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

RESPONDING TO RANSOMWARE: EXPLORING POLICY SOLUTIONS TO A CYBERSECURITY CRISIS

BEFORE THE

CYBERSECURITY, INFRASTRUCTURE PROTECTION, & INNOVATION SUBCOMMITTEE

COMMITTEE ON HOMELAND SECURITY

Wednesday, May 5, 2021

Washington, D.C.

Thank you, Chairwoman Clarke, Ranking Member Garbarino 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, efforts to mitigate ransomware attacks, 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 the current public health crisis.

State Cybersecurity Overview and Challenges

As President of NASCIO, I am 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 the past six years, I will also be providing the members and staff of the subcommittee with national trends and data from NASCIO's 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 eight years. In my state and across the country, I have seen a palpable shift among government leadership that IT and cybersecurity are not simply regarded as a technology problem but a key tenet to the continuity of our government. While we used to be concerned only with the theft of data and personally identifiable information (PII), the nature and scope of cyber attacks today are aimed at crippling the entire functioning of our government. Recent attacks on water treatment facilities and hospital systems have shown us how these incidents have progressed from digital consequences to sophisticated strikes designed to threaten the health and safety of our nation's citizens.

The threat environment we face is incredibly daunting with state cyber defenses repelling an estimated 50 to 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.

Lack of adequate resources for cybersecurity has been the most significant challenge facing state and local governments, even prior to the COVID-19 pandemic. 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.

The question of why the federal government should be contributing to the cybersecurity of the states is straightforward as states are the primary agents for the delivery of a vast array of federal programs and services. A lack of budgeting at the state level for cybersecurity is also a significant impediment. The 2020 Deloitte-NASCIO Cybersecurity Study found that only 36 percent of states and territories have a dedicated cybersecurity budget and nearly a third have seen no growth in those budgets. The study also found that state cybersecurity budgets are typically less than three percent of their overall IT budget, which is far less than federal agencies and financial institutions.

NASCIO has long encouraged state government officials to establish a dedicated budget line item for cybersecurity as a 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. While we still have a long way to go, I greatly appreciate legislative efforts by numerous members of this subcommittee to encourage state legislators to begin budgeting for cybersecurity.

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 key tenets include: a centralized approach to cybersecurity, the adoption of a cybersecurity strategic plan and framework based on the NIST Cybersecurity Framework, the development of a cyber disruption response plan and the implementation of regular security awareness training for employees and contractors.

One key initiative is the whole-of-state approach to cybersecurity, which NASCIO has advocated for over 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. According to our 2020 CIO survey, more than 79 percent of state CIOs have implemented a whole-of-state approach in their states, are in the process of implementing or planning to implement.

Crucially, numerous state IT agencies are conducting cyber incident training and incident response exercises with these partners to ensure they are able to quickly operationalize their incident response plans. One example of this type of training is the inaugural State-wide Cyber Summit for Local Governments that we held in New Hampshire earlier this spring. We had over 250 local government attendees from towns, cities, counties and school districts with federal participants from CISA and the Secret Service. Regular cyber exercises not only increase cyber awareness across all levels of the state but foster key relationships and trust among officials allowing for a more successful and rapid response when an incident occurs.

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, Texas CIO and Executive Director of the Texas Department of Information Resources, 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. In fact, more than 76 percent of CIOs reported increased collaboration and communication with local governments in the last year.

In 2020, NASCIO released a research paper with the National Governors Association 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 Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). While this relationship is still in its infancy, CIOs and CISOs appreciate the cybersecurity resources, services and guidance provided by CISA. NASCIO has and will continue to support efforts to define CISA's roles and responsibilities more clearly in assisting state and local governments. We've also endorsed federal legislation to increase CISA's resources within each state. This includes the recent passage and enactment of **S. 3207, the Cybersecurity State Coordinator Act**, which will ensure greater continuity between the efforts of states and the federal government. It will also provide a stronger state voice within CISA, helping them to better tailor their assistance to states and localities.

