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

"Cyber Incident Response: Bridging the Gap Between Cybersecurity and Emergency Management"

Testimony of Craig Orgeron, Ph.D., CPM
President, National Association of State Chief Information Officers (NASCIO)
Executive Director, Department of Information Technology Services, State of Mississippi

October 30, 2013

Thank you Chairs Brooks and Meehan, Ranking Members Payne and Clarke, and members of the Committee, for inviting me to speak to you today. I am honored by the invitation. As we wrap up Cybersecurity Awareness Month it is timely that we are having this hearing on one of our nation's most significant vulnerabilities.

As Executive Director of the Mississippi Department of Information Technology Services (ITS), as well as President of the National Association of State Chief Information Officers, better known as NASCIO, I can report that each year states are facing greater numbers of evolving and sophisticated cyber-attacks. In addition to states serving as a repository of sensitive data about our citizens and homeland, states increasingly utilize the online environment to deliver vital services, maintain critical infrastructure such as public utilities, and ensure our first responders receive the data they need in crisis situations. State government IT systems are a vital component of the nation's critical infrastructure.

Today, with this testimony, I want to provide the Committee information on the readiness of our state governments to defend against and respond to major cyber-attacks, as well as opportunities to collaborate to minimize the risk to our nation. I hope to give you a sense of the threat landscape and how states and the federal government, along with the private sector, can work together to better secure our homeland.

State governments are at risk from a host of new and aggressive security threats that require a formal strategy, adequate resources, and constant vigilance. Cybersecurity continues to be one of the major "hot button" issues for state CIOs and one that receives increasing attention from governors and other elected officials.

State CIOs are taking the lead in securing state systems. According to NASCIO's 2013 survey of State CIOs conducted by in collaboration with TechAmerica and Grant Thornton LLP, significant improvements have been made in the last few years. Over three-quarters of states have adopted a cybersecurity framework, implemented continuous vulnerability monitoring capabilities, and developed security awareness training for employees and third-party contractors. These are key steps toward building a more secure state cyber environment. Unfortunately, less than half of states are documenting the effectiveness of the cybersecurity program they have in place, and even fewer have developed a cybersecurity disruption response plan.

In the same survey, CIOs were asked about the major barriers they faced in addressing cybersecurity. The increasing sophistication of threats, followed closely by a lack of funding and inadequate availability of security professionals, topped the list. Additionally, the survey data reveals that only 8 percent of states have implemented identity and access management of state data systems across the enterprise, although 42 percent of respondents noted an in-process implementation.

The state CIO role in disaster recovery appears to be increasing each year. According to the NASCIO 2013 survey almost two-thirds of states pursue a federated strategy to disaster recovery, with responsibilities split between the CIO and state departments and agencies. The survey also queried state CIOs regarding their role in helping their state respond to and recover from a natural or manmade disaster. The survey results show almost all CIOs see their role as one of coordinating with other state officials and restoring and maintaining infrastructure and communications services. I have attached the full results of this survey to my testimony today, along with the 2012 Deloitte-NASCIO Cybersecurity Study entitled *"State governments at Risk,"* for your further review.

The State of Mississippi's IT systems, like systems from all states, face cyber-attacks every day, ranging from a few thousand attempts to as many as 10 million per day—some domestic, many international. To win this ongoing battle, state IT experts have to be right every time, while hackers need to only be right once. As these attacks continue to grow more sophisticated, both public and private sector entities will need to develop better tools and increase collaboration to both deter attacks and plan a coordinated response to contain the damage from successful attacks. This ultimately requires a multi-sector approach, with all levels of government and private industry working together. Securing systems in cyberspace, and responding to successful hacking attempts, has little in common with traditional emergency management after a disaster. Advanced cyber threats are much more akin to an aggressive, new strain of virus: the threat is diffuse, and almost impossible to prevent before it comes into being. In addition, just like a new viral strain, it takes time to properly identify and contain the virus, educate the populous about how to avoid contracting it, and treat those infected.

As the federal government and private sector ramp up their defenses against sophisticated hackers, state governments are becoming a prime target of foreign, state-sponsored entities and international crime syndicates. Sophisticated hackers may hide in IT systems for years—creating what is referred to as an "advanced persistent threat." These hackers can remain in state systems monitoring data and waiting to unleash significant harm to our nation's financial systems, transportation systems, supply chain, and key utilities such as the electrical grid, and pipelines, to name a few. In worst case scenarios, a sophisticated hack on public safety communication systems or critical infrastructure could coincide with a physical attack or natural disaster to impede the ability of authorities to respond to one or both events.

Elected leaders at all levels have come to understand that cybersecurity is a significant issue that requires their attention. The National Governors Association (NGA) is working with the National Emergency Management Association (NEMA), NASCIO, and members of the private sector, to build upon this greater understanding. Based on this collaboration, NGA released "A Call to Action for Governors for Cybersecurity," which provides strategic recommendations governors can immediately adopt to improve their state's cybersecurity posture. By gaining support from the Governor's office, a state can tackle key issues of governance and create an authority structure that builds comprehensive cybersecurity across the state enterprise. It is well known that when compared with the private sector and the federal government, states do not have comparable resources and tools to provide similar levels of protection to their systems, despite the fact that they often maintain the same sensitive information and key critical infrastructure.

This is only partially a financial issue—it is also a policy and skilled personnel issue. On the latter two fronts, there is a great deal the federal government can do to help state governments improve preparedness and response to cyber-attacks.

On policy, perhaps the single key to ensuring a substantial attack does not blindside us is the federal government facilitating greater information sharing between federal agencies, the private sector, and state and local partners. NASCIO believes the implementation of Executive Order 13636 and Presidential Policy Directive 21 will be a first step to achieving these goals.

