CompTIA | pti Public Technology Institute

Questions from Chairman Gerald E. Connolly

Subcommittee on Government Operations

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

Response by Dr. Alan R. Shark

Executive Director, CompTIA’s Public Technology Institute

July 28, 2021

1. How should local governments prepare for and respond to attacks on their information technology (IT) systems?

Today local governments successfully fend of thousands attacks every week. The ones we read about are the reported failures. Since there are no uniform requirements for reporting attacks, we lack the very information needed to better counter growing threats.

Response: Based on PTI’s research and shared experiences to date, the following recommendations are offered.

a. Each local government should designate one individual to oversee cybersecurity. Many larger jurisdictions have created the position of chief information security officer (CISO) with smaller entities relying on a local CIO or equivalent.

b. Each local government entity should involve its elected leaders and senior management in areas of cyber policy, cyber performance, risk assessment as well as greater cyber awareness. Elected leaders need to be more involved with insuring adequate funding for hardware and software requirements which includes staff training and certifications.

c. Every state should designate a senior staff member to serve as the state’s cybersecurity coordinator. Today, each state does “its own thing – its own way” and the level of services and support from states are widely varied and inconsistent. Most local government IT managers have no idea what a state may offer, let alone who to call in case of an emergency.

d. Formalize, and standardize where possible, the National Guard’s ability to step in for certain cyber emergencies. The list of National Guard units who offer such services has grown to 26, which is a remarkable jump from just two years ago, but more still needs to be done.

e. States and localities should work towards requiring advanced training and cyber certifications for IT professionals. Doctors, lawyers, CPAs, and firefighters all must maintain their certifications to practice their profession. Given the huge amounts of critical and confidential data entrusted to local governments, it is imperative that our IT professionals are encouraged – if not required to be certified (and recertified) in cyber and network security.

f. All state and local governments should be both encouraged and required to report all “significant” breaches and hacks to a central federal authority, i.e., CISA, FBI, MS-ISAC, etc.

g. States, with the help of the federal government, should consider certifying all local governments for cybersecurity best practices, expertise, and cyber resilience. Such a certification would be similar to how health facilities, institutions of higher learning, and other public institutions to provide both a framework for compliance as well as helping to ensure that local governments are utilizing the best practice for prevention as well as remediation if something does go wrong. The closest thing we have standards and certification of an entity, rests in the pre-qualification process of insurance companies offering cyber insurance as well as public auditing firms who have increasingly begun to look at cyber practices and record and data integrity.

2. Are grant programs administered through the Federal Emergency Management Agency and other federal agencies to address acts of terrorism including cyberattacks sufficient to update state and local IT systems? Why or why not?

Response: When asked, IT professionals are often kept in the dark as to what federal agencies provides needed help in the areas of cybersecurity preventions and remediation. This is true of many Federal programs that do not find there way to the local level. Traditionally, senior public managers tasked with tracking federal funding opportunities do so without any communications from IT professionals at the local level. Hence IT professionals are left out of funding strategies and helping with the articulation of needs.

The best source for help comes from the MS-ISAC funded by the Department of Homeland Security (DHS) But while all 50 states are members, only a small percentage of U.S. territories, tribal nations, and local governments are represented in MS-ISAC membership. Every local government should be and required to join. Over the years, PTI has been a strong supporter of MS-ISAC and whose logo endorsing it appears on their home page. We view this as the primary place to see what is happening across the nation and take advantaged of the many valuable and free cyber information and cyber tools.

In summary, the Federal government has often struggled to provide information that reached local governments – often relying on State governments to fulfill this critical informational mission. Judging from the response PTI members have voiced – more direct communication must be considered. Here is where local government institutions, such as PTI and the International City/County Management Association, can play a key communications outreach role.

3. How might federal grant programs to assist state and local governments in fortifying their IT systems be improved?

Response: As mentioned above in response to question two, the federal government has often struggled to provide information directly to local governments, instead typically relying on state governments to fulfill this critical informational mission. PTI members believe more direct communication between the federal government and localities must be considered. This would be beneficial in providing programs better suited for local governments that list specific categories for cybersecurity improvement. Additionally, the federal government could consider leaving a category open for "innovation" and encourage responding jurisdictions to justify using federal funding for innovative approaches that could be replicable elsewhere. Money for CARES and ARP were quite general and flexible – but there was nothing specified in having some of it go towards cybersecurity.

4. Would a formalized forum for collaboration across levels of government similar to the Advisory Commission on Intergovernmental Relations have been helpful throughout the pandemic? Why?

