A CENTER FOR DIGITAL GOVERNMENT BRIEFING

CARES ACT FUNDING: CYBERSECURITY

The public sector faces ongoing cybersecurity threats, and the pandemic has only made these threats more severe. In the early days of the pandemic, according to the FBI, cyberattacks increased 400 percent compared to before the crisis.[1] Experts say these attacks will continue and only get more sophisticated.[2]

State and local governments already faced significant IT budget constraints and issues with modernization. The pandemic exacerbated these challenges while creating new demands (such as remote work and distance learning) that rely on strong cybersecurity.

However, the CARES Act — the $2.2 trillion stimulus bill Congress passed in March 2020 — gave governments access to funds to strengthen their security posture. State and local governments received more than $150 billion of stimulus money to help them respond to the pandemic.

In December, Congress passed another stimulus bill. Though this legislation didn't provide additional direct aid to state and local governments, it did extend the deadline for these organizations to use their original CARES Act funding. This extension is critical because our research indicates state, local and county governments still have billions of federal dollars left to spend.

Over the past year, the Center for Digital Government has tracked several CARES Act federal funding streams, including the Coronavirus Relief Fund, the Education Stabilization Fund, the Higher Education Emergency Relief Fund, the Elementary and Secondary School Emergency Relief Fund and the Governor's Emergency Education Relief Fund.

Our research indicates governments and public institutions have applied federal funding — particularly from the Coronavirus Relief Fund and Education Stabilization Fund — to address an array of cybersecurity challenges. However, with a substantial amount of funding remaining, organizations may need more guidance for how they can effectively use federal aid to prevent or minimize security threats in the future.

This brief provides an overview of remaining federal funding streams, outlines how state and local governments and public education institutions have already used available funding, and relays key information public leaders need to know to optimize remaining federal aid this year.

CARES ACT APPROPRIATIONS FOR CYBERSECURITY

Coronavirus Relief Fund (CRF)

How much funding is left: According to February federal reporting data analyzed by the Center for Digital Government, there is more than $26 billion remaining in this fund across 48 states. The states with the most funding remaining include:[3]

1. California:	$5.4 billion
2. Texas:	$2.6 billion
3. North Carolina:	$1.9 billion
4. Oregon:	$1.5 billion
5. Florida:	$1.2 billion

Allowable uses: Federal data indicates telecommunications and networking-related expenses have accounted for 1,389 CRF expenditures out of the nearly 20,000 expenditures reported so far. Administration costs, which also partly include technology spending according to the data CDG analyzed, accounted for 926 CRF expenditures.[4]

The federal government has provided broad guidance for how funding recipients can use CRF aid for technology-related needs, including:

- **Broadband access:** State and local governments can significantly expand broadband capacity to facilitate distance learning as a result of the pandemic.[5] (Note: The federal government has specific rules around the types of broadband projects that can be funded with CRF money).
- **Equipment purchases:** Expenses incurred for distance learning, including laptops and other digital devices for students, teachers and staff and technological improvements related to school closures and maintaining compliance with COVID-19 precautions.
- **Remote work infrastructure:** Expenses to improve telework capabilities for employees to comply with COVID-19 precautions.

Next steps: Award recipients have until Dec. 31, 2021, to use these funds. Primary recipients of this funding may have specific guidelines for how sub-recipients can use their allocation. Therefore, sub-recipients should contact their awarding agencies for more information on the application process and for specific guidance (such as whether receiving federal funds will affect certain forms of state aid) as they decide where to invest their allocation.

Education Stabilization Fund (ESF)

Congress originally allocated $30.75 billion to the ESF, which is divided into three funding streams: the Higher Education Emergency Relief Fund (HEERF), the Governor's Emergency Education Relief Fund (GEER) and the Elementary and Secondary School Emergency Relief Fund (ESSER).

How much funding is left: This varies by state. However, in total across all three funding streams, states have spent between 18.5 percent of their allocation (Alaska) and 72.2 percent of their allotted funds (Iowa). On the whole, 47 states have spent less than half of their ESF allocation, according to the most recent federal reporting data from early October.[6]

Allowable uses: Federal guidance for ESF usage is broad, but recipients can use these funds for expenses related to preventing, preparing for and responding to COVID-19,[7] and to expand their technology capabilities for distance learning and ensure the continuity of their operations.

