From: **Yejin Cooke**
Date: Mon, Apr 10, 2017 at 4:45 PM
Subject: NASCIO
To: cyberframework <cyberframework@nist.gov>

Dear NIST,

Attached is the NASCIO response to the NIST Framework revisions.

Please contact me should you have any questions.

Thank you,

Yejin

Yejin Cooke
Director of Government Affairs
National Association of State Chief Information Officers (NASCIO)
444 North Capitol Street NW, Suite 642, Washington, DC 20001
www.nascio.org

[Attachment Copied Below]

Submitted electronically to: cyberframework@nist.gov

April 10, 2017

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 write to provide our comments on the proposed revisions to the NIST Cybersecurity Framework first released in 2014. We applaud the inclusion of cybersecurity metrics and recognize the value of addressing supply chain management.

NASCIO represents state chief information officers (CIO) and information technology (IT) executives and managers from the states, territories, and D.C. State CIOs are leaders of 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, NASCIO Top Ten Policy and Technology Priories Survey).

State governments were early adopters of the Framework; upon release of the Framework in 2014, nearly two out of five chief information security officers (CISO) reported that they were currently reviewing the Framework and an additional 47 percent they planned to leverage it within the next 6 months – 1 year (See, 2014 Deloitte-NASCIO Cybersecurity Study). According to the 2016 NASCIO State CIO Survey, 94 percent of states report "adopting a cybersecurity framework, based on national standards and guidelines."

State governments are utilizing the Framework to properly identify cybersecurity risk and adopt measures to address gaps in their security posture. Now that Framework adoption has matured in state governments, state CISOs are actively focusing on more proactive and prophylactic activities like: training and awareness (39%), monitoring/security operations centers (37%), strategy (29%), identity and access management (29%), governance (29%), **metrics to measure and report effectiveness (29%)**, among others. (See, 2016 Deloitte-NASCIO Cybersecurity Study Turning Stategy and Awareness into Progress, at 5). This trend is encouraging because in 2014, NASCIO data showed that the lack of cybersecurity metrics contributed to the disconnect between cybersecurity budgets and strategy. (See, 2014 Deloitte-NASCIO Cybersecurity Study: State Governments at Risk, at 9).

The inclusion of *4.0: Measuring and Demonstrating Cybersecurity* in the