

Ensure Responsible Implementation of the State and Local Cybersecurity Grant Program

Issue and Background

- There is a growing recognition at all levels of government 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 2025 NASCIO State CIO Top 10 Priorities.
- As cited in the, 2024 NASCIO-Deloitte Cybersecurity Study, just over half of all states have a dedicated cybersecurity budget line item and only a handful allocate more than ten percent of their IT budget to cybersecurity.
- The inclusion of the State and Local Cybersecurity Grant Program 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.
- The \$1 billion/4-year program will be administered by FEMA with subject matter expertise from DHS CISA and requires significant input by state CIOs and CISOs, who are charged with approving and implementing a statewide cybersecurity plan.
- States have already begun putting this money to good use, but more work is needed to ensure this program remains effective.
- NASCIO has worked proactively with other state and local associations to highlight how this money is being used and to stress to Congress continued support of the program is needed.

Recommendation

- **Work with FEMA and CISA** to ensure grant guidance includes flexibility for states, promotes whole-of-state cybersecurity, emphasizes cyber hygiene, 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 ten 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.