As each state's cybersecurity level of maturity and governance is different, NASCIO would be concerned about any effort by the federal government to designate a single state entity as the responsible point for sharing and disseminating information between state and federal entities. Such decisions should ultimately be left to each state's governor to fit their model of cyber governance. Just as each state has different geography and vulnerabilities to extreme weather or manmade disasters, state Information Technology systems and the governance of those IT systems are very different. Federal resources and support to states must respect and bolster the state organizations.

States rely on multiple external resources for threat information, such as the Multi-State Information Sharing and Analysis Center (MS-ISAC), United States Computer Emergency Readiness Team (US-CERT), and FBI's InfraGuard. States then act on this information through various channels: some states have built a sophisticated cyber capacity at their state fusion center, others have bolstered the authority of their Office of Information Technology, and some coordinate with a cyber-division of their state National Guard. The federal government should support all these approaches. Public sector cybersecurity is in its infancy; best practices must be shared, but diverse approaches—particularly when it comes to governance and methodology—should be nurtured.

Due to the diverse landscape at the state level, the federal government must be as inclusive as possible in disseminating threat information, and work outside the public safety and intelligence sector's traditional one-to-many comfort zone. Cybersecurity works best when more people have an understanding of the threats. Therefore, NASCIO and its members applaud the ongoing effort to provide greater declassification of cyber threat information. We hope this will be followed by collaborative effort to standardize information exchange models for sharing threat data.

Classified threats will always exist, though, and therefore, greater access to classified information is needed at the top echelons of state government. As of now, the U.S. Department of Homeland Security (DHS) will only provide state governments with two Top Secret clearances. Typically, these go to the Governor and their homeland security advisor or director of public safety. This means in many states, Chief Information Officers or their Chief Information Security Officers are not cleared to the appropriate level to receive vital information from the Intelligence Community on the most advanced international threats against our networks. This should be remedied.

Additionally, while opportunities for limited federal assistance for cyber threats have been included in the National Preparedness Grant Program (NPGP), the formulaic structure of the program means states do not have enough funding to do much more than maintain legacy homeland security investments and administer grants to local governments. For NPGP to meet the current threats faced by our states and localities, changes will need to be made by Congress and the Administration.

Besides fixing funding models to meet the current threat, there are other policy efforts that can be undertaken to maximize the impact of existing cybersecurity resources. NASCIO believes the National Cyber Security Review, or NCSR, is an excellent opportunity to review our national preparedness and provide resources and technical assistance to fill gaps in our defenses.

The NCSR is a voluntary self-assessment survey designed to evaluate cyber security management within state, local, tribal and territorial governments. At the request of Congress, DHS has partnered with MS-ISAC, NASCIO, and the National Association of Counties (NACo) to develop and conduct the NCSR. The survey is now in the field and we expect final results to be provided in the first quarter of next year. Much like the Threat and Hazard Identification and Risk Assessment (THIRA) provides a guide for investment in traditional homeland security gaps, the NCSR could be followed up with the promise of federal technical assistance to state and local participants who lag behind in vital areas. This will have the dual benefit of safeguarding citizen data and encouraging greater participation in national level vulnerability assessments.

NASCIO also supports efforts to include state governments as a participant in programs that build the public sector cybersecurity workforce. One of the greatest difficulties states face is attracting and retaining talent in this information security sector. States cannot compete with the salaries provided by the private sector, or the allure of positions in the U.S. federal intelligence services. Federal scholarships to study cybersecurity in exchange for working several years in the federal government, or for state or local governments, has the twofold benefit of better protecting our citizens and expanding the available talent pool of cyber security experts. Scholarships should be expanded to ensure those who take advantage of them can work at any level of government protecting IT systems.

As many successful cyber-attacks could be prevented by good cyber hygiene and security practices, federal collaboration with state and local governments to create a culture of awareness and preparedness would also be a significant step forward. Just like ‘see something, say something,’ clicking one’s seatbelt before driving, or even covering your mouth when you sneeze, public awareness and habit is one simple way to significantly reduce the threat.

The federal government can also take steps to reduce burdens on state and local governments by harmonizing cybersecurity standards and requirements across federal programs so state governments can provide more efficient and effective security of programs at a lower cost to taxpayers. Under the Federal Information Security Management Act, better known as FISMA, states are required to check certain boxes regarding security when taking federal grant dollars. However, federal agencies interpret these rules differently, and require different security standards. This often means that states must spend money on redundant systems to comply with a patchwork of federal rules. It also means a lack of compatibility between various systems that states manage, which could otherwise be consolidated and more secure. Congress should work with NASCIO and the states to replace FISMA with cybersecurity rules that better conform to universal, outcome-based standards that would provide both federal agencies and states with better security as well as greater efficiency.

Cybersecurity is a complex issue, and we have a long road ahead of us to making our nation’s systems more secure. There is no single solution here—or in tech speak, there isn’t a “killer app.” With the diffuse threat and diverse actors, cybersecurity requires a many-to-many approach. Most public safety response efforts are command and control, line of command efforts. Such efforts will not work when it comes to cybersecurity and response. With cyber-attacks and the resultant impact, there is rarely a front line and the “path of the storm” is usually not obvious.

Holding hearings such as this one and finding ways to share information and resources will be crucial moving forward. We ask that Congress continue to work with the states in identifying ways to protect our nation’s digital assets, including rapidly maturing threat information sharing entities and developing a common framework that can serve as a roadmap and provide funding justification for state cybersecurity. Thank you for the opportunity to testify and your time today.