Written Testimony of Dr. Alan R. Shark

Executive Director of CompTIA's Public Technology Institute

Before the House Committee on Oversight and Reform

Subcommittee on Government Operations

"Catalyst for Change: State and Local IT After the Pandemic."

June 30, 2021

Chairman Connolly, Ranking Member Hice, and Members of the Subcommittee:

Thank you for the invitation to testify today to discuss, in particular, how local governments, on the frontlines of unprecedented events such as the pandemic have fared – and more importantly, lessons learned and what can be done by the Federal government to help ensure our frontlines of communications and services receive the needed support for possible future occurrences. It is my hope to further elaborate on local governments as catalysts for change.

Allow me to begin by defining the lenses in which I view the topics at hand. I bring to this discussion some 30 years of experience and even as of today I wear multiple hats that enable me to address this critical and timely issue. Currently I serve as the executive director of the Public Technology Institute (PTI) and have served in this capacity since 2004. PTI was formed in 1974 by numerous groups such as the National League of Cities, the National Association of Counties, and the International City and County Managers Association to name just a few. Our mission has always been to assist through programs and services and provide thought and action leadership on appropriate uses of current and emerging technology for cities and counties throughout the nation – regardless of size. In 2019 PTI merged with the Computing Technology Industry Association better known as CompTIA. CompTIA is a leading voice and advocate for the $5 trillion global information technology ecosystem; and the estimated 75 million industry and tech professionals who design, implement, manage, and safeguard the technology that powers the world's economy.

Through education, training, certifications, philanthropy and market research, CompTIA promotes industry growth; the development of a highly skilled workforce; a commitment to creating an environment where innovation happens, and the opportunities and benefits made possible through technology and available to all. CompTIA is has become a highly respected vendor-neutral, independent source of information on a wide range of technology topics, including cybersecurity; education, training, and certification of the global tech workforce; new and emerging technologies; legislation and policies affecting the industry and workforce data, development, and trends.

Finally, for the past 6 years I have served as Fellow and Chair for the National Academy of Public Administration's (NAPA) Standing Panel on Technology Leadership. I should also add that for the past 12

years I have taught a master's level course on "Technology and Public Administration" – most recently at the Schar School at George Mason University.

My comments today represent my own views and are derived in part from PTI's and CompTIA's research as well my direct experiences working daily with public managers and technology leaders in local governments across the nation.

Summary: What the pandemic revealed:

The pandemic brought local governments together in ways never experienced before – and most were able to pivot to a comprehensive remote environment in a remarkable period of time. It must also be pointed out the vendor community stepped up in near warp-speed too and assisted in many critical ways where many public-private partnerships were formed and accelerated. Cities and Counties across the nation stepped up to provide citizens with enhanced website offerings, developing apps, and the expanded use of social media outreach to share the latest COVID information in addition they developed registration systems for testing and vaccinations, pivoted many in-building services to digital citizen outreach services offered 24/7. And they did this all while supporting a near-remote workforce.

Despite all the dramatic and positive gains not every entity fared the same – the pandemic exposed weaknesses and serious short and longer term vulnerabilities. It also demonstrated the need for greater IT modernization and resiliency. The pandemic also laid bare the gaps in IT staff and competencies, and cybersecurity protections. For example, when everything pivoted to digital, it paved the way for greater cyber incidents leading to costly ransomware attacks.

The pandemic underscores the need to address on-going and newly found local government deficiencies regarding digital infrastructure and the growing costly attacks from cyber criminals who are targeting cities and counties. These criminal activities have greatly increased as more local government services are now online.

We must also recognize not only the vital role technology plays and will continue to play in government – but we must also recognize the human factor. Tools are nothing without able mechanics and similarly, technology is but a highly sophisticated set of tools that require humans to master their new and growing toolboxes.

In all, I wish to point out 5 major areas of concern, they are:

1. IT Modernization is still lacking in providing greater digital services directly to citizens. IT modernization must also include a focus on addressing the need for greater agility and resiliency.

2. Pressing need for enhanced intergovernmental relations. We all have so much to share, learn, and coordinate – yet we continue to be stuck in silos.

3. Significant Cyber threat protection – Both in terms of *Prevention* and *Remediation*.

4. Abundant need for professional development and certifications aimed at existing staff.

5. Actively address manpower shortages requiring more creative approaches to recruitment and retention in IT-related positions.

IT Modernization is still lacking and in providing greater digital services directly to citizens. IT modernization must also include a focus on addressing the need for greater agility and resiliency.

As the pandemic grew, local governments had little choice but to pivot towards online services critical to maintaining government operations and connecting with citizens. Despite all the dramatic and positive gains not every entity faired the same – the pandemic exposed weaknesses and many local governments were forced to remain open in order to serve its citizens. Local government leaders tell us that they are somewhat aware of some of the new funding opportunities that are aimed at generally helping local governments but are unclear just how they can be used for technology modernization. They further state that they see many rules and regulations that often conflict with the funding agency/source. At the very least it would make sense for someone to step in and clarify how IT spending at the local, level can be applied for and clear up the various reporting rules and regulations.

