Reauthorize the State and Local Cybersecurity Grant Program

Issue and Background

- It is well understood that cybersecurity is no longer an IT issue; it is a business risk that impacts the daily functioning of our society and economy, as well as a potential threat to our nation's security.
- Cybersecurity has remained a top priority for the state CIOs for the past ten years, according to the 2026 NASCIO State CIO Top 10 Priorities.
- The inclusion of the State and Local Cybersecurity Grant Program (SLCGP) in the Infrastructure Investment and Jobs Act recognized this tremendous need. With this grant, states and localities have an unprecedented opportunity to improve their security posture, increase collaboration between state, local and federal governments and promote a whole-of-state approach to cybersecurity.
- Rural communities have used SLCGP funds to strengthen long-overlooked defenses, modernizing outdated systems, training local IT staff and expanding shared security services, dramatically improving their ability to prevent, detect and respond to cyber threats with limited resources.
- States have worked diligently to put the $1 billion provided through the four-year program to good use. It has been used to provide cybersecurity training, migrate to .gov domains, install multi-factor authentication and other vital cyber hygiene goals.
- NASCIO has worked proactively with other state and local associations to highlight how this money is being used.
- Congress has recognized the value of the SLCGP and included a temporary extension in an agreement to reopen the federal government, and the House passed the PILLAR Act, which would re-authorize SLCGP for 10 years, under a suspension of the rules.

Recommendations

- **Congress should quickly pass long-term reauthorization of the SLCGP, and the president should sign it into law immediately**. The final version of this legislation must be one that states can actually implement, should include attainable financial requirements for recipients and be accompanied by appropriate funding levels.
- **Work with FEMA and CISA** to ensure grant guidance includes flexibility for states, promotes whole-of-state cybersecurity, emphasizes cyber hygiene, places an emphasis on shared services models and establishes minimum requirements for local government eligibility to receive grant funding.
- **Continue to advocate for states to budget for cybersecurity**. The State and Local Cybersecurity Grant Program requires states to match a portion of federal funding, which increases by 10 percent each year. NASCIO contends this grant program should serve as a change agent for states to either begin to include cybersecurity in their state budget or increase their allocation. In line with Congressional intent and through federal assistance, state governments must realize cybersecurity cannot be solved with a one-time appropriation. Inclusion of a cybersecurity line item is the minimum states should do to meet the seriousness and sophistication of the current threat environment.
- **Ensure state CIOs and CISOs set policy for the grant program**. While State CIOs and CISOs should not serve as grant administrators, they understand the unique cybersecurity challenges facing their state. In consultation with their planning committees, they should set policy parameters and prioritize funding opportunities for this grant program.