WRITTEN TESTIMONY

OF

DENIS GOULET

COMMISSIONER OF THE DEPARTMENT OF INFORMATION TECHNOLOGY

STATE OF NEW HAMPSHIRE

AND

PRESIDENT OF THE NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO)

FOR A HEARING ON

"STATE AND LOCAL CYBERSECURITY: DEFENDING OUR COMMUNITIES FROM CYBER THREATS AMID COVID-19"

BEFORE THE

UNITED STATES SENATE

FEDERAL SPENDING OVERSIGHT AND EMERGENCY MANAGEMENT SUBCOMMITTEE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

Wednesday, December 2, 2020

Washington, D.C.

Thank you, Chairman Paul, Ranking Member Hassan and the distinguished members of the Subcommittee for inviting me today to speak on the numerous cybersecurity challenges facing state government that have been amplified during the COVID-19 pandemic. As Commissioner for the Department of Information Technology in New Hampshire and the President of the National Association of State Chief Information Officers (NASCIO), I am grateful for the opportunity to discuss cybersecurity, as well as highlight the vital role that state information technology (IT) agencies have played in providing critical citizen services and ensuring the continuity of government throughout this current public health crisis.

State Cybersecurity Overview and Challenges

As President of NASCIO, I am extremely honored to represent my fellow state chief information officers (CIOs) and other state IT agency leaders from around the country here today. While some of my testimony will be based on my experiences as CIO in New Hampshire for over the past five years, I will also be providing the members and staff of the Subcommittee with national trends and data from NASCIO's recently completed 2020 State CIO Survey and the 2020 Deloitte-NASCIO Cybersecurity Study.

It may come as little surprise to you that cybersecurity has remained the top priority for state CIOs for the past seven years. There is certainly growing recognition at all levels of government that cybersecurity is no longer an IT issue; it is a business risk that impacts the daily functioning of our society and economy, as well as a potential threat to our nation's security. The threat environment we face is incredibly daunting with state cyber defenses repelling between 50 and 100 million potentially malicious probes and actions every day. State and local governments remain attractive targets for cyber-attacks as evidenced by dozens of high-profile and debilitating ransomware incidents. The financial cost of these attacks is truly staggering with a recent report from EMSISOFT finding that ransomware attacks in 2019 impacted more than 960 government agencies, educational institutions and healthcare providers at a cost of more than $7.5 billion.

Inadequate resources for cybersecurity has been the most significant challenge facing state and local governments, even prior to the COVID-19 pandemic. The question of why the federal government should be contributing to cybersecurity of the states is straightforward as states are the primary agents for the delivery of a vast array of federal programs and services. I do want to point out that a large majority of state CIO agencies operate on a cost recovery or chargeback model, whereby they bill state agencies for services provided. While this model has its own challenges, half of the states and territories currently lack a dedicated cybersecurity budget and more than a third have seen no growth or a reduction in those budgets. According to our recent national survey, state cybersecurity budgets are typically less than 3 percent of their overall IT budget.

As state CIOs are tasked with additional responsibilities, including providing cybersecurity assistance to local governments, they are asked to do so with shortages in both funding and

cyber talent. Only half of all states have a dedicated cybersecurity budget line item while federal government agencies report cybersecurity funding in the president's budget as a portion of their overall IT spending. This is marginal compared to private industry cybersecurity budgets.

NASCIO has long encouraged state government officials to establish a dedicated budget line item for cybersecurity as subset of the overall technology budget. While the percentage of state IT spending on cybersecurity may be much lower than that of private sector industry and federal agency enterprises of similar size, the line item can help state IT leaders provide the state legislature and executive branch leaders the right level of visibility into state cybersecurity expenses in an effort to rationalize spending and raise funding levels. State legislation could demand visibility into cyber budgets at both the state and individual agency levels. In addition, the Deloitte-NASCIO Cybersecurity study results indicate that federal and state cybersecurity mandates, legislation, and standards with funding assistance result in more significant progress than those that remain unfunded.

