NASCIO

Representing Chief Information Officers of the States

Statement before the Committee on Homeland Security

Joint Hearing of the

Subcommittee on Emergency Preparedness, Response, and Communications and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

"Enhancing Preparedness and Response Capabilities to Address Cyber Threats"

Testimony of Mark Raymond

Vice President, National Association of State Chief Information Officers (NASCIO)
Chief Information Officer, Bureau of Enterprise Systems and Technology,
Department of Administrative Services, State of Connecticut
May 24, 2016

Thank you Chairmen Ratcliffe and Donovan and Ranking Members Payne and Richmond for inviting me to testify before you today.

My name is Mark Raymond and I serve as the chief information officer (CIO) for the State of Connecticut and also as the vice president of the National Association of State Chief Information Officers (NASCIO). At NASCIO, I also co-chair the cybersecurity committee. NASCIO is a nonprofit, 501(c)(3) association representing state chief information officers and information technology executives and managers from the states, territories, and the District of Columbia.

Today, I would like to provide the committee an overview of the status of cybersecurity preparedness in the states, what states are doing to improve and enhance resilience to cyber attacks, and opportunities to enhance the security profile of our nation.

State chief information officers are state executive branch officials who serve as business leaders and advisors of information technology policy and implementation at the state level. All states have a CIO and all CIOs serve within the executive branch of state government. The office of the state CIO takes many forms, some are cabinet officials and others are executive directors; regardless of the title, all state CIOs share a common function of setting and implementing a state's IT policy.

State CIOs are also responsible for providing IT services to state executive branch agencies. This not only includes the more typical business of provisioning enterprise data or phone services but also securing the digital business of state government. The most critical role today for the CIO includes the security of state networks, protection of state data, and helping formulate the response for a cyber incident or disruption. These responsibilities are shared with the chief information security officer (CISO), a position that exists among all fifty states and duties for whom are becoming increasingly standardized.

State CIOs and CISOs operate in an increasingly challenging environment. In the *2014 Deloitte-NASCIO Cybersecurity Study, State governments at risk: Time to move forward*, (2014 Deloitte-NASCIO Study), we studied the current cybersecurity environment in the states, common challenges, and barriers to a strong state cybersecurity posture. The *2014 Deloitte-NASCIO Study* showed that the top barriers to states addressing cybersecurity were insufficient budgets, increased sophistication of threats, and the inadequate availability of security professionals. These challenges remained the same in 2015.

Insufficient budgets for cybersecurity have been cited as a top barrier since the inception of the Deloitte-NASCIO Cybersecurity Study in 2010. The majority of states spend in the range of 1-2 percent of their overall IT budget on cybersecurity. The federal government spends around 14-16 percent of their IT budget on cybersecurity. Combined with recent events, this disparity shows that there is no one correct amount or percentage; states must assess their cybersecurity risk and spend commensurate with that risk.

Funding challenges also affect the ability of states to hire and retain skilled IT security personnel. NASCIO's *State IT Workforce: Facing Reality with Innovation* survey shows that a shortage in the state IT workforce has been predicted for some time and states are finding that those with IT security skills are the most difficult to recruit and retain (67.3%) followed by application development, programming and support (57.1%); and architecture (55.1%). 92 percent of respondents reported that salary rates and pay structures are a challenge in bringing on top IT talent. States are responding to the dearth of qualified IT security personnel by getting innovative.

In Maine, state CIO Jim Smith confronted the reality that 24 percent of his 480 state IT workers would be eligible to retire in the next two years thus highlighting the need to recruit and retain new IT talent. He has addressed one aspect of the workforce issue by updating the application process, moving it online, and making it mobile friendly. He has also created an IT intern program and over 70 percent of those interns have become full time employees. High school students are also welcome to visit Maine's Office of Information Technology for its annual "Technight," where students participate in a variety of tech-related activities, which introduces them to exciting IT careers.

While insufficient budgets and workforce shortages continue to be obstacles for state CISOs, three out of five also reported that the increasing sophistication of threats was also a major barrier to addressing cybersecurity. In the *2014 Deloitte-NASCIO Study*, CISOs reported their top three cyber concerns: malicious code (74.5%), hacktivism (53.2 %), and zero-day attacks (42.6%). Malicious cyber activity happens daily in state government, but state CIOs have been able to better prepare for known threats through information sharing, a concept with which emergency managers are acutely aware.

