WRITTEN TESTIMONY

OF

DOUG ROBINSON

EXECUTIVE DIRECTOR

OF

THE NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO)

FOR A HEARING ON:

CATALYST FOR CHANGE: STATE AND LOCAL IT AFTER THE PANDEMIC

BEFORE THE:

U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON OVERSIGHT AND REFORM

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

Wednesday, June 30, 2021

Washington, D.C.

Introduction

Thank you, Chairman Connolly, Ranking Member Hice and the distinguished members of the Subcommittee for inviting me today to speak on the numerous information technology (IT) challenges facing state government that have been amplified during the COVID-19 pandemic. As Executive Director of the National Association of State Chief Information Officers (NASCIO), I am grateful for the opportunity to provide an overview of the IT landscape in state government, highlight the critical role state IT agencies have played throughout the current public health crisis and discuss specific areas where the federal government can best assist their state and local counterparts as they look to enhance digital government services and advance IT modernization initiatives. I also want to stress that any discussion concerning IT modernization needs to include an enhancement of cybersecurity. IT modernization and cybersecurity are inextricably linked and cannot be viewed as separate issues.

NASCIO is a nonprofit, 501(c)(3) association representing state chief information officers (CIOs), state chief information security officers (CISOs) and IT executives and managers from the states, territories, and the District of Columbia. State CIOs are governor-appointed, executive branch officials who serve as business leaders and advisors of IT policy and implementation within their state. The state CIO's roles and responsibilities may vary from state to state, yet all CIOs share the common function of setting and implementing a state's IT policy. As the Executive Director of NASCIO since 2004, I am humbled to represent our members here today, as well as provide data from our recent and in-progress national surveys.

State Governments Remain at Risk

Based on the 2020 Deloitte-NASCIO Cybersecurity Study, states experienced elevated security threats during pandemic. This is not surprising given the need to protect state systems delivering unprecedented levels of online services and distribution of the state workforce to remote settings. For state CIOs, cybersecurity has long been an enterprise imperative and has been their top-ranked priority for the last eight years. During the last decade, there have been three consistent themes facing the states: inadequate cyber funding given the risks to the continuity of government, increasing sophistication of the cyber threats and the challenge of recruiting and retaining cybersecurity professionals. Moving forward, state CIOs expect to focus on promoting an enterprise cybersecurity model, whole-of-state collaboration, the adoption of a zero trust architecture and the need for improved fraud detection capabilities.

Lessons learned from COVID-19

There is no doubt COVID-19 served as the forcing mechanism for states to rapidly invest in short-term technology improvements and automation to ensure the continuity of

government in a largely remote environment. Yet, as the worst of the deadly pandemic appears behind us, we are currently at a crossroads as to whether the technology and business practice lessons learned over the past fifteen months are here to stay or were just short-term stopgaps. From countless conversations with state IT leaders and as evidenced in our recent surveys, state CIOs overwhelmingly believe it is time for state governments to invest significantly in IT modernization initiatives, including legacy modernization, to deliver improved digital services to citizens. In our view, this must be coupled with investments in cybersecurity, which only 36 percent of states currently fund as a line item in their budget.

While the vast majority of governments—at all levels—have been slow to make to investments in IT transformation and modernization, the demand and expectation among citizens to improve digital services has only increased during the pandemic. Citizens want and expect an Amazon.com consumer experience when interacting with their state government to renew their driver's license or file an unemployment claim. From the perspective of state and local governments, the pandemic was a clear example that there is a long way to go in their ability to deliver this type of experience.

Top issues and priorities for state CIOs in a post COVID-19 world

While improving digital services and legacy modernization initiatives have been a top priority for state CIOs for the past few years, COVID-19 was the catalyst to drastically expedite many of these efforts in an unprecedented manner. When asked to rank their business processes, practices, or investments after COVID, state CIOs identified the following five priorities:

1. **Increased attention on digital government services and improved citizen experience.** States have expanded digital services and are focused on a better online experience for citizens. Targets of opportunity include streamlining services, user centric design, stronger security, more automation and digital identity services. Preliminary data from our ongoing survey found 94 percent of CIOs report that the demand for digital services has increased and accelerated.