A Whole-of-State Approach

More than 90 percent of CIOs are responsible for their state's cybersecurity posture and policies. In collaboration with their chief information security officers (CISOs), whose role has expanded and matured in recent years, CIOs have taken numerous initiatives to enhance the status of the cybersecurity program and environment in their states. I believe these initiatives are also fundamentally crucial as Congress considers the implementation of a cybersecurity grant program for state and local governments. Some of these include: the adoption of a cybersecurity strategic plan, the adoption of a cybersecurity framework based on the NIST Cybersecurity Framework, the development of a cyber disruption response plan, obtaining cyber insurance and the development of security awareness training for employees and contractors.

One key initiative is the whole-of-state approach to cybersecurity, which NASCIO has advocated for the past decade. We define the whole-of-state approach to cybersecurity as collaboration among state agencies and federal agencies, local governments, the National Guard, education (K-12 and higher education), utilities, private companies, healthcare and other sectors. By approaching cybersecurity as a team sport, information is widely shared and each stakeholder has a clearly defined role to play when an incident occurs. Additionally, many states who have adopted the whole-of-state approach have created statewide incident response plans.

Crucially, numerous state IT agencies are conducting cyber incident training and incident response exercises with these partners to ensure the ability to quickly operationalize their incident response plans. According to our recent CIO survey, more than 65 percent of state CIOs are either in the process of implementing a whole-of-state approach or have implemented one in their states.

In August 2019, more than two dozen local governments, education institutions and critical infrastructure systems in Texas were struck by debilitating and coordinated ransomware attacks. However, it was the successful collaboration and cooperation among federal, state and local officials – a whole-of-state approach combined with a detailed cyber incident response plan – that prevented these attacks from succeeding. In fact, as Amanda Crawford, Executive Director of the Texas Department of Information Resources (DIR), testified before the Senate Homeland Security and Governmental Affairs Committee in February 2020, all impacted entities were remediated within one week after the attacks.

State and Local Collaboration

As the Texas ransomware attacks illustrate, under-resourced and under-staffed local governments continue to remain an easy target for cyber-attacks. Due to the combination of a whole-of-state approach to cybersecurity and the proliferation of numerous high-profile ransomware attacks across the country, state CIOs have significantly increased collaboration with local governments to enhance their cybersecurity posture and resilience. More than 76 percent of CIOs reported increased collaboration and communication with local governments in the last year.

Earlier this year, NASCIO released a research paper with the National Governors Association (NGA) focused on state and local collaboration titled "Stronger Together." As Congress considers the components of a state and local cybersecurity grant program, I would urge you to incorporate some of the conclusions from that paper. This includes encouraging states to continue building relationships with local governments and helping states raise awareness for IT and cybersecurity services offered to local governments. Additionally, Congress should assist state and local governments with more easily purchasing cybersecurity tools and services through existing models at the federal level. Streamlining the procurement of cybersecurity services would also expedite a currently bureaucratic process and result in significant cost savings.

Partnership with DHS CISA

In terms of partnerships with federal agencies, I do want to highlight state IT's growing partnership with the DHS CISA. While this relationship is still in its infancy, CIOs and CISOs appreciate the resources provided to state and local governments by CISA in the wake of cyber attacks. NASCIO has supported efforts to more clearly define CISA's roles and responsibilities in assisting state and local governments and has endorsed federal legislation to increase CISA's resources within each state.

In January 2020, NASCIO endorsed **S. 3207, the Cybersecurity State Coordinator Act of 2020**, introduced by Ranking Member Hassan, which would be a major asset to state and national cybersecurity efforts by ensuring greater continuity between the efforts of states and the Federal Government. It would also provide a stronger state voice within CISA, helping them to better tailor their assistance to states and localities.

Supported Federal Legislation

I would like to reiterate my appreciation to this subcommittee for its attention to cybersecurity issues impacting state and local governments. The 116th Congress certainly has focused significantly on these issues and introduced legislation endorsed by NASCIO. If passed, these bills would greatly improve the cybersecurity posture for state and local governments by creating new, dedicated funding streams.

