NASCIO
Representing Chief Information Officers of the States

April 8, 2013

Ms. Diane Honeycutt
Division Secretary for Computer Security Division
National Institute of Standards and Technology
Computer Security Division
U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20899

RE: Docket Number 130208119-3119-01

Dear Ms. Honeycutt:

On behalf of the National Association of State Chief Information Officers (NASCIO), we are writing to submit comments in response to NIST's request in the Federal Register on February 26, 2013, for input on developing a framework to reduce cyber risks to critical infrastructure (or "cybersecurity framework").

NASCIO represents state chief information officers and information technology executives and managers from the states, territories, and the District of Columbia. State CIOs are on the front lines of cybersecurity in the public sector, responsible for activities from securing detailed data on our citizens and critical infrastructure, to providing cloud services for state and local agencies, to managing large IT infrastructure projects such as law enforcement and public utility telecommunications. Our members are responsible for protecting against, mitigating the effects of, response to, and rapid recovery following cyber-attacks on these state systems. As states move toward internet-hosted applications using new technologies like "big data," mobile solutions, and cloud computing, protecting these systems becomes increasingly complex.

Similar to the federal government, State CIOs face many hurdles—ranging from the bureaucratic, to the legislative, to financial—in reducing the vulnerability of these systems. Attached to this letter you will find our 2012 Deloitte-NASCIO Cybersecurity Study, *"State governments at risk: a call for collaboration and compliance."* As the study shows, there is clear support from public sector leaders for a greater focus on cybersecurity in their states, but a lack of funding, governance, stakeholder support, trained personnel, and awareness of risks—all of which impede progress. Perhaps most importantly, though, the study finds NIST guidance provides an important foundation for the adoption of security frameworks and controls in state government.

States rely heavily on externally developed guidance and standards to craft their security architecture and implement cybersecurity programs. State CIOs understand

201 East Main Street, Suite 1405
Lexington, KY 40507
Phone :: (859) 514-9153
FAX :: (859) 514-9166
www.NASCIO.org

that with the current landscape of competing and often conflicting frameworks and regulatory requirements, the adoption of an enterprise approach to security can guide agencies in the right direction with common goals and measureable outcomes. Based on the responses to the 2012 Deloitte-NASCIO cybersecurity study, 82% of the respondents rely on NIST standards (i.e. SP800-53, FIPS 199) as the foundation for enterprise-wide security policies, standards and procedures.

The following recommendations for action outlined in the study may be informative as NIST considers the opportunities and impact of a cybersecurity framework on state stakeholders:

- ✓ Assess and communicate security risks
- ✓ Better articulate risks and audit finds with business stakeholders
- ✓ Explore creative paths to improve cybersecurity effectiveness within states' current federated governance model
- ✓ Focus on audit and continuous monitoring of third-party compliance
- ✓ Raise stakeholder awareness to combat accidental data breaches
- ✓ Agressively explore alternative funding sources including collaboration with other entities
- ✓ Make better security an enabler of the use of emerging technologies

The executive order "Improving Critical Infrastructure Cybersecurity" prescribes intergovernmental engagement requirements in the creation of the cybersecurity framework. The processes utilized by NIST to achieve a sufficient level of engagement among state stakeholders and thus ultimate buy-in are significant concerns for state governments, as the final framework will certainly impact state governments and the intergovernmental relationship both explicitly and implicitly. The role of key state actors as stakeholders in the framework development should be clearly defined. Specifically, NASCIO would suggest that NIST engage state governments regarding framework decisions that impact: critical infrastructure sectors that states currently regulate, directly operate, or administer; the Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities; Identity Management; Privacy Controls; and, Federal Information Security Management Act (FISMA) Implementation and federal grant requirements.

NASCIO is supportive of efforts to synchronize and mature cybersecurity norms across both the public and private sector enterprise. However, the federal government must be careful not to inadvertently create unfunded mandates on state and local partners. Public budgets are still strained at all levels of government, and while state and local stakeholders wish to contribute to the overall cybersecurity effort, the ability to fund initiatives independently is unlikely at this time. For instance, the administrative burden of additional information sharing could have a significant impact on already strained state resources. It should also not preempt or otherwise hinder state authority to take its own steps to secure critical public or private infrastructure.

NASCIO believes there are potential opportunities for state governments in any national cybersecurity framework, though. For instance, a cybersecurity framework would be helpful if it provides a prioritized cybersecurity roadmap in addition to the currently existing menu of varied standards. Further, best practice fundamentals such as the links between budgetary strategies, authority and governance, and highlighting emerging threats can be significant for states. Such a roadmap could assist states in prioritizing their cybersecurity investments and help state executive agencies justify to state legislators the needed funding improvements to vulnerable systems.

Establishing and promoting common practices will require changes in how the federal government interacts with stakeholders. As NIST examines normalizing cybersecurity standards and information sharing, it should begin by reviewing the federal example and look to promote an existing standard based approach to exchanging information. NASCIO recommends the National Information Exchange Model (NIEM) as a proven, non-proprietary model that could be widely utilized across public and private enterprises for information sharing on cybersecurity.

NASCIO also believes the federal government must make changes to how it currently interacts with common stakeholders on cybersecurity if it hopes to create an effective, relevant framework. Many federal initiatives fund internet and information security programs. However, without cross-cutting communication and coordinated assets, the efforts do not realize maximum efficiency and impact. States are a key partner in delivering over $600 billion in federal programs to citizens, and therefore the federal government has a direct interest in helping states secure their data and systems against attack. The overarching demand to be efficient with taxpayer funds and ensure as much funding as possible goes to the end users of public services often means that veiled costs of operation such as cyber defenses, training, and identity management are severely neglected. This is detrimental to the long-term efficiency of government, as well as the security of both the citizens we serve and the government we are tasked with protecting.

As NIST drafts the cybersecurity framework, it should keep in mind that privacy and security requirements that are preconditions of federal programs and funding must be uniformly interpreted and implemented across all agencies and levels. The varied approaches to FISMA compliance across the federal enterprise evolve into divergent and often conflicting requirements for grant recipients. This “silo” funding approach to security, where each grant funds IT infrastructure protection separately, provides no incentive for states to seek enterprise solutions and shared services models that are typically more secure and efficient. State CIOs need flexibility to prevent the creation of new “stove piped” security systems that are repetitive, a less efficient use of taxpayer funds, and less secure. NASCIO believes NIST should consider recommending alignment among FISMA compliance requirements, as well as set asides on the programmatic side of grant programs for the protection of data.

NASCIO and State CIOs look forward to serving as a resource and partner as NIST considers how to draft and ultimately implement a cybersecurity framework. We appreciate your consideration of NASCIO's comments.

Sincerely,

Doug Robinson
Executive Director

Mitch Herckis
Director of Government Affairs

ATTACHMENT