 1—Spend till Sept. 30, 2022
- ESSER 2—Spend till Sept. 30, 2023
- Funding flows via ESEA Title 1 Part A from the SEA to the LEA
- FAQ on Ed.gov
- Find K–12 funding status through round 2 at https://covid-relief-data.ed.gov/

Higher Education

- CARES 1 ($30B) and CARES 2 ($22B)
- American Rescue Plan ($30B)
- HEERF 1 and HEERF 2
- FAQ on Ed.gov
- Find higher education funding status through round 2 at https://covid-relief-data.ed.gov/

For the latest information on COVID relief and funding, please visit your state's Department of Education website, and search for ESSER (K–12) and HEERF (EDU).

Technology Considerations

As a result of the COVID-19 crisis, schools have had to rapidly adapt in-person classes and programs to online modes. This rapid transition has impacted the functionality of school IT networks—while radically expanding the attack surface to potential cyberattacks. Looking forward, schools will need to address the influx of devices when students return to in-person learning.

Schools need to secure the dramatic increase in new connections to their networks and ensure their networks are ready when students, faculty, and staff return to campus. They also have to be nimble as they move forward in preparation for the next outbreak or emergency that could face their region.

We have highlighted key areas where your peers have utilized the funding to address deficits and gaps discovered in the capacity, security, and management of the hybrid and remote learning network.

Hybrid/Remote Learning and Working

- Additional security for remote/virtual private network (VPN) access so as to prevent higher numbers of cyberattacks
- Automated ransomware protection for full detection and remediation
- Additional off-net security for laptops and Chromebooks
- Secure "internet in a box" solutions for teleworking and remote digital learning
- Secure Wi-Fi leading to enhanced VPN tunnel support for teleworking and remote digital learning
- Enhanced security posture with multi-factor authentication solutions for remote users

Website and Internet Security

- Additional security to public and private websites to prevent escalating numbers of attacks
- Prevention of distributed denial-of-service (DDoS) attacks as bad actors use COVID-19 masking to gain entry or deny service access

In-person and Infrastructure Solutions

- Secure unified communications, including Voice over Internet Protocol (VoIP) and softphones for laptops
- Device security automation as well as onboarding for Internet of Things (IoT) and new-user devices, including but not limited to visitor computers, wireless printers, digital learning devices, environmental devices, etc.

Network and Security Monitoring

- Additional visibility into increased number of attacks
- Automated remediation of detected vulnerabilities
- End-to-end network and security integration so as to block high numbers of, or potentially critical, incidents

Fortinet partners with K–12 and higher education institutions to provide unified, cost-effective solutions that secure them across campuses. An integrated approach not only alleviates the strain on lean IT teams but also helps them achieve their ultimate goal—delivering a network that streamlines education while securing students.

To help build your strategy for spending these federal funds, contact SLEDhelp@fortinet.com to set up some time to review how Fortinet can help address these challenges.

May 25, 2021 11:28 PM
1050935-0-0-EN