New Cyber Coverage Requirements & Available ARPA Funds Prompt Investment in Cybersecurity.

Alison Cline Earles, Senior Associate General Counsel CIPP/US, Georgia Municipal Association

This article is not legal advice or a substitute for legal advice. It reflects the author's understanding of published treasury guidance as of October 28, 2021.

Underwriting changes and likely availability of American Rescue Plan Act (ARPA) Coronavirus State and Local Fiscal Recovery Funds make the time ripe for cities to invest in "must have" cybersecurity measures.

City Leaders Should Review Underwriting Questionnaires with IT and Develop a Plan to Implement Missing Information Security Measures. Faced with the rapidly increasing threat of ransomware and other cyberattacks, many cities rely heavily on cyber coverage to protect them from financial damage and provide immediate access to response services such as forensic analysis, identification of legal obligations, preparation and delivery of required notifications, and replacement of lost servers and other IT equipment.

In the past six months, cyber coverage carriers have overhauled underwriting requirements. City leaders should review the new underwriting questionnaires with IT support and take actions necessary to meet expected requirements. ***Per Lockton, without certain specific cybersecurity measures in place (see asterisks), cities will be unable to purchase or renew cyber coverage. Moreover, coverage may be limited by deductibles and ransomware sub-limits if the following "MUST HAVE" security controls are not in place.***

- Multifactor authentication* (where you need a password and a one-time code sent to a trusted device) is in place for all email, privileged accounts, and remote.
- Endpoint detection and response* (a tool that continuously scans computers for infection and automatically quarantines and reports the problem) has been deployed for all computers and servers.
- An offline, offsite, current backup of critical data is available*, so the city can restore the data and continue critical business.
- Workers complete user training and regular phishing tests
- Sensitive data is encrypted (so if data is stolen, it is unusable). Note: even if the city could restore from backup and continue business without paying the ransom, if the attacker threatens disclosure of unencrypted information (such as SSNs of utility customers, source and witness information maintained by the police department), the city may feel great pressure to pay.
- City employs (or contracts for) a skilled, empowered security team (to patch rapidly, and share and incorporate threat information in your defenses).
- City periodically tests restoration of backups.
- City promptly updates and patches operating systems, applications, and firmware.
- City maintains and periodically tests an incident response plan.
- A 3rd party performs penetration tests of systems and the city's ability to defend against a sophisticated attack.
- City has segmented its networks, so an attack does not impact all systems.

City Leaders Should Determine Whether ARPA State and Local Fiscal Recovery Funds May Be Used to Pay for New Security Measures.

City leaders may be able to use American Rescue Plan Act Coronavirus State and Local Fiscal Recovery Funds (SLFRF) to pay for the above security measures. The Interim Final Rule provides important guidance, expressly authorizing certain cybersecurity investments and providing a mechanism for determining whether other cybersecurity investments are eligible.

Investments in cybersecurity that fall under the Revenue Replacement/Government Services category and the Water & Sewer Infrastructure category are expressly authorized in the Interim Final Rule.

- If a city can document revenue losses attributable to the pandemic, SLFRF may be used for government services, which include "modernization of cybersecurity, including hardware, software, and protection of critical infrastructure," up to the amount of revenue lost due to COVID.[1]
- Regardless of revenue losses, a city may use SLFRF "for cybersecurity needs to protect water or sewer infrastructure." Note: the EPA water security guide for states[2] and the EPA Incident Action checklist[3] identify specific cybersecurity steps to protect water and sewer infrastructure, many of which are the same as the measures listed above.

Other cybersecurity investments may be eligible, if they are made in response to the COVID-19 public health emergency or its negative economic consequences. The Interim Final Rule states that assessing whether investments "respond to" the public health emergency or its negative economic impact "requires the recipient to, first, identify a need or negative impact of the COVID-19 public health emergency and, second, identify how the program, service, or other intervention addresses the identified need or impact."[4] A city implementing remote municipal courts, expanding telework, and promoting remote payment for services as a result of the pandemic might determine that implementing appropriate security measures associated with these changes responds to the emergency or its negative impact.[5] Treasury has published guidance that cities may use SLFRF to pay attorneys or consultants for guidance about which investments are eligible.[6]

Treasury has provided written assurance that SLFRF spent in accordance with the Interim Final Rule (either expenses expressly listed, or expenses identified as being responsive to the public health emergency or its negative impact) will not be recouped: "Recipients can and should rely on the Interim Final Rule to determine whether uses of funds are eligible under this program. Treasury encourages recipients to use funds to meet needs in their communities. Funds used in a manner consistent with the Interim Final Rule while the Interim Final Rule is effective will not be subject to recoupment."[7] Cities that act in reliance on the express terms of the Interim Final Rule or a legal opinion supporting eligibility should feel confident that SLFRF used to pay for the above information security measures will not be subject to recoupment.

---

[1] Interim Final Rule, p. 60

[2] https://www.epa.gov/sites/default/files/2018-06/documents/cybersecurity_guide_for_states_final_0.pdf

[3] https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf

[4] Interim Final Rule, p. 10

[5] See CISA Alert re: telework https://www.cisa.gov/telework-reference-materials-non-federal-organizations

[6] FAQ 10.5 https://home.treasury.gov/system/files/136/SLFRPFAQ.pdf

[7] IFR Explainer. https://home.treasury.gov/system/files/136/IFR-Explainer.pdf