



# Maximizing ARP Funding to Strengthen IT Security and Performance in K-20 Schools

**Ransomware and distributed denial-of-service (DDoS) attacks** have become more common over the past two years as schools across the country shifted to remote learning. Attackers launched nearly 80 million assaults targeting educational institutions in the first half of 2021 alone, according to data from NetScout, a leading cybersecurity, application, and network performance management provider.<sup>1</sup>

As K-12 schools and higher education institutions have entered their third school year disrupted by the pandemic, security considerations remain a top concern. In addition, other challenges – including bandwidth bottlenecks, poor application performance in data centers, and issues with the end-user experience on third-party videoconferencing and digital collaboration platforms – will continue to impact the quality of teacher-to-student communications, as well as administrative meetings and collaboration.

Whether a school is conducting in-person instruction or hybrid learning, every education institution must take steps to ensure its learning environment is accessible, secure and resilient.

With the most recent round of federal funding through the American Rescue Plan (ARP), schools have an opportunity to make impactful long-term investments in broadband, cybersecurity and connectivity. ARP has made more than \$162 billion

in supplemental funding available for the Elementary and Secondary School Emergency Relief Fund (ESSER) and the Higher Education Emergency Relief Fund (HEERF), along with an additional \$7 billion in new aid through the Emergency Connectivity Fund (ECF).

Federal guidance is extremely broad, but many of these funding streams can be used to strengthen schools' security and availability posture (Congress actually has asked the Education Department to make it explicitly clear that schools can, in fact, use the latest round of funding to increase their resilience).<sup>2</sup> Depending on the funding stream, schools will have until either Sept. 30, 2023, or Dec. 31, 2024, to use federal aid to cover eligible technology-related expenses.

This brief provides an overview of currently available funding, allowable uses and important deadlines, and explains how schools can potentially use this funding to enhance security, performance and reliability.

## **ARP Funding Opportunities for Schools**

### **ELEMENTARY AND SECONDARY SCHOOL EMERGENCY RELIEF FUND (ESSER III)**

**Available funding:** The federal government has made an additional \$122.7 billion in funding available through the ESSER Fund; two-thirds of this aid

is now available to states, but they must submit implementation plans that detail how they intend to use this money to access the remaining funding.<sup>3</sup>

**How the money is distributed:** State education agencies (SEAs) are tasked with distributing this aid within their jurisdictions. They must award at least 90 percent of their total ESSER allocation to local education agencies (LEAs) based on their share of E-Rate Title I-A grants – federal funding that has historically gone to schools disproportionately serving low-income children.<sup>4</sup>

**Allowable uses:** LEAs must use at least 20 percent of their allocated funds to provide evidence-based interventions that address learning loss. The remaining funds can be used for activities that support distance education and “promote long-term improvements in technology infrastructure and operations,”<sup>5</sup> as well as efforts to improve cybersecurity as part of schools' ongoing COVID-19 response.

**Deadline:** Funding is available through Sept. 30, 2023.

### **HIGHER EDUCATION EMERGENCY RELIEF FUND (HEERF III)**

**Available funding:** Nearly \$40 billion in additional funding is available through HEERF III.

**How the money is distributed:** Funding is divided between public and private Title IV participating nonprofits and institutions,

historically black colleges and universities (HBCUs), minority-serving institutions, and institutions the Department of Education deems to have the greatest unmet needs due to the pandemic.<sup>6</sup> Aid is awarded based on a complex federal allocation formula that factors in each school's share of Pell Grant recipients who were either enrolled or not enrolled in distance learning before the pandemic.<sup>7</sup>

**Allowable uses:** Eligible institutions must use at least half their funding for emergency financial aid grants, but can also use some of their allocation to offset technology costs associated with distance learning, faculty and staff training, and payroll management. The federal government has left guidance broad in this area to provide more room for local discretion.<sup>8</sup>

**Deadline:** Funding is available through Sept. 30, 2023.<sup>9</sup>

## EMERGENCY CONNECTIVITY FUND

**Available funding:** An additional \$7.17 billion in funding is available through the Emergency Connectivity Fund, a new funding stream that was created with the passage of the ARP in March 2021.

**How the money is distributed:** Schools and libraries that are eligible to receive support through the Federal Communications Commission (FCC) E-Rate program<sup>10</sup> are also eligible to receive federal aid through the Emergency Connectivity Fund. Institutions do not have to be current E-Rate participants to be eligible for ECF aid.

**Allowable uses:** This fund covers the purchase of equipment, including laptops and tablets; mobile hotspots; modems; air cards; routers; and fixed or mobile broadband internet connections and services for library patrons, students and staff who would otherwise lack connectivity to engage in remote learning or access information. In some cases, schools and libraries that lack service options may use this funding to offset the costs of building new wireless networks.