Despite these challenges, states are progressing toward a more secure cyber environment. NASCIO has long called for states to adopt a cybersecurity framework and quickly endorsed the National Institute of Science and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework) upon its release in February, 2014. In the *2014 Deloitte-NASCIO Study*, we found that 88 percent of states were reviewing or planning to leverage the *NIST Cybersecurity Framework* within the year. In the NASCIO, Grant Thornton, CompTIA *2015 State CIO Survey, The Value Equation: Agility in Sourcing, Software and Services*, we found that 80 percent of states had adopted a cybersecurity framework based on national standards and guidelines.

States are adapting to shared cybersecurity challenges and utilizing public and private resources to enhance their cybersecurity posture both in times of relative rest and in times of emergency. The *NIST Cybersecurity Framework* identifies five basic functions: identify, protect, detect, respond, and recover. States are making progress in each of these areas.

To better identify and detect cyber threats to protect a wealth of state digital assets, states are increasingly sharing threat information through established forums like fusions centers and the Multi State-Information Sharing and Analysis Center (MS-ISAC). From the *2015 State CIO Survey*, we know that 80 percent of states have established trusted partnerships for information sharing and response. Additionally, 80 percent of states have also acquired and implemented continuous vulnerability monitoring capabilities in order to better identify and detect malicious cyber activity. Knowing that the ability to identify and detect are our first line of defense, NASCIO has called on states to invest in advanced cyber analytics as a part of the practice of business intelligence and recently published, "*Advanced Cyber Analytics: Risk Intelligence for State Government*." To that end, Connecticut is the first state to take advantage of DHS' threat intelligence offering provided via iSight Partners. Many states also participate in ALBERT, a joint program between MS-ISAC and DHS which brings an EINSTEIN-based, cyber-traffic monitoring system to the states.

In my state, in addition to participating in the information sharing through MS-ISAC and utilizing ALBERT, Emergency Management Deputy Commissioner and state Homeland Security Advisor, William Shea, and I co-chair a cybersecurity task force whose membership includes a diverse mix of stakeholders including higher education, law enforcement, public utilities, private businesses and others. We meet regularly to discuss the latest threat and vulnerability information because we know that information sharing is key to cultivating a culture of information security and is a best practice to which states should conform.

In the realm of response and recovery, states are also showing maturity. State CIOs are expected to play a role in helping state governments respond to and recover from natural and manmade disasters. According to the *2015 State CIO Survey*, the top three functions for which state CIOs were responsible are maintaining a robust, reliable, and secure infrastructure; coordinating with other state officials; and restoring communications services.

When riots broke out in and Baltimore, Maryland, Governor Larry Hogan declared a state of emergency. Maryland's CIO organization, led by Secretary of Information Technology David Garcia, assisted with the swift deployment of "Maryland First Responders Interoperable Radio System Team (FIRST)," the statewide radio communications equipment for first responders and stood up a website, "Maryland Unites" to which state and local leaders could direct members of the affected community. They also worked with public and private partners to reverse engineer Anonymous' attack on state networks. Information sharing was also helpful; officials in Missouri shared their experience with Maryland as they had faced a similar crisis. In ways like these, state CIOs are showing maturity in response in both the cybersecurity and emergency management fronts and especially when those two worlds collide.

Recognizing that states could face a catastrophic emergency event that coincides with or is caused by a cybersecurity event, NASCIO has called on states to develop a cyber disruption plan and recently released the "*Cyber Disruption Response Planning Guide*." A cybersecurity disruption is defined as: “an event or effects from events that are likely to cause, or are causing, harm to critical functions and series across the public and private sectors by impairing the confidentiality, integrity, or availability, of electronic information, information systems, services, or networks that provide direct information technology services or enabling and support capabilities for other services; and/or threaten public safety, undermine public confidence, have a negative effect on the state economy, or diminish the security posture of the state.” A cybersecurity disruption differs from a cybersecurity incident which is limited in scope and impact.

