Questions for Doug Robinson
Executive Director, National Association of State Chief Information Officers (NASCIO)

Questions from Chairman Gerald E. Connolly
Subcommittee on Government Operations

June 30, 2021, Hearing: "Catalyst for Change: State and Local IT After the Pandemic"

---

1. **Please list examples of federal cybersecurity regulations state governments must follow that might be in conflict with other regulations or requirements.**

   State CIOs support the mission of state agencies and the federal programs they administer with technology and are rarely, if ever, the direct recipients of federal funds or grants. Because state CIOs deliver enterprise IT services to state agencies that administer federal programs or receive federal funds or grants, state CIOs and the larger IT enterprise must also comply with and abide by federal data security regulations that are imposed on those state agencies. Thus, state CIOs find themselves operating in an increasingly complex regulatory environment driven by disjointed federal regulations.

   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.

   Below are some of the federal data security regulations which state executive branch agencies must comply:

   - Internal Revenue Service (IRS) Publication 1075
   - FBI Criminal Justice Information Services Security Policy (FBI-CJIS)
   - Health Insurance Portability and Accountability Act (HIPAA)
   - Office of Child Support Enforcement security requirements
   - CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E)
   - Social Security Administration (SSA) Electronic Information Exchange Security Requirements
   - U.S. Department of Labor - State Quality Service Plan: Agency Assurances
   - 42 CFR part 2 - Substance Abuse and Mental Health Services Administration
   - Family Educational Rights and Privacy Act (FERPA)
   - Gramm Leach Bliley Act
   - Child Internet Protection Act of 2000
   - Child Online Privacy Protection Rule of 2000

In addition to various federal regulations, state CIOs are also pushed to adopt other standards and frameworks that federal grants and contracts necessitate:

- NIST and FIPS standards (e.g. NIST 800-53 Revision 4)
- NIST Cybersecurity Framework
- NIST Risk Management Framework
- SANS and CIS Top 20 Controls
- Federal Information Security Management Act (FISMA)
- Control Objectives for Information and Related Technologies (COBIT)
- ISO/ISE 27000 Series
- Payment Card Industry Data Security Standard (PCI-DSS)

2. **How can state and local chief information officers more effectively respond to the recent uptick in cybercrime?**

As cybersecurity has remained the top priority for state CIOs for nearly the past decade, NASCIO has long encouraged a whole of state approach to cybersecurity. Certainly the evolution of cyber incidents has rapidly progressed from merely digital consequences to sophisticated strikes designed to threaten the health and safety of our nation's citizens – with state and local governments remaining some of the most vulnerable entities.

State governments need effective governance structures and clearly delineated roles and responsibilities to address the growing cybersecurity threats. In order to better protect our citizens, state leaders must begin to view cybersecurity as a business risk that can impact the daily functioning of state government. We have seen this lack of understanding and certainly prioritization of cybersecurity in the 2020 Deloitte-NASCIO Cybersecurity Study, which found that only 36 percent of states and territories have a dedicated cybersecurity budget and nearly a third have seen no growth in those budgets.

We have also authored numerous reports on cybersecurity, including the 2016 Cyber Disruption Planning Guide, which served as a call to action for states to develop governance structures that clearly define roles and responsibilities during cyber incidents. The Planning Guide and subsequent publications advised states to put a greater emphasis on basic cyber hygiene. The lack of mandatory cybersecurity training for state employees and contractors is certainly one area that still remains a vulnerability nationally.

Additionally, increased information sharing and collaboration between state and local governments should be a top priority. In January 2020, NASCIO and the National Governors Association released Stronger Together: State and Local Cybersecurity Collaboration, which outlines promising programs that states have initiated to enhance collaboration with their local government counterparts for cyber resilience. It also provides high-level recommendations for state officials looking to strengthen partnerships with local government officials on cybersecurity.

3. **How might federal grant programs designed to assist state and local governments improve their information technology systems be more effective?**

In order to best assist state governments in terms of IT modernization, states would benefit significantly from consistent direction from the federal government to include more expansive advice from federal agencies and programmatic guidance. As Congress considers such a grant program, flexible usage of funds to include common shared services for grant recipients would maximize federal investments in program delivery. For example, shared funding of an enterprise identity and access management solution that all agencies could use.