Speaking for myself, I believe the proposed *State and Local Digital Service Act of 2021* would greatly assist local entities in applying for grants aimed at IT modernization. From what I have viewed thus far the proposed Act provides guidance and funding for state and local governments to form digital service teams focused on delivering fair and effective public services. My only concern is that funds have a tendency to go to the states first with little left to be carved up among the many thousands of cities, counties, townships, and Tribal governments. My fear is the legitimate collective needs of all these entities exceeds however generous, the Bills proposed funding.

Often left out of legislative remedies and funding discussions is the fact that local governments are largely on the front lines of citizen engagement and serve as agents for state and federal program information and services.

Pressing need for enhanced intergovernmental relations. We all have so much to share, learn, and coordinate – yet we continue to be stuck in silos.

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. We simply need more

effective means of communications across all levels of government and to be able to share collective needs, concerns, review policy and legislative, and judicial implications across all lines of government. I find the accountability section of the proposed Act to be enlightened and sorely needed. I believe when the ACIR was abandoned, it was argued that the Office of Management and Budget (OMB) would assume much of the ACIR functionality, albeit more streamlined. However, this responsibility never materialized and thus the needs and opportunities have only increased dramatically over the years.

Significant Cyber threat protection – Both in terms of Prevention and Remediation.

The Federal Bureau of Investigation's Internet Crime Complaint Center logged 791,790 complaints of suspected internet crimes last year — an increase of more than 300,000 complaints from 2019. Reported losses exceeded $4.2 billion. Unfortunately, there is no requirement that local governments report cybercrimes unless personally identifiable information has been breached. I am personally aware of many ransomware attacks and sadly they are clearly on the increase, are demanding greater sums of money via Bitcoin, and to add to the pressure to deliver – the criminals are starting to expose sensitive record of public employees and residents.

According to a published report in March 2021, by Comparitech, over the last few years, ransomware has become a huge cause for concern for all kinds of organizations. For governmental entities, it can mean extended downtime, lost files, and the inability to access key infrastructure and services. This includes 911 services and utilities. The report's researchers found a total of 246 separate ransomware attacks were carried out on government agencies in the last three years (from 2018 to 2020). These have potentially impacted over 173 million people and may have cost $52.88 billion.

Cyber security has three main components, appropriate and necessary tools to prevent cyberattacks including on-going cyber awareness training; necessary tools and procedures to remediate if an attack occurs by at least having safe back-ups; and finally skilled and certified IT professionals who have been trained and updated on the very latest types of attacks and best practices. Many local governments were able to utilize CARES Act funding and now are contemplating the American rescue Plan Act – though there are no specifics related to cyber security. We all need to remind local governments that this is a resource that should be targeted in part for cybersecurity.

PTI's parent organization, CompTIA is on record in supporting the *State and Local Cybersecurity Improvement Act of 2021*. This important legislation will provide the Department of Homeland Security the tools, authority, and funding it needs to advance its cyber mission. CompTIA believes this legislation

can significantly impact the ability of state, local and tribal governments to deter ransomware and other cybersecurity attacks.

Abundant need for professional development and certifications aimed at existing staff.

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, Professional skills. Local governments when faced with uncertain financial outcomes due to a crises such as the great recession of 2008-2009 and the pandemic are the first to cut training and travel. 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.

Actively address manpower shortages requiring more creative approaches to recruitment and retention in IT-related positions.

Research as shown there is an IT manpower gap – and this was well before the pandemic which has only exacerbated the situation. Making matters worse is the fact as the economy recovers many IT professionals are leaving local government for higher paying jobs in the private sector. Any incentives that would keep qualified IT professionals in place would be welcomed.

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 than12 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.

Concluding remarks

In preparing my remarks many different ideas came to mind that did not necessarily fit with the 5 areas I had identified. I present them in list form in hopes that it may elicit further thoughts and possibly action:

Recommended Solutions

• More direct aid to localities.

• Renewed effort to sync all the various rules and regulations often in conflict with one another.

• More and enhanced state government partnerships.

• Seek and demonstrate regional approaches to infrastructure sharing..

• Greater curation of available tools from federal agencies including HHS.

• Greater use of the National Guard to assist localities in Cybersecurity.

• Consider guidelines and standards for technology competencies and infrastructure.

• Consider a cyber audit process.

• Improved coordination of funding sources within the federal government.

• Encourage/subsidize professional development and certifications.

I applaud this subcommittee for providing the leadership in conducting this hearing and the ensuing discussion. It has been said that a tragedy is a terrible thing to waste, and I believe we can all agree that this is an opportune time to reflect on the recent past of what were the lessons learned stemming from the pandemic and more importantly how can we best prepare for the future.