

Ensure Dedicated Cybersecurity Funding for State and Local Governments with CIOs as Key Decisionmakers

- ***Nearly half of all US states do not have a dedicated cybersecurity budget line item; most state cybersecurity budgets are between 0-3 percent of their overall IT budget, compared with an average of more than 10 percent in the private sector***
- ***Less than 4 percent of Homeland Security Grant Program funding has been allocated to cybersecurity***

State CIOs continue to face an increasingly complex cybersecurity threat environment without dedicated cybersecurity funding. Nearly half of states don't have a separate cybersecurity budget and more than a third have seen no growth or a reduction in those budgets. As state CIOs are tasked with additional responsibilities, including providing cybersecurity assistance to local governments, they are asked to do so with shortages in both funding and cyber talent. Nearly half of all states have a dedicated cybersecurity budget line item while federal government agencies report cybersecurity funding in the president's budget as a portion of their overall IT spending. Additionally, private US industries spend an average of 28 percent of their IT budget on cybersecurity.

NASCIO encourages state governments to establish a dedicated budget line item for cybersecurity as subset of the overall technology budget. While the percentage of state IT spending on cybersecurity may be much lower than that of private sector industry and federal agency enterprises of similar size, the line item can help state CISOs and CIOs give the state legislature and executive branch leaders the right level of visibility into state cybersecurity expenses in an effort to raise funding levels. State legislation could demand visibility into cyber budgets at both the state and individual agency levels. In addition, our 2018 survey results indicate that federal and state cybersecurity mandates, legislation, and standards with funding assistance result in more significant progress than those that are unfunded.

Similarly, cybersecurity spending within existing federal grant programs- such as the Homeland Security Grant Program - can prove a challenge in the face of declining federal allocations, increased allowable uses, and a strong desire to maintain existing capabilities that states have spent years building. In fact, less than four percent of all Homeland Security Grant Program funding has been allocated to cybersecurity over the last decade. It is for these reasons that NASCIO supports legislative efforts including S. 1846, the State and Local Government Cybersecurity Act and S. 1065/H.R. 2130, the State Cyber Resiliency Act to provide increased and dedicated cybersecurity funding to state and local governments. NASCIO urges Congress to pass this legislation with provisions that stipulate that state CIOs play a significant role in the allocation of federally-funded cybersecurity resources. The passage of such legislation would prioritize best practices at all levels of government and greatly assist state and local governments to coordinate resources, better respond to threats, and plan for a strong and resilient cyber future.

