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

February 23, 2016
Submitted electronically via cyberframework@nist.gov

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

RE: Docket No. 151103999-5999-01

Dear Ms. Honeycutt,
On behalf of the National Association of State Chief Information Officers (NASCIO), thank you for the opportunity to submit comments in response to the National Institute of Standards and Technology's (NIST) Request for Information (RFI), "Views on the Framework for Improving Critical Infrastructure Cybersecurity."

NASCIO represents the state chief information officers (CIO) and information technology executives and managers from the states, territories and D.C. State CIOs are leaders of state information technology policy and implementation and continually look for opportunities to improve the 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, NASCIO Top Ten Policy and Technology Priorities Survey, 2013-2016).

Guidance from NIST has been a valuable resource to state CIOs and state chief information security officers (CISOs). Even prior to the release of the NIST Framework for Improving Critical Infrastructure Cybersecurity (hereinafter, "Framework"), our data show that 82 percent of CISOs relied upon NIST standards as the predominant external cybersecurity standard/guidance (See, 2012 Deloitte-NASCIO Cybersecurity Study: State governments at risk: a call for collaboration and compliance). Data from the 2014 Deloitte-NASCIO Cybersecurity Study indicate again the predominance of NIST standards and the value of the Framework. In 2014, 49 percent of states planned to leverage the NIST Framework and another 38.8 percent of states were reviewing the Framework. Again, the predominant external cybersecurity standards used were NIST standards (93.9 percent) and the Framework (46.9 percent). NASCIO's most recent survey of state CIOs, "The Value Equation: Agility in Sourcing, Software and Services," shows that 80 percent of states have adopted a cybersecurity framework based on national standards and guidelines.

To combat the increasing cybersecurity threat, state and federal governments are issuing rules that aim to address cybersecurity in some form. Though the intent is commendable, the issuance of cybersecurity regulations have led to a regulatory environment that is complex and difficult to manage. State CIOs and CISOs must comply with a variety of federal laws and regulations including: IRS Publication 1075, FBI Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPAA), Family Education Right and Privacy Act (FERPA), and the Federal

Information Security Management Act (FISMA), among others. As previously mentioned, an overwhelming majority of state CIOs and CISOs utilize the Framework to secure state networks and digital assets. However, though the Framework is the predominant resource for state CIOs, there has not been an effort to harmonize federal agency regulations and security requirements to the Framework. This creates an environment where CIOs and CISOs are spending more time responding to audit findings rather than devoting time to their core mission of securing public networks. As such, NASCIO would encourage NIST to engage with federal agencies to ensure that cybersecurity goals are met without undue burden or duplication at the state level.

We appreciate the work that NIST has done to further our nation's cybersecurity posture. NASCIO members have taken advantage of the Framework and are likely to continue to do so. NASCIO would also request that NIST initiate a discussion with NASCIO and federal agencies that impose cybersecurity requirements to gauge the feasibility of harmonizing those requirements to the Framework. For further information, please contact NASCIO Director of Government Affairs, Yejin Cooke, at 202.624.8477 or ycooke@NASCIO.org. Thank you for considering NASCIO's comments.

Sincerely,

Darryl Ackley
NASCIO President and Secretary of Information Technology, State of New Mexico

Doug Robinson

Doug Robinson
Executive Director