CENTER FOR
DIGITAL
GOVERNMENT

July 28, 2021

The Honorable Gerald E. Connolly, Chairman
Subcommittee on Government Operations
Committee on Oversight and Reform
2157 Rayburn House Office Building
Washington DC, 20515-6143

Subject: Catalyst for Change: State and Local IT After the Pandemic

Dear Chairman Connolly,

Thank you so much for inviting me to participate in the hearing. Enclosed are my written responses to the post-hearing questions.

I appreciate the opportunity to engage in this important discussion. If you need additional information, please feel free to contact me.

Respectfully submitted,

Teri Takai

Teri Takai
Vice President
Center for Digital Government
Teri.Takai@erepublic.com
248-561-4064

Questions for Ms. Teri Takai
Vice President, Center for Digital Government

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. Would re-establishing the Advisory Commission on Intergovernmental Relations help state, local, Tribal, and territorial leaders find more effective ways to collaborate and communicate on issues of national importance? If so, which issues do you think are best suited for this type of forum?

   The re-establishment of the Advisory Commission on Intergovernmental Relations has the potential to open up a dialogue on many important technology issues that state and local governments face today. This is especially important in an ever-changing technology landscape that affects government as well as citizens and businesses.

   To ensure that there is representation of all parties in the Advisory Commission, the legislation should consider the establishment of a state advisory commission on technology modernization that includes cybersecurity, critical infrastructure, and technology skills in that state. A representative of these commissions would represent the state on the federal commission looking at issues of national importance. This will help promote a sharing within a state and also ensure that representation on a federal commission considers all jurisdictions.

   Issues that are best suited to this type of forum might be:

   a. Cybersecurity mutual aid, including funding and resource sharing, is especially critical given today's climate.

   b. Joint procurement contracts and expertise sharing so that smaller jurisdictions can take advantage of pricing and contracts.

   c. Shared services, particularly for smaller local, Tribal, and territorial jurisdictions within a state to provide sharing of skilled resources, contracts, and technologies.

2. In your written testimony, you talk about the opportunity for shared services on the state level. Can you elaborate on how that could work and create efficiencies?

   The opportunity for shared services at the state level has potential both within state government and across local, Tribal, and territorial jurisdictions within a state.

   a. Many states have already organized to provide a single service that all state agencies use. The best example is email and the collaborative technologies that were essential in response to the pandemic. This provides the opportunity to leverage resources and improve pricing and contract negotiations due to a higher volume under one contract.
   b. The second opportunity for shared services is the establishment of contracts where state agencies and local governments share contracted services especially with technologies like cloud computing. This provides efficiencies, improved services, and improved security because the services are established once and used by many organizations.
   c. There is opportunity for state agencies and local government to share contracts. This often requires states or larger jurisdictions to develop and create the contracts that other jurisdictions can use to purchase commodities and/or services. This approach is similar to the role that GSA plays for the federal government agencies. The GSA contracts are also used at the state and local level.

3. Can you briefly explain what StateRAMP is and why you think it is important to state governments?

   StateRAMP has the same intent as FedRAMP to provide a framework and requirements for state government cloud-based services as well as providing an organization to ensure that companies are employing cybersecurity tools and processes for continuous monitoring against threats and intrusions.

   This is important for state governments:

   a. There are companies who wish to provide cloud-based services to only state government. These companies are not able to apply and receive FedRAMP certification because they do not have a federal agency sponsor.
   b. States would like to have the same assurance of a company's compliance with FedRAMP requirements so that they can utilize the cloud-based services provided by those companies with the assurance that a set of cybersecurity standards are met. In some cases, these may be local companies that the state is interested in growing from an economic development perspective.
   c. The use of the StateRAMP certification eliminates the need for each state to establish different requirements, have an independent certification process, and expend both technical and procurement resources to validate technology companies.

4. What might prevent states from participating in something like StateRAMP?

   States may decide not to participate in StateRAMP based on the overall technology governance in the state:

   a. The state procurement or technology organization may decide that they would prefer to set their own requirements or may decide that they want to use different requirements for different cloud providers.
   b. The central state information technology organization may not have the authority to set a standard across state agencies.

5. 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?

   The goal of StateRAMP is reciprocity across states, just as the goal of FedRAMP is reciprocity across Federal agencies.

   a. States are already stressed with long lead times in procurement, lack of skills to create, execute, and manage cloud services, and the ability to ensure adequate cybersecurity controls are in place.
   b. StateRAMP provides a standard set of requirements and also a non-profit organization that will review the continuous monitoring data that the companies are required to provide, much as GSA does for FedRAMP.
   c. A benefit to both the states and to the technology providers is to provide a set of standards that are accepted by those states that decide to utilize the StateRAMP certification. Without a standard, companies are required to meet each individual state or in some cases state agency requirements for cybersecurity.
   d. The upfront cost of StateRAMP certification and the ongoing cost of providing monitoring data is borne by the technology companies at no cost to the states.

6. How do we ensure that state and local governments do not revert back to business as usual, and leverage lessons learned during the pandemic to improve services?

   The main threats to ensuring that state and local governments continue to improve citizen services are a lack of leadership and a lack of funding, which are interdependent. It is essential that technology modernization and the move to bring technology to improve all citizen services be a priority for executive and legislative branches. Chief Information Officers, as the lead for technology efforts, must report into the executive branch, receive funding support from the budget office, and be supported in obtaining funds by the legislature. This will result in recruiting and retaining the talent needed to ensure that technology continues to improve government services. The right talent and the right reporting relationships are essential.

7. 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 actions that Congress and the federal government can take to accelerate and provide focus for state and local government:

   a. Congress and the federal government must ensure that there is a clear path for state and local governments to take advantage of the knowledge and expertise of the federal agencies in cybersecurity. This includes knowledge transfer, transparency, and lessons learned provided to all levels of government.

   b. As NASCIO has stated, there is a need for the federal government to standardize various compliance regulations that the states face coming from different federal agencies. The regulations are redundant and often conflicting, causing an administrative burden at the state and local level.

   c. Congress must continue to fund technology modernization in the federal agencies, especially those that interact and fund state and local government operations. As the federal agencies modernize, the state and local agencies will need to ensure that they also have the technologies to integrate and provide citizen services.