2025 POLICY BRIEF

REAUTHORIZE THE STATE AND LOCAL CYBERSECURITY GRANT PROGRAM

ACTION NEEDED:

Urge your Members of Congress to reauthorize the State and Local Cybersecurity Grant Program (SLCGP), which provides cybersecurity support to state and local governments throughout the country. The SLCGP was authorized by the Bipartisan Infrastructure Law in 2021 and is set to expire on September 30, 2025. The SLCGP has demonstrated success in providing resources to counties to assess where their networks and services are most vulnerable, help smaller counties begin to implement basic cybersecurity protocols and allow counties to utilize many of the offerings from their state governments to improve security. There is more funding that is needed for local cybersecurity demands that exceed the parameters of the SLCGP, and more flexibility and direct funding needed for counties of different size. Nonetheless, the SLCGP should be reauthorized to continue supporting critical cybersecurity efforts in the interim, while Congress can evaluate and propose changes to the program to improve efficiency.

THE SLCGP HAS HELPED USHER IN NEW RESOURCES FOR CYBERSECURITY PLANNING AND IMPLEMENTATION AT THE STATE AND LOCAL LEVEL.

AS THE CYBERSECURITY LANDSCAPE CONTINUES TO EVOLVE IN COMPLEXITY, AND THREATS PROLIFERATE FOR CRITICAL INFRASTRUCTURE SECTORS ACROSS THE COUNTRY, **CONGRESS SHOULD REAUTHORIZE THE SLCGP TO ENSURE STATE AND LOCAL GOVERNMENTS ARE PREPARED TO BOLSTER SECURITY IN AN INCREASINGLY COMPLEX THREAT LANDSCAPE**

BACKGROUND:

The State and Local Cybersecurity Grant Program (SLCGP), passed as a part of the Bipartisan Infrastructure Law in 2021, providing a total of $1 billion across four years to support state and local cybersecurity planning and implementation efforts. The SLCGP requires state recipients of funds to provide pass-through funding of 80% to local governments, in the form of direct funding or in-kind services. Local governments have received benefits that increased minimum benchmarks for local government cybersecurity readiness, while contributing to state efforts to enhance existing cybersecurity plans or create new plans that address the evolving cybersecurity landscape.

To view the most up-to-date information, scan the QR code below:

As the SLCGP completes its final Fiscal Year of operation, it is imperative that Congress seeks to reauthorize the program to ensure operational readiness, as local governments continue to assume an increased role in preserving the safety of residents' information and

the security of critical infrastructure.

As Congress deliberates future iterations of cybersecurity funding sources for state and local governments, they should provide flexibility in the use of funds across different levels of local government to ensure that funding is addressing areas of respective need. This can include permitting counties at a high cybersecurity readiness posture to access direct funding for advanced cybersecurity infrastructure needs while allowing counties with lower cybersecurity readiness postures to implement basic infrastructure needs such as multi-factor authentication and conversion to the Dot Gov domain.

KEY TALKING POINTS:

- The SLCGP has provided a funding source dedicated to state and local government to improve our cybersecurity readiness posture, and the SLCGP should be reauthorized to continue these efforts.

- Rising cybersecurity demands on local government necessitate a federal funding source that is reliable and flexible for the varied needs of state and local governments.

For further information, contact Seamus Dowdall at 202.942.4212 or sdowdall@naco.org