As you may know, cybersecurity spending within existing federal grant programs, including the Homeland Security Grant Program, has proven challenging in the face of declining federal allocations, increased allowable uses and a strong desire to maintain existing capabilities that states have spent years building. In fact, less than four percent of all Homeland Security Grant Program funding has been allocated to cybersecurity over the last decade.

These proposed cyber grant programs through legislation introduced during the 116th would provide vital resources for state IT agencies that would prevent my fellow CIOs and I from having to compete against other agencies and states. Ultimately, a specific cybersecurity grant program would allow us to better assist our local government partners and thwart well-funded nation-states and criminal actors that continue to grow in sophistication.

NASCIO supports **S. 1846**, **the State and Local Government Cybersecurity Act**, which would help states access resources, tools, and expertise developed by our Federal partners and national cybersecurity experts. This includes making available to state and local governments the experts at the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCIC) for training and consulting. It would also afford these organizations with greater access to security tools, policies, and procedures to help drive vital improvements.

Additionally, NASCIO worked closely with bipartisan members of the House Committee on Homeland Security on the introduction of **H.R. 5823**, **the State and Local Cybersecurity Improvement Act**, a $400 million annual grant program for state and local governments to strengthen their cybersecurity posture. H.R. 5823 would require grant recipients to have comprehensive cybersecurity plans and emphasizes significant collaboration between DHS Cybersecurity and Infrastructure Security Agency (CISA) and state and local governments.

NASCIO also urges Congress to pass **S. 2749**, **the DOTGOV Act**, which would go a long way in providing greater security assurance for state and local government websites. Nearly twenty years after making the .gov domain available to state and local governments, the vast majority of local governments are still not taking advantage of this trusted domain. As of today, there are only approximately 8.5 percent of all eligible local governments on .gov, allowing cyber criminals to spoof websites and further wage misinformation and disinformation campaigns.

The DOTGOV Act seeks to ease the process for these governments to obtain .gov domain names, providing the sites themselves with greater security and offering greater assurances to

residents that they are, in fact, looking at a government website. The bill also charges DHS with providing information to make the transition to the .gov domain easier and allows the Director of CISA to waive fees related to .gov registration.

Conclusion

For more than the past eight months, the COVID-19 pandemic has clearly exacerbated the cybersecurity challenges for state IT agencies. In response to the pandemic, state CIOs and their teams quickly provided a secure remote work environment for more than 90 percent of state employees. Since March, my colleagues and I have rapidly implemented policies on how state employees should use personal devices, patch their systems and ultimately, how to conduct telework safely in this new environment. We have also assisted numerous state agencies to help them improve their technological capabilities and quickly deliver critical services to citizens, including unemployment insurance.

In New Hampshire, I have worked closely with our public health agencies to ensure they have the necessary digital tools for them to improve capabilities in the areas of testing, contact tracing, case management and personal protective equipment (PPE) inventory.

My colleagues and I at the Department of Information Technology have been honored to play a role in fighting COVID-19 in New Hampshire. We have taken on additional responsibilities and incurred new expenses while continuing to face an unrelenting cybersecurity threat environment. I am truly concerned about how crucial IT and cybersecurity initiatives will remain funded in the coming months and years. We all know that states have seen significant declines in revenue and will be forced to make difficult budgetary decisions in the coming years.

As President of NASCIO, I know I speak for all of my colleagues around that country that a federally funded cybersecurity grant program for state and local governments is long overdue. There can be no doubt that state governments need to change their behavior and begin providing consistent and dedicated funding for cybersecurity moving forward. It is my hope that the states will follow the lead of the federal government in this area, especially if grant programs require them to match a portion of federal funds. I look forward to continuing to work with the members of this subcommittee in the creation of a grant program to improve the cybersecurity posture for our states and local governments.