NASCIO
Representing Chief Information Officers of the States

October 10, 2014

Submitted electronically to cyberframework@nist.gov

Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

RE: Docket No. 140721609–4609–01

Dear Ms. Honeycutt,

On behalf of the National Association of State Chief Information Officers (NASCIO), I am writing to share the findings in the attached 2014 Deloitte-NASCIO Cybersecurity Study, *"State governments at risk: Time to move forward."* We believe the study will be informative in NIST's efforts to continue to improve the Framework for Improving Critical Infrastructure Cybersecurity (hereafter referred to as simply the "framework"), the associated roadmap, and other key cybersecurity efforts such as the National Initiative for Cybersecurity Education (NICE) Framework.

Our study found insufficient funding, increasingly sophisticated threats, and shortage of skilled talent are all fueling this concern and putting state governments at risk. However, it also found the efforts put forth by NIST to provide tools to secure the cyber environment are being significantly leveraged at the state level.

State Chief Information Officers (CIOs) consistently rank cybersecurity as a primary concern and priority. As such, NASCIO has teamed with Deloitte to survey the states on this crucial issue. Participants from 49 states answered 58 questions designed to characterize the enterprise-level strategy, governance, and operation of security programs. 84 percent of respondents were enterprise state Chief Information Security Officers (CISOs); another six percent were the state CIOs.

NASCIO found that states are welcoming guidance from NIST. Our survey shows that 93.9 percent of states' CISOs responding are using NIST standards. The NIST cybersecurity framework seems to be gaining traction, with 47% of CISOs planning to leverage it within the next six months to a year, and an additional 38.8% responding that they are currently reviewing the framework. Only two percent of state CISOs responded that they had no plan to leverage the NIST cybersecurity framework.

About one in seven CISOs indicated the state is implementing portions of the NICE Framework, and over a third responded that they are currently reviewing it. CISOs believe that scarcity of qualified professionals willing to work in the public sector is one of the biggest barriers to effectively addressing cybersecurity challenges. That said, our data shows that CISOs are also becoming more proactive about closing competency gaps, and are making cybersecurity training

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

a top priority. In addition, CISOs are gaining more confidence in their staffs. Only one in ten said employees have large gaps in competencies versus nearly a quarter in 2012; a greater percentage said their employees are up to the job compared with two years ago.

In an effort to repel the cyber threat, federal and state governments are rapidly adding rules that are exponentially increasing the regulatory complexity to the state cybersecurity landscape. NASCIO has not seen any evidence of an effort by federal regulatory agencies to utilize the framework to harmonize these regulations or provide other consistency across the patchwork of cybersecurity regulations that federal activities impose upon state governments. This is to the detriment of both the federal regulators and the states we represent, both of who could benefit from streamlined and efficient cybersecurity standards that are coherent across government enterprises. NASCIO would ask that NIST and DHS work with our association and other national organizations representing state and local governments to promote common standards across agency grants and build a state and local overlay to the NIST framework that could be promoted by regulatory and grant-making agencies.

NASCIO would also like to explore how our organization can facilitate a discussion between state CIOs, CISOs, and NIST in an effort to provide a more intimate portrait of the states' work to secure their systems by leveraging the NIST Framework and other tools.

We appreciate your consideration of NASCIO's comments. Our organization and members hope we can continue to serve as a resource and partner as NIST continues to improve and promote the cybersecurity framework. Please feel free to contact our Director of Government Affairs, Mitch Herckis, at (202) 841-9130 or mherckis@nascio.org, with any questions you might have about this submission or regarding further state collaboration with NIST on the framework.

Sincerely,

Doug Robinson
Executive Director

ATTACHMENT: 2014 Deloitte-NASCIO Cybersecurity Study, *"State governments at risk: Time to move forward."*