A grant program should also emphasize modular and agile development, as well as uniformity. As the Chairman has highlighted, compliance with the disparate federal cybersecurity regulations is one such example. Additionally, a grant program that emphasizes a greater understanding by the federal programmatic agencies of the operating models of state IT agencies would be beneficial.

4. **How could your members make effective use of a forum like the Advisory Commission on Intergovernmental Relations? What topics do you think are most ripe for discussion at an intergovernmental forum?**

   While NASCIO has not taken a formal position on the re-establishment of the Advisory Commission on Intergovernmental Relations or a similar organization, there are numerous areas that such a commission could improve communication and information sharing between federal, state and local governments. One such area of emphasis is on the critical nature of the cybersecurity relationship and ecosystem between federal, state and local governments. There is no forum to raise and highlight the myriad challenges of intergovernmental cybersecurity information sharing. The commission could serve as a place where those discussions could occur and to bring together the various associations that represent state, local, tribal and territorial governments, including NASCIO, to share information.

5. **How can we streamline state- and local-government-level acquisition of technologies in ways that are secure and effective?**

   The most important aspect of the acquisition of technologies is to be informed by the enterprise architecture and standards of the state. There should be an increased focus on business problems and outcomes and not on defining specific technology solutions available from the marketplace. This would allow the vendor community to propose modern, flexible and interoperable solutions. To streamline technology acquisition, states have utilized NASPO ValuePoint, cooperative agreements and multistate cooperative contracts, as well as GSA Schedule 70.

6. **Are there any structural barriers that might prevent states from participating in something like StateRAMP?**

   There are a few structural barriers that could prevent states from participating in StateRAMP. For example, if a state had its own solicitation and competitive procurement vehicle and is unable to use StateRAMP certifications, a state had already established a cloud service provider certification and acquisition policy and process, or if the state information technology agency may lack the authority to set a cloud certification standard across all agencies.

7. **A core tenet of FedRAMP is reciprocity—that a FedRAMP certification in one space can be reused in another. Do you think reciprocity is realistic among states? Why or why not?**

   Yes, reciprocity is realistic among the states. States have a long history of negotiating and supporting reciprocity agreements. Examples include interstate compacts, mutual aid for emergency assistance, employee income tax reciprocity and multi-state licensure for occupations.

   StateRAMP provides the foundational certification under the model of "certify once and then use many times" by the states. However, not all use cases in the states will be appropriate for the StateRAMP model. The key issue here is not reciprocity among states – it is reciprocity between FedRAMP and StateRAMP.

8. **What other resources, besides funding, should Congress and the federal government use to accelerate this type of digital transformation at the state and local level?**

   There are numerous areas where Congress and the federal government can best assist state governments, including a better understanding of the CIO operating models. Nearly every state in the country has seen increased consolidation and centralization of IT services, which are delivered by the state CIO. This consolidation has given the CIO purview, and in many cases the authority, over all IT operations, policies and initiatives across each state agency. As the state CIO has emerged as the central leadership figure in state IT, the federal government and agencies should make a strong effort to increase communication, collaboration and information sharing with the CIO. The development and subsequent revisions of federal programmatic agency cybersecurity regulations encapsulates the lack of communication and coordination between federal and state governments. Nearly every regulation mentioned in our response to Question 1 has been implemented and periodically updated with minimal input from state governments. The outreach to solicit comments or feedback from the state CIOs is marginal at best. Encouraging agencies to proactively work with states as they revise these regulations would be beneficial to all parties.

   The federal government should also issue grant guidance that emphasizes adoption of digital services and emerging technologies that would stimulate the improvement of digital services at the state level. As states function as the laboratory of democracy, the federal government should encourage innovation with their counterparts at the state level. By embracing technological advances and working with private sector solution providers, state CIOs seek to enhance the effectiveness of state government in delivering services to citizens. State CIOs regularly contemplate issues related to communications infrastructure, data standardization, privacy, security, and IT asset management. It would be premature to regulate an emerging technology when applications are being tested or are in the early phases of deployment. A premature regulatory framework or preemption of state approaches could stifle innovation and introduce unintended consequences.