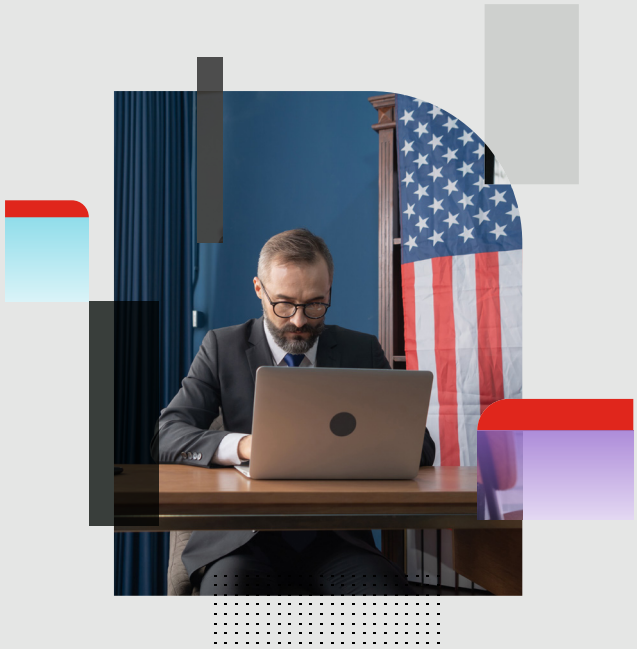
REFERENCE GUIDE

Government and Education Funding: A Reference Guide



Congress has passed three acts for COVID-19 recovery: CARES, CRRSA, and ARP, and have finalized the new infrastructure bill. Poised for possible funding in spring 2022 is the "Build Back Better" funding program. These funds could provide substantial flexibility for each jurisdiction to meet local needs, including support for households, small businesses, impacted industries, essential workers, and the communities hardest hit by the crisis. These funds could also deliver resources that recipients can invest in building, maintaining, or upgrading their water, sewer, and broadband infrastructures. Eligible state, territorial, metropolitan city, county, and Tribal governments may request Coronavirus State and Local Fiscal Recovery Funds through the Treasury Submission Portal. Concurrent with this program launch, the treasury has published an "Interim Final Rule" that implements the provisions of this program.

This round of funding allows governmental agencies to fund IT and security projects that will enable agencies to move forward with their missions. Governmental entities 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 governmental services. IT departments have a critical opportunity to secure and shore up their networks, but they must be proactive.

State, County, Metro, and Smaller City Government

Funding flows via the U.S. Department of the Treasury. Read the fact sheet.

Funding Sources

The U.S. Department of the Treasury

For the latest information on COVID relief and funding, please visit the U.S. Department of the Treasury website.

Get Coronavirus State & Local Fiscal Recovery Funds information.

Get The American Rescue Plan Act Funding information.

The Infrastructure Bill is pending final allocations. Learn more about it here.

Technology Considerations

As a result of the COVID-19 crisis, agencies have had to rapidly change in-person services and programs to remote working and online service modes. This hurried transition has impacted the functionality of agency IT networks—while radically expanding the attack surface to potential cyberattacks. Looking forward, government agencies will need to address the new reality of working from anywhere and the need to expand online services. As well as implementing a comprehensive digital transformation (DX), it is imperative that government at all levels embraces a comprehensive security transformation (SX).

Eligible uses with a technology focus (ARP Funding)

- Technology Contact Tracing
- Technology Related to COVID-19 Vaccinations and Sites
- Establishing and Operating Telemedicine Capabilities
- Establishing or Enhancing Public Health Data Systems
- Health and Public Health Program Data and Technology Infrastructure
- Data and Technology Infrastructure To Improve Programs Addressing Negative Economic Impacts
- Government Services to the Extent of Revenue Reduction
- Roads, Health Services, Environmental Remediation, School or Educational Services, Cybersecurity (including hardware and software), Public Safety Services
- Cybersecurity for Water, Sewer, & Broadband Infrastructure
- Broadband Infrastructure

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 hybrid, remote networks.

Hybrid/Remote Working

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

Website and Internet Security

- Provide additional security to public and private websites to prevent escalating numbers of attacks
- Prevent denial-of-service (DoS) attacks as bad actors use COVID-19 masking to gain entry or deny service access

In-person and Infrastructure Solutions

- Secure unified communications (UC), including Voice over Internet Protocol (VoIP) and softphones for laptops
- Automated device security as well as onboarding for Internet of Things (IoT) and new user devices, including 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 critical incidents

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.

January 28, 2022 3:03 AM
1429451-0-0-EN