Expanding and Strengthening 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 2023 State CIO Top 10 Priorities, workforce concerns were listed as the third most important issue for respondents. State CIOs are focused on preparing for the future workforce and reimagining the government workforce; transformation of knowledge, skills and experience; 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 governments 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.

Harmonize Disparate Federal Cybersecurity Regulations

Issue and Background:

- As the primary agent of the federal government, states administer dozens of crucial federal programs and deliver vital services to citizens. As a result, state governments must store data and exchange data with federal programmatic agencies and thus become subject to federal security regulations that govern the use and protection of shared data.
- Federal cybersecurity regulations largely address the same controls and outcomes but differ in their specific requirements. Compliance with disparate regulations is an obstacle for state CIOs who are actively seeking savings for taxpayers through IT initiatives like consolidation/optimization. Further, when state data centers are audited for compliance, states receive inconsistent findings from federal auditors despite reviewing the same IT environment.
- As state IT agencies have become increasingly centralized across the country – whereby the state CIO has greater purview over the IT operations of each state agency – compliance with duplicative requirements of federal cybersecurity regulations has grown significantly in cost, both financial and in personnel time.
- In 2018, Congress tasked the Government Accountability Office (GAO) to study the various federal cybersecurity regulations and to issue corresponding recommendations.
- In May 2020, GAO issued their report, ***Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States***, which found that between 49 and 79 percent of federal agency cybersecurity requirements had conflicting parameters and urged the federal agencies to collaborate on cybersecurity requirements.
- At this time, only four of the twelve recommendations for strengthening cyber security have been addressed, and much additional work remains.
- During a June 2021 hearing before the U.S. House Oversight Subcommittee on Government Operations, Chairman Connolly and Ranking Member Hice, as well as numerous other members of the Subcommittee, expressed frustration with the burdensome and duplicative regulations.

Recommendation:

- **Congress and the federal agencies should continue to implement the recommendations of the GAO report** and urge the Office of Management and Budget (OMB) to coordinate collaboration among federal agencies on the development and implementation of cybersecurity regulations.
- **Congress should empower OMB with requisite authorities** to ensure OMB can mandate consultation by federal agencies before updating their cybersecurity regulations.
- **Federal agencies should work with State CIOs and CISOs to streamline cybersecurity regulations**. Addressing duplicative regulations and inconsistent audit practices will not only save taxpayer funds but will also improve our nation's cybersecurity posture. State CIOs and CISOs remain committed to working with federal agencies and auditors to harmonize disparate interpretations of security regulations and to normalize the audit process.

Continued Adoption of DotGov Domain is Essential

Issue and Background:

- The .gov domain provides enhanced security features and increases the public trust in government.
- With rampant misinformation and disinformation campaigns from issues ranging from election security to COVID-19, it is paramount that citizens receive accurate and trusted information from government websites.
- Nearly twenty years after making .gov available to state and local governments, less than 10 percent of local governments are registered on the domain.
- In April 2021, administration of the .gov top-level domain (TLD) was transferred from the General Services Administration to the Cybersecurity and Infrastructure Security Agency (CISA), reflecting the inherent linkage between domain registration and cybersecurity.
- NASCIO's advocacy was instrumental in CISA's announcement to waive the annual $400 registration fee for .gov, which was cost prohibitive and unnecessarily burdensome for the majority of local governments.
- While waiving the registration fee was a key step in the right direction to increase migration to .gov, there needs to be increased education, outreach and advocacy to local governments.

Recommendation:

- **CISA should establish a stakeholder advisory group** to work with key stakeholders and educate local governments on the business case and security benefits of migrating to .gov. CISA should utilize the state CIOs and CISOs to assist in this educational campaign and to highlight a 24/7 help desk and other inherent operational benefits of the .gov program, which will provide tremendous support to resource and personnel-constrained local governments.
- **Expand opt-in centralized cybersecurity services for .gov entities** CISA has built a strong team focused on providing technical support and information to SLTTs. With ownership of the .gov program, they can now make available opt-in cybersecurity shared services on top of the .gov TLD. Doing so will create a compelling case for local governments to migrate to a .gov and leverage the additional capabilities CISA can make available.
- **Tie federal grant funding for local governments to .gov adoption/migration**. With the recent passage of the State and Local Cybersecurity Grant Program, local governments will receive 80 percent of federal funding. CISA and FEMA should mandate local governments will only be eligible for grant funding if they agree to migrate to the .gov domain.
- **Allow flexible usage of State Homeland Security Grant Program funds** to be used for migration to .gov domain to include non-technical transition costs on items including communication outreach to citizens, marketing materials and revisions to stationary, business cards and other printed collateral.

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 ten years, according to the 2023 NASCIO State CIO Top 10 Priorities.

- As cited in the, 2022 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.

- With the release of the Notice of Funding Opportunity in September of 2022, states and territories can now begin planning how they intend to use this funding to meet their cybersecurity needs.

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.