Response: Having a formalized forum for collaboration across all levels of government would have been helpful throughout the pandemic. The need to communicate across and through lines of government at all levels has always existed – but the pandemic served as an accelerant for the need for more information and help across all levels of government. Improved and established lines of communication could have led to improved coordination of citizen-facing services, better identification of critical resource unmet needs and requirements, improved communication regarding federal and state resources, improved communication about cyber threat activities and known remedies, and finally, more detailed information about federal programs aimed at assisting state and local governments.

5. Would a permanent formalized forum for intergovernmental deliberation be beneficial to both government and the public it serves? If so, how?

Response: There has always been an ongoing need for a formalized role for intergovernmental relations. This was highlighted during the pandemic when communications between and among all levels of government occurred in an ad hoc manner. An ongoing, robust intergovernmental forum requires a well-reasoned governance plan with established roles and responsibilities throughout. This is very well addressed in the currently proposed legislation, H.R. 3883 as proposed in the current session of Congress. It is my hope this Bill ultimately passes and becomes law.

Prior to 1996, the Advisory Commission on Intergovernmental Relations (ACIR) served as both a forum for intergovernmental dialogue and as a neutral analytical commission, much like the Congressional Budget Office that published reports and guidance on how to create partnerships across the different levels of government. Today with the growing sophistication of technology and policy there has never been a greater need to restore and improve upon the ACIR. Based on my personal experience, I would strongly support H.R. 3883, the Restore the Partnership Act in its current form.

Finally, there is one significant difference that makes the latest initiative more promising is the growth of broadband and collaboration tools that are now commonly utilized by government officials found in all levels of government.

6. How can and should local governments most effectively leverage the Coronavirus State and Local Fiscal Recovery Fund?

Response: Much by way of the *Coronavirus State and Local Fiscal Recovery Fund* is still unfolding – at least when it comes to local governments. Focusing solely on cyber needs, we strongly believe local governments need to focus resources beyond hardware and software solutions and include also the human-factors that can go along way towards better fighting cyber threats. The pandemic exposed numerous deficiencies – including the lack of trained or certified IT staff to help counter the enormous burdens placed on IT system integrity. IT staff have evolved into a profession and like any worthy profession there is an on-going need to train and certify just as is expected with public safety, pilots, CPA's and more. The pace of change in IT is nothing short of dizzying and requires the need for staff professionals to keep up on the latest tech developments.

There are numerous certification programs from which to choose including such broad areas as IT fundamentals, cybersecurity, cloud, infrastructure, and professional skills. More must be done to encourage current IT professionals by supporting IT certifications and other forms of IT training and development. Research has found that when government entities are viewed as investing in their professional staff – a greater sense of commitment, job satisfaction, and increased productivity can be expected.

Research has also show there is an IT manpower gap that was further exacerbated by the pandemic. Making matters worse is the fact as the economy recovers many IT professionals are leaving local government for higher paying jobs in the growing private sector.

Apprenticeships can play a role in growing the next generation of talent in these government IT departments. They increase retention, attract diverse talent, and provide a reliable talent development strategy. To date CompTIA has played a leadership role in promoting apprenticeships in IT.

Today's economy is increasingly dependent on the technology industry to generate economic growth and the skills gap is a significant hurdle. In 2020, the technology industry contributed nearly $2 trillion to the U.S. economy and employed more than 12 million workers. However, there were also nearly 4 million tech job openings. These findings, coupled with the recent calls by the White House to build a diverse and accessible talent pipeline to strengthen our nation's supply chains, demonstrate the urgent need for Congress to work quickly to address this important matter.

CompTIA supports the Championing Apprenticeships for New Careers and Employees in Technology (CHANCE in Tech) Act. The CHANCE in Tech Act would make commonsense reforms to the Department of Labor's registered apprenticeship program, creating jobs and economic growth. The current proposal would create technology apprenticeships and help forge public-private partnerships to serve as intermediaries between employers participating in the registered apprenticeship program, industry, training partners, and government entities. Each intermediary would assess and train potential apprentices in coordination with local and regional workforce demands. The intermediaries would lessen the regulatory burden on participating employers by tracking success indicators and managing other reporting requirements. Collectively, the CHANCE in Tech would better align workforce upskilling with local and regional demands and provide an alternative pathway into the tech workforce for countless Americans.

7. What can leaders at all levels of government do to ensure that cybersecurity is a foundational component of all public sector IT purchases?

Response: The IT acquisition process is cumbersome at all levels of government. However, in order to ensure that cybersecurity becomes a foundational component of all public sector IT purchases, there needs to be a better dialogue between tech professionals and senior public mangers. Over the years but more recently highlighted by the pandemic, we often hear from local government tech leaders there is a fundamental and growing disconnect between needs articulation from among tech professionals and senior public managers sorting through competing government-wide needs. It would be helpful if the federal, perhaps with some help from the states, could score cyber-related expenditures (including IT training, development, and certifications) higher and encourage greater investments in cybersecurity protection.