



Real-Time Risk



TIMELY NEWS AND TIPS TO HELP REDUCE RISK

October 2021

OCTOBER IS CYBERSECURITY MONTH; AMERICAN RESCUE PLAN ACT FUNDS MAY BE ABLE TO HELP

Cyberattacks continue to be costly and debilitating for public agencies. Some Oregon cities and counties have learned firsthand how disruptive they can be. For CIS' members with cybersecurity issues, the [American Rescue Plan Act](#) (ARPA) may be able to help. An estimated \$2.6 billion in federal funds are earmarked for Oregon — and some of those dollars may be used to address computer software and hardware issues that make public entities vulnerable.

Reviewing ARPA Sections 602(c)(1)(C) and 603(c)(1)(C) suggests that federal funds may be available for cybersecurity. According to [U.S. Treasury guidance](#), government agencies can use ARPA funds for broadband investments such as programs related to cybersecurity or digital literacy training. Recipients may also use funds to protect critical infrastructure, and “as part of provision of government services up to the amount of revenue lost due to the public health emergency.”

To get started, work with your IT manager or service provider to determine security risks. Once security issues are identified, creating a scope of work is the next step.

“An estimated \$2.6 billion in federal funds are earmarked for Oregon...”

Continued on next page



Real-Time Risk

Continued from previous page



Selecting an IT consultant comes next. The consultant can review and assess your current system and provide recommendations on how to correct issues.

Currently, ARPA funds can be used for cybersecurity in three of the main spending categories. Cities will have the most flexibility in terms of allowed cybersecurity uses under the revenue replacement category. The Treasury specifically calls out “modernization of cybersecurity, including hardware, software, and protection of critical infrastructure” as an allowed use of those funds, but only up to the dollar amount that a city or county can demonstrate a revenue loss since the start of the pandemic. Allowed uses could include:

- Investing in IT consulting services to identify current system/network weaknesses and implementing any software and hardware improvements that the assessment recommends.
- Implementing data encryption on all portable devices and media, including laptops.
- Transitioning to operating systems and other applications that are fully supported by the software provider.
- Implementing a multi-factor authentication system for all internet-connected use of municipal devices and systems.
- Completing Compliance with Payment Card Industry (PCI) Security Standards (where credit cards are accepted for payment).
- Implementing end-point detection and response software.
- Improving disaster recovery efforts, such as moving to the cloud for network applications.

Other spending categories are more restricted in terms of allowed cybersecurity uses, but unrestricted in the amount of the investment. Under the infrastructure category funds may be used for cybersecurity needs to protect water or sewer infrastructure, consistent with eligibility

Disclaimer:

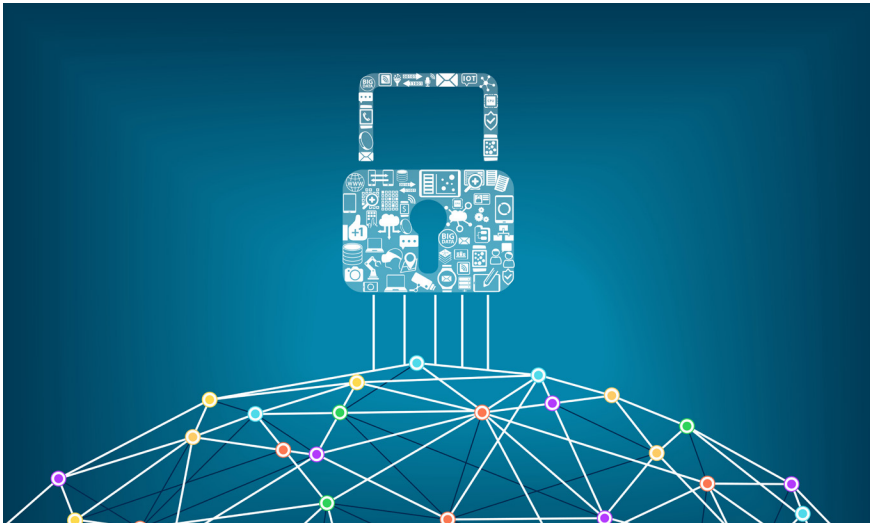
The ARPA information provided above may be subject to change based on updates from the U.S. Department of the Treasury, and the State of Oregon. All potential recipients should confirm that they are eligible to receive federal ARPA funds before moving IT projects forward. ARPA fund recipients will be required to submit one interim report and thereafter quarterly Project and Expenditure reports through the end of the award period on Dec. 31, 2026.

Continued on next page



Real-Time Risk

Continued from previous page



CIS Risk Management Consultants

Adrian Albrich
503-763-3858

Tom BeLusko
503-763-3852

Katie Durfee
503-763-3853

Lisa Masters
503-763-3859

Laurie Olson
503-763-3851

under the Clean Water State Revolving Fund (CWSRF) or Drinking Water State Revolving Fund (DWSRF). Under the assistance to households facing negative economic impacts category funds may be used for digital literacy training.

Once the IT work has been completed, public agencies will have protections in place that will serve their community well. To learn more, visit the [League of Oregon Cities](#) website. CIS is also investigating free cybersecurity services offered by the Department of Homeland Security made available to local government.

CIS' Coverage for Cyber

Because of targeted ransomware on local governments, insurers are making it increasingly difficult to place coverage. Currently, CIS offers excess cyber coverage over the \$50,000 bundled through its liability policy. However, CIS' excess carrier has said that this will be the last year that they'll offer it. Therefore, it is more important than ever for public agencies to take advantage of the new ARPA funds. CIS is investigating excess cyber insurance alternatives for our members.

Currently, CIS partners with Reflare to help members with cybersecurity. CIS' Senior Risk Management Consultant Lisa Masters' [article](#) provides more information. CIS is committed to supporting members by providing resources to reduce cybersecurity threats. For more information, contact your CIS Risk Management Consultant.