2. **Expanded work from home/remote work options.** At the outset of the pandemic, state CIOs faced enormous challenges to ensure widespread remote work was manageable and secure. This was made even more difficult in states that did not have a culture of remote work. Working with private sector partners, state CIOs adapted to a nearly universal remote environment almost overnight. Because of the increased vulnerability of the state network and end user devices, cybersecurity investments were a critical element of this transformation.

3. **Expanded use of collaboration platforms.** With widespread and mandated remote work requirements for employees, states were compelled to adopt virtual

meeting platforms for collaboration and engagement. Video conferencing and streaming technologies became the norm, especially for public meetings with citizens and stakeholders. Demonstrating both efficiency and enhanced productivity, state CIOs predict continued and expanded use.

4. **Investments in broadband expansion and adoption.** Broadband services were certainly strained during the pandemic and found to be inadequate in many cases. From supporting remote work solutions to providing education and healthcare opportunities for their citizens, state CIOs know that they need an expansive and reliable broadband network to make these needs accessible and successful. The pandemic only heightened those needs, which is why 81 percent of our survey respondents said that their states will now accelerate the implementation of their broadband strategies.

5. **Increased investments in legacy modernization.** The overwhelming demand for citizen services during the pandemic exposed the fragility of aging state systems. Many of the most significant and critical services were hampered by technology platforms that were not flexible, adaptable and scalable. Based on our preliminary 2021 survey data, half the states have accelerated modernization initiatives with a greater focus on online citizen services. The state CIOs report the near future priorities for capital IT modernization investments will be in human services, administration/finance, labor/employment, health services and licensing/permits.

In addition, expansion of cloud services, Software-as-a-Service (SaaS) deployment and accelerated use of data analytics were highly ranked. States are certainly moving more services to the cloud and 89 percent of the CIOs intend to expand SaaS adoption over the next three years.

State government IT environment today

Today, more than ever, IT has a significant impact on how citizens live, communicate and interact with government agencies. IT has become a part of the fabric of state government, supporting the mission and business of agencies and enabling innovative services and facilitating the transformation of government functions. The business of IT is a serious undertaking in the states. Collectively, state and local governments are expected to spend an estimated $100 billion or more on IT this year. Thousands of critical projects will be undertaken. Many large, complex systems delivering critical state government programs are funded by the federal government.

This last point cannot be stressed enough as states are charged by the federal government to be the primary agents to deliver critical programs and services to citizens across the country. These programs and services touch nearly every facet of our lives including

human services, health care, public education, nutrition, housing, community development, childcare, job training and transportation. As many of the IT systems supporting these programs are built upon legacy and outdated technologies, they remain susceptible to debilitating cyber-attacks and an overall inability to ensure the reliable delivery of services in a timely and secure manner.

In response to the pandemic, citizen expectations and the fiscal realities in the states, governors across the country are currently focused on delivering critical state services, streamlining government operations and reducing costs. IT is contributing significantly to this effort by bringing to state government the tools to realize economies and efficiencies of scale in procurement, achieve interoperability of systems, eliminate redundant and duplicative processes and improve data-sharing capabilities.

IT modernization challenges

All state CIOs aspire to have a "modern" IT environment. States maintain and operate a wide variety of IT systems that represent a high degree of diversity and complexity. The challenges are similar across all government entities: proprietary platforms that can no longer support the business of government, increasing costs of hardware and software maintenance, lack of skilled IT personnel for legacy environments and difficulties modernizing a complex system while supporting operation of the existing system.

Along with this technical debt, state agencies also face financial and organizational impediments. State CIOs and their agency partners are often unable to get sustained funding for modernization for the necessary multi-year time horizon. Any IT modernization initiative requires a strong partnership between the state CIO and agency business partner. In NASCIO's view, without collaboration, regular communication and skilled project management capabilities, these projects fail to deliver the desired outcomes.

