NASCIO
Representing Chief Information Officers of the States

2022 FEDERAL ADVOCACY PRIORITY

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 the top priority for the State CIOs for the past nine years, according to the 2022 NASCIO State CIO Top 10 Priorities.
- Less than half of all states have a dedicated cybersecurity budget line item while federal government agencies and private sectors allocate a significant percentage of their IT budget on cybersecurity.
- With the inclusion of the State and Local Cybersecurity Grant Program in the *Infrastructure Investment and Jobs Act*, 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.

Recommendation:

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