NASCIO
Representing Chief Information Officers of the States

December 13, 2013

Submitted electronically to csfcomments@nist.gov

Information Technology Laboratory
ATTN: Adam Sedgewick
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

RE: Docket No.: 130909789-3789-01

Dear Mr. Sedgewick,

The National Association of State Chief Information Officers (NASCIO) appreciates the opportunity to comment on the cybersecurity framework. NASCIO believes the framework will serve as a valuable tool to create greater comprehension of cyber risk landscape, raise the profile of cybersecurity assessment and preparedness in state government, and focus leadership on the need for an enterprise approach to information technology—and with it cybersecurity.

NASCIO applauds NIST's work developing the preliminary cybersecurity framework. We appreciate the outreach and collaborative efforts undertaken during its development, particularly the direct outreach to the public sector and state CIOs. The preliminary framework does not attempt to determine what level of security or risk acceptance makes the most sense. Rather, it provides a roadmap for organizations attempting to make those assessments and helps it gauge progress towards self-prescribed goals. NIST has achieved this in a straightforward, accessible form that is understandable throughout the organization and scalable to a diverse range of operations, both public and private. This will be particularly useful for those organizations that have not previously undertaken a significant risk management assessment.

Historically, the public sector classified cybersecurity as an operational or administrative cost to be minimized rather than a vital, core responsibility of government. NASCIO believes that the preliminary framework will help state CIOs present the business case to key stakeholders in the state executive and legislative branch about the importance of investing in cybersecurity. For the first time, public and private sector entities will have a common tool to assess the maturity of their cyber defenses, have a common platform to make comparisons to other states' actions, and make adjustments as necessary. Further, with over 80 percent of states relying on NIST standards (SP-800-53) as guidance to develop, comply or execute information security programs,[1] NIST is clearly a trusted and reliable actor to be leading this effort.

[1] "State governments at risk: a call for collaboration and compliance." 2012 Deloitte-NASCIO Cybersecurity Study. Page 18, Figure 13.

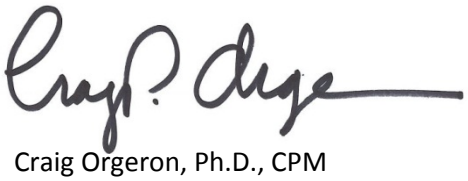
201 East Main Street, Suite 1405
Lexington, KY 40507
Phone :: (859) 514-9153
FAX :: (859) 514-9166
www.NASCIO.org

In an effort to make the NIST framework more accessible and beneficial for public sector entities, we would invite NIST and other federal actors to collaborate with NASCIO in creating a state and local government overlay that clearly outlines federal regulations and program requirements with information security requirements that states must consider when implementing a comprehensive cybersecurity plan and to better inform risk management decisions. NASCIO believes this will be a crucial step in achieving high adoption rates in the public sector. It will make the framework of greater interest to public sector entities, particularly those that already have a significant risk management program in place or have utilized other tools such as the Department of Homeland Security's Critical Resiliency Review.

Ultimately, the usefulness of the framework will be proven through the work of early-adopters. NASCIO hopes a number of states will choose to be at the forefront in this effort. NIST may be able to incentivize early public sector adoption by engaging with states that choose to utilize the framework and providing technical assistance in both planning and management of cyber risk. We understand from our members that some initial engagement with the states around adoption has already begun, and strongly commend NIST for this highly proactive approach.

NASCIO looks forward to continuing to engage with NIST as the states begin to review and make decisions regarding adoption of the framework. Please feel free to contact our Director of Government Affairs, Mitch Herckis, at (202) 841-9130 or mherckis@amrms.com, with any questions you might have about this submission or regarding further state collaboration with NIST on the framework.

Sincerely,



Craig Orgeron, Ph.D., CPM
President, NASCIO
CIO, State of Mississippi