Examples of a cybersecurity disruption include: a cyber attack on the power grid which leads to a loss of power for a significant population; a cyber attack on water treatment and delivery leading to a loss of water supply to a significant population; a cyber attack on network capabilities leading to loss of communications which then hampers, interrupts or prevents the operation of government and requires implementation of a continuity of operations plan; or a hurricane, flood, or other natural disaster that impairs or destroys key infrastructure assets that then precipitates the loss of connectivity over the internet or internal network.

With these scenarios in mind, states like Michigan, taking the “whole community” approach, convened state and local government representatives and private sector critical infrastructure owners and operators to develop the Michigan Cyber Disruption Response Strategy, initially completed in 2013. Michigan’s Cyber Disruption Response Strategy provides a common framework to encourage a statewide effort among public and private partners to defend Michigan’s critical networks. Specifically the plan prompts critical infrastructure owners and operators to address: data backup, disaster recovery/business continuity, halt key processes, equipment shutdown, log file, communications, and how to activate the cyber disruption response plan.

States like the Commonwealth of Massachusetts, New Hampshire, and Rhode Island have taken a regional approach to cyber disruption planning, an effort supported by FEMA’s Regional Catastrophic Preparedness Grant Program and Urban Areas Security Initiative (UASI) funding. In 2012, as part of the New England Regional Catastrophic Preparedness Imitative (NERCPI), these three states along with the City of Boston and Providence completed regional cyber disruption planning and created a Cyber Disruption Response Annex which outlines how cyber responders will support industrial control system (ICS) structure in each jurisdiction, how critical cyber incident information will be shared, and how IT organizations can support public safety and each other. NERCPI also created cyber disruption teams in each state and the City of Boston; these teams are comprised of experts from IT, emergency management and public safety and are responsible for coordinating resources and information during catastrophic events.

As these previous examples exhibit, **protection from cybersecurity attacks requires a “team” or “whole community” approach and a key partner to the states has been the U.S. Department of Homeland Security (DHS)**. States are heavy utilizers of DHS’ cybersecurityfocused state and local programs including: ICS-CERT, FedVTE (virtual training environment), and cyber security advisors (CSA). Also, federal programs like “CyberCorps: Scholarship for Service” allow qualifying students to serve in an IT assurance role with a federal, state, or local government after graduation; this helps shore the IT security workforce gap that all states are facing.

The federal government, principally through DHS, has and hopefully will continue to provide support for successful cybersecurity programs. There is, however, **another way the federal government could aid in enhancing states’ ability to identify, protect, detect, respond, and recover – by harmonizing federal security requirements.**

When states receive federal funds, they are required to certify that certain security measures are in place; this is mandated by the Federal Information Security Management Act (FISMA). CIOs and CISOs must also comply with a variety of federal regulations, typically promulgated in a silo-ed fashion. Some of the federal regulations with which our community must comply include: IRS Publication 1075, FBI-Criminal Justice Information Services (FBI-CJIS), the Health insurance Portability and Accountability Act (HIPAA), social security administration security standards, Family Educational Rights and Privacy Act (FERPA), Office of Child Support Enforcement (OCSE) security requirements, the Center for Medicare and Medicaid Services’ Minimum Acceptable Risk Standards for Exchanges (MARS-E), among others.

The overarching goal of these regulations is data/information security. Knowing that the vast majority of states are utilizing national standards like those issued by NIST, the federal government could lessen the regulatory burden on states by harmonizing federal requirements especially since most if not all of these regulations share a common security goal.

Cybersecurity is an issue that will only become more complex as we enter an age where the internet of things will become more prominent and technology like unmanned aerial systems (UAS), body-worn cameras, and cloud adoption are a norm. New technologies will require state governments to constantly assess security vulnerabilities as citizens demand consumer-level technology services to be deployed on a whole-of-government or enterprise basis. Given this background, the Congress and federal agencies should continue to partner with state CIOs and CISOs when reviewing or promulgating new data security laws or regulations to ensure that the goal of security is achieved without undue burden or redundancy.

Thank you for opportunity to testify today on this critical issue.