Business alignment including robust project governance and organizational change management are also critical components to any modernization effort. Agency business processes are tied to the legacy system, so these initiatives often require major business process redesign before project initiation. With these changes, leaders often confront the organizational or cultural resistance to the new way of doing business.

Federal-State collaboration to enhance IT modernization initiatives

> **Broadband Expansion:** As discussed earlier in this testimony, the importance of secure, reliable and affordable connectivity cannot be understated. While broadband expansion, and expansion of networks to rural and underserved areas of the country, has been a significant priority in recent COVID-19 relief legislation, there are still nearly 18.5 million Americans who lack even basic access to broadband. As Congress and the Biden Administration debate infrastructure legislation, NASCIO strongly urges improvements to our digital infrastructure.

Accessible broadband is the most fundamentally important tenet of any IT modernization strategy. Accessibility and affordability in rural and disadvantaged communities should be the highest priority, and these efforts should not stop at simply providing coverage but establish speed goals of at least 100 Mbps download, 20 Mbps upload. Congress and the Federal Communications Commission (FCC) should increase and enhance state-federal partnerships to resolve the numerous challenges associated with broadband expansion in rural and low-income areas across the country. These challenges include lack of economic incentive for internet providers and lack of competition that keep broadband prices too high.

Congress and the FCC should also look to leverage broadband mapping strategies that have been deployed in state broadband offices, including Georgia's Broadband Deployment Initiative, to challenge and amend the FCC's broadband data collection processes. A more accurate mapping process will result in improved tools to inform citizens and measure the progress of broadband programs. The post-pandemic world will run on a more robust digital economy and expanded hybrid and remote work environments that demand greater bandwidth.

State and Local IT Modernization Grant Program:
In the 116th Congress, NASCIO endorsed the *State and Local IT Modernization and Cybersecurity Act*, bipartisan legislation introduced by Congressmen James Langevin (D-RI) and Mike Gallagher (R-WI). The legislation, which was a result of the recommendations from the Cyberspace Solarium Commission, sought to establish a grant program for state and local governments to modernize their IT infrastructure to modern, secure platforms, including cloud-based services.

Importantly, the legislation aimed to create a Modernizing Information Technology Program to support migration of legacy systems to new, secure platforms in line with state IT modernization strategies reviewed by the Cybersecurity and Infrastructure Security Agency (CISA). While federal funding was an important aspect of the proposal, the *State and Local IT Modernization and Cybersecurity Act* would have established key security frameworks, provided technical assistance and ensured Congressional and CISA oversight as state and local governments implemented IT modernization strategies.

Harmonization of Federal Cybersecurity Regulations:
As state governments continue to implement strategies to improve their IT systems and infrastructure, they are simultaneously looking to achieve cost savings and improve their overall cybersecurity posture. One area of opportunity for the federal government to assist state governments in their modernization strategy is the further harmonization of federal cybersecurity regulations. NASCIO greatly

appreciates the bipartisan work of numerous members of this Subcommittee who tasked the Government Accountability Office (GAO) in 2018 to study this issue and issue corresponding recommendations.

As you may know, 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 addition to various federal regulations, state CIOs are also pushed to adopt other standards and frameworks that federal grants necessitate.

State CIOs invest an inordinate amount of time identifying duplicative regulatory mandates or their differences, participating in federal audits, and responding to inconsistent audit findings. These challenges in and of themselves are not unmanageable; the real issue is that they can and have impeded efforts of state CIOs to introduce efficiencies and generate savings for taxpayers.

In fact, the May 2020 GAO report, "Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States," 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.

Congress should empower the Office of Management and Budget (OMB) to mandate collaboration among federal agencies on the development and implementation of cybersecurity regulations. As Congress considers reforms to the *Federal Information Security Management Act of 2002*, NASCIO encourages the inclusion of provisions to allow for the streamlining of federal agencies cybersecurity requirements. These reforms would not only burdensome and redundant regulations and provide significant cost savings for state IT agencies but also enhance security frameworks as states implement various IT modernization initiatives.

Closing

Chairman Connolly, Ranking Member Hice and the distinguished members of the Subcommittee, thank you again for the opportunity to testify today. I look forward to answering any questions you may have.