However, software solutions such as videoconferencing tools are not eligible.<sup>11</sup>

## Education institutions have an invaluable opportunity to implement a forward-looking technology strategy.

Licenses, software, content filtering and security services included in the price of purchased connected devices are eligible for support, but separately priced licenses aren't eligible.<sup>12</sup>

**Deadline:** During the initial application window for this aid, which closed Aug. 13, 2021, the FCC received requests for \$5.137 billion of the \$7.17 billion fund. The FCC announced it would open a second window from Sept. 28 to Oct. 13, 2021, for schools and libraries to request funding to offset eligible costs for the 2021-22 school year.<sup>13</sup>

## How Schools Potentially Can Apply ARP Funding

Because schools can use this aid to cover technology infrastructure improvements as well as cybersecurity, they can consider leveraging it to enhance network and application management. An examination of how other education institutions deployed federal aid in the past could provide a roadmap for how K-20 schools can take advantage of ARP funding.

For instance, one consortium of community colleges has used previous rounds of federal funding for cybersecurity awareness training,<sup>14</sup> which can be just as crucial to effective network and application security as a technology-based approach.

Another school district has used network monitoring and application performance solutions to reduce the risks of DDoS attacks and other security incidents that could consume bandwidth and shut down its network. With the new solutions in place, the district was better able to monitor traffic from its data center and cloud service edges to the network edge, improving the user experience for faculty, staff, students and teachers.<sup>15</sup>

Schools can work independently or with a managed services provider to

access automated DDoS protection and cybersecurity risk assessment services, which can increase network and application visibility in on-premises and cloud environments. They can complement these services with solutions such as cloud-based monitoring platforms that provide real-time insights for suspicious network traffic and anomalies within their environment. They can also implement threat detection systems that automatically remove attack traffic to prevent network disruptions, and global threat intelligence feeds that allow their IT and security teams to make more informed decisions about how to protect their organizations.<sup>16</sup>

Education institutions have an invaluable opportunity to implement a forward-looking technology strategy. They can leverage federal resources to adopt a more holistic approach to security and service performance that position themselves to better serve students this school year — and beyond.

*This paper was written and produced by the Center for Digital Education, with information and input from NetScout.*

### Endnotes

- <https://www.netscout.com/blog/help-for-educators-against-cyberattacks>
- <https://edscoop.com/schools-pandemic-relief-cybersecurity/> & <https://www.warner.senate.gov/public/index.cfm/2021/6/with-cyberattacks-on-the-rise-warner-collins-urge-department-of-education-to-empower-schools-to-bolster-cyber-defenses>
- <https://www.ncsl.org/ncsl-in-dc/standing-committees/education/cares-act-elementary-and-secondary-school-emergency-relief-fund-tracker.aspx#:~:text=The%20American%20Rescue%20Plan%20Act,1%25%20for%20summer%20learning%20programs.>
- <https://www2.ed.gov/programs/titleiparta/index.html>
- [https://oese.ed.gov/files/2021/05/ESSER-GEER\\_FAQs\\_5.26.21\\_745AM\\_FINALb0cd6833f6f46e03ba2d97d30aff953260028045f9ef-3b18ea602db4b32b1d99.pdf](https://oese.ed.gov/files/2021/05/ESSER-GEER_FAQs_5.26.21_745AM_FINALb0cd6833f6f46e03ba2d97d30aff953260028045f9ef-3b18ea602db4b32b1d99.pdf), pgs. 21 & 41
- <https://www2.ed.gov/about/offices/list/ope/ccrcaa.html>
- <https://www2.ed.gov/about/offices/list/ope/arpa1methodology.pdf>
- <https://www2.ed.gov/about/offices/list/ope/arpafaq.pdf>, pg. 12
- <https://www2.ed.gov/about/offices/list/ope/arpafaq.pdf>
- <https://www.fcc.gov/general/e-rate-schools-libraries-usf-program>
- <https://www.fcc.gov/emergency-connectivity-fund-faqs>
- [https://www.fcc.gov/sites/default/files/ecf\\_faqs\\_printable\\_pdf.pdf](https://www.fcc.gov/sites/default/files/ecf_faqs_printable_pdf.pdf), pg. 2
- <https://docs.fcc.gov/public/attachments/DOC-375210A1.pdf>
- <https://www.ednc.org/state-board-of-community-colleges-begins-spending-covid-19-funds/>
- <https://www.netscout.com/case-studies/school-district-ensures-quality>
- <https://www.netscout.com/case-studies/university-detects-prevents-ddos>



Produced by:



For: Guardians of the Connected World

The Center for Digital Education is a national research and advisory institute specializing in K-12 and higher education technology trends, policy and funding. The Center provides education and industry leaders with decision support and actionable insight to help effectively incorporate new technologies in the 21<sup>st</sup> century. [www.centerdigitaled.com](http://www.centerdigitaled.com)

For more information, visit <https://www.netscout.com/solutions/higher-education>