

Expand and Strengthen the State Cyber Workforce

Issue and Background

- States are currently facing a severe shortage of qualified and experienced workers to address the many IT and cyber-related needs of their constituencies. Data from MissionSquare Research Institute indicates that from December 2021 to February 2022, the state and local government job opening rate was the highest it has been in over 20 years.
- In NASCIO's 2025 State CIO Top 10 Priorities, workforce concerns were listed as a key issue for respondents. State CIOs are focused on preparing for the future workforce and reimagining the government workforce; transformation of knowledge, skills and experience; and more defined roles for IT asset management, business relationship management and service integration. All of these tasks require a strong workforce for successful completion.
- However, wage competition, worker attrition, resistance to modernizing the workplace, lack of training programs, administrative delays and countless other obstacles are preventing state government from filling these vacancies, putting critical state services in jeopardy.
- Despite these challenges, states have worked proactively to address employment gaps by removing entry barriers to the cyber workforce, offering on-the-job training, updating remote and flexible work offerings, collaboration with the private sector and much more.
- While states can do much on their own, there is a need for support from Congress and federal agencies to ensure that networks are protected and effective digital governance continues. Cybersecurity is a shared responsibility and it requires a whole-of-government approach to fix key vulnerabilities.

Recommendation

- **Increase partnerships and collaboration between state and federal governments.** While states and the federal government compete for the same talented workers, a collaborative approach to solving workplace shortages will maximize and most efficiently leverage the resources needed to train, prepare and retain these workers, ensuring that the nation's IT and cybersecurity infrastructure is properly protected.
- **Expand existing worker training and education programs.** Existing programs such as the Scholarship for Service program are excellent starting points to develop the cyber workforce, but more can be done to support these programs and ensure they're accessible to state governments.
- **Develop comprehensive solutions.** There is no "silver bullet" or universal solution to solving cyber worker shortages. Instead, stakeholders should consider a variety of policy proposals, and develop them with input from states, the federal agencies and private industry.