Next steps: For ESSER, state education agencies must award funds to sub-recipients by June 2021. Recipients then have until Sept. 30, 2022, to use their award. For GEER, governors must allocate funds to sub-recipients by June 2021. They also have until Sept. 30, 2022, to use their allocation. Higher education institutions have one year from the date of their award to spend HEERF funds, which can be used to cover expenses dating back to March 13, 2020.[8]

HOW THE PUBLIC SECTOR IS USING CARES ACT FUNDING FOR CYBERSECURITY

State and local governments and education institutions are deploying CARES Act funding for a variety of cybersecurity and technology needs.

North Carolina has allocated $4.5 million of federal aid to its Department of Public Instruction to create a shared cybersecurity infrastructure and facilitate district cybersecurity monitoring and support,[9] which has become even more essential as the schools in the state experience a surge in ransomware attacks.[10]

The University of Texas at El Paso is using $115,000 of its federal funding on cybersecurity technologies. The Idaho State Board of Education plans to use its allocated funds to support a $1 million statewide cybersecurity initiative.[11]

The city of Bozeman, Mont., used 20 percent of its $4.25 million allocation to strengthen its security defenses as it offered more virtual and online services.[12] Oklahoma has used its federal aid to fund a secondary data center with higher availability and advanced disaster recovery capabilities. The state says this investment was critical to help it continue delivering core public services.[13]

As other public sector organizations make similar investments in cybersecurity, adopting a zero trust approach helps state and local governments safeguard their networks in the most comprehensive way possible. Unlike traditional approaches, which focused on securing network perimeters through firewalls and other fortifications, zero-trust strategies ensure data is secure and employees are productive no matter where they may be working or what device they may be using.

With zero trust, users and their devices are verified at the time of authentication during each application access request, irrespective of the employee's location or the network used. User credentials are established through multi-factor authentication, which is repeated and re-established every time a user signs in. A dashboard view shows what types of devices are on the network — even if they are employee-owned — and what the devices are accessing, no matter the platform. Each device being used to access applications is also verified for trustworthiness, giving remote users a secure and consistent login experience to all applications from anywhere.

CARES Act funding is enabling the public sector to advance technology capabilities in response to the pandemic while simultaneously strengthening its security posture. Remote work, distance learning and delivering digital services are data-intensive endeavors, which means government organizations must focus on improving enterprise security as they onboard new technologies to facilitate these efforts. Doing so will increase their resilience, streamline constituents' access to critical services, and safeguard critical government systems and all the valuable public data they collect.

Endnotes

1. https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic
2. https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html
3. CDG Research: CRF Spending Data - Summary Tables
4. CDG Research: CRF Spending Data - Spending Categories
5. https://home.treasury.gov/system/files/136/CRF-Guidance-Federal-Register_2021-00827.pdf, pg. 9
6. CDG Research: CARES Act Education Spending - States
7. https://oese.ed.gov/files/2021/01/Final_ESSERII_Factsheet_1.5.21.pdf
8. https://www2.ed.gov/about/offices/list/ope/factsheetheerfii.pdf & https://oese.ed.gov/files/2021/01/Final_ESSERII_Factsheet_1.5.21.pdf & https://oese.ed.gov/files/2021/01/FINAL_-GEER_Fact-Sheet_1.8.211.pdf
9. https://www.ncasa.net/cms/lib/NC02219226/Centricity/Domain/1065/SBELegUpate_5-7-20.pdf
10. https://www.citizen-times.com/story/news/local/2020/08/28/ransomware-cyberattacks-nc-schools-rise-during-covid-19-pandemic/5644879002/
11. https://www.idahocountyfreepress.com/news/everything-done-for-idaho-students----that-has-been-the-goal-education-week/article_87bad5f0-64c3-11eb-bce4-0b39a95e8f00.html
12. https://www.bozemandailychronicle.com/news/city/city-of-bozeman-doles-out-millions-to-nonprofits-for-covid-19-relief/article_04d2618d-ffcd-51b7-9abf-d651df5f061b.html
13. https://oklahoma.gov/content/dam/ok/en/omes/documents/TX1DRHAv2.pdf

This piece was developed and written by the Center for Digital Government Content Studio, with information and input from Duo Security.

Produced by

CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

For

DUO

Duo Security, now part of Cisco, is the leading secure access and multi-factor authentication (MFA) provider. Duo comprises a key pillar of Cisco Secure's Zero Trust offering, the most com-prehensive approach to securing access across IT applications and environments, from any user, device, and location. Duo offers federal tailored product editions delivering device visibility and continuous, dynamic authentication with FedRAMP authorized security controls at their core. Learn more at **Duo.com**.