Additionally, NASCIO was a strong advocate of the **DOTGOV Act**, which was included in the omnibus government funding bill signed into law in December 2020. The DotGov Act transferred ownership of the DotGov Program from the General Services Administration to CISA, which officially took place last month, and reinforced the important cybersecurity aspect of domain registration. I want to praise CISA and the DotGov Office for their announcement last week to waive all fees for new DotGov registrations. The $400 annual fee had been a significant barrier of adoption for local governments, who remain most vulnerable to misinformation and disinformation campaigns. With less than 10 percent of all eligible local governments currently on DotGov, NASCIO looks forward to continuing our work with CISA to

better improve the cybersecurity of local governments. Now more than ever, it is essential to ensure the American people are receiving accurate and authoritative information from their government websites.

Dedicated Cybersecurity Funding for State and Local Governments

I would again like to reiterate my appreciation to this subcommittee for its attention to cybersecurity issues impacting state and local governments. The 116th Congress focused significantly on these issues and introduced numerous pieces of legislation endorsed by NASCIO. In particular, I look forward to continuing to work with the members of this subcommittee to ensure the passage of a state and local cybersecurity grant program.

Currently, 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.

NASCIO urges the reintroduction and passage of the bipartisan **State and Local Cybersecurity Improvement Act**, a $400 million annual grant program for state and local governments to strengthen their cybersecurity posture. This legislation would require grant recipients to have comprehensive cybersecurity plans and emphasizes significant collaboration between CISA and state and local governments. The legislation would also allow state and local governments to make investments in fraud detection technologies, identity and access management technologies and implement advanced cybersecurity frameworks like zero trust. We would also be able to invest in cloud-based security services that continuously monitor vulnerabilities of servers, networks and physical networking devices.

Passage of the **State and Local Cybersecurity Improvement Act** would provide vital resources for state IT agencies, meaning my fellow CIOs and I would not have to compete against other agencies and states. Ultimately, a specific cybersecurity grant program would allow us to better assist our local government partners and address threats from well-funded nation-states and criminal actors that continue to grow in sophistication. As I mentioned earlier in my testimony, NASCIO also supports provisions within this legislation that would ensure state governments are budgeting for cybersecurity.

We also greatly appreciate the recent passage of the American Rescue Plan Act (ARP), which includes $350 billion in flexible aid to state and local governments. While we await guidance from the Department of the Treasury on allowable expenditures, I believe the ARP will create significant resources for states to invest in legacy modernization, cybersecurity improvements and broadband expansion over the next three years.

Conclusion

When COVID-19 spread across the country last March, my fellow state CIOs and I 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 our private sector partners, we adapted to a nearly universal remote environment almost overnight.

We expedited lengthy, bureaucratic acquisition processes, deployed AI-powered chatbots to assist overburdened state agencies and assisted school districts with virtual learning. We implemented

numerous digital government initiatives to improve how citizens interact with their state government websites, a crucially important project as citizens relied more than ever on state services and authoritative information sources.

CIOs also implemented COVID-19 testing websites, contact and exposure notification applications and now, vaccine websites.

In New Hampshire, we have taken numerous measures to improve the cybersecurity posture of our entire state – including with the education and health care sectors. New Hampshire recently passed legislation that mandated the establishment of "Minimum Standards for the Privacy and Security of Student and Employment Data." Through a cooperation with the state, our schools have established a Student Data Privacy Agreement, which participating districts ask vendors to sign, in order to comply with the "Minimum Standards." We've also furthered our partnership between the state CISO and the New Hampshire Chief Technical Officer Council on issues relating to cybersecurity and privacy.

On the healthcare front, the New Hampshire Information and Analysis Center routinely distributes cybersecurity alerts and advisories to healthcare entities within New Hampshire from the state and federal government. A recent debilitating ransomware attack on a hospital system in a neighboring state was also a real awakening for many hospital operators in New Hampshire. It helped them to understand that ransomware can have a profoundly destructive impact on their ability to operate and treat patients, as well as understand that a centralized approach to cybersecurity is superior to the more decentralized and permissive approach employed by some organizations.

In closing, as President of NASCIO, I know I speak for all 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.