NASCIO
Representing Chief Information Officers of the States
WWW.NASCIO.ORG

Submitted electronically to: cyberframework@nist.gov

January 19, 2018

Edwin Games
National Institute of Standards and Technology (NIST)
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Mr. Games,
On behalf of the National Association of State Chief Information Officers (NASCIO), we appreciate the opportunity to provide comments on the second draft of Version 1.1 (hereinafter “draft 2”) of the Cybersecurity Framework. NASCIO previously provided comments regarding the first draft of Version 1.1 (hereinafter “draft 1”) which added new language on supply chain risk management and cybersecurity metrics. In this letter, our aim is to update NIST on new data received in the *2017 State CIO Survey* that speaks to aforementioned topics. Again, we applaud the work of NIST to further improve Version 1.1.

NASCIO represents state chief information officers (CIO) and information technology (IT) executives and managers from the states, territories, and D.C. State CIOs lead state IT policy and implementation and continually look for opportunities to improve operations, bring innovation, and transform state government through technological solutions. Naturally, cybersecurity has been a top priority for state CIOs for the past several years (See, State CIO Top Ten Policy and Technology Priorities for 2018).

In the *2017 State CIO Survey*, 95 percent of CIOs report that they have “adopted a cybersecurity framework based on national standards and guidelines.” It is also clear from the 2017 survey that state CIOs continue to work on cybersecurity metrics; only 57 percent of state CIOs report being able to “document[ed] the effectiveness of your cybersecurity program with metrics and testing.” We asked state CIOs to specifically characterize the status of the enterprise cybersecurity metrics program: program is in the planning state (12%); program underway, but not complete (57%); program complete and fully operational (12%); program delivering significant value (14%); ad hoc/not defined (5%). Only 26 percent of state CIOs report having a complete and fully operational program though only 14 percent of that figure report that the metrics program is delivering value.

Draft 2 includes section 4.0 *Self-Assessing Cybersecurity Risk with the Framework* and makes reference to *NIST Special Publication 800-55 Performance Measurement Guide for Information Security*, and while these resources exist, state CIOs continue to work on perfecting a metrics program to accurately measure cybersecurity investment and its associated security gains. The draft Roadmap Version 1.1 makes mention of NIST’s efforts in initiating a cybersecurity measurement program including the evolution of *NIST SP 800-55*. State CIOs would appreciate continual effort and engagement on this issue and welcome the opportunity to collaborate on cybersecurity metrics.

For more information, please contact Yejin Cooke, director of government affairs, NASCIO at ycooke@NASCIO.org or 202.624.8477.

Sincerely,

James L Reese II

Bo Reese,
President, NASCIO & Chief Information Officer, State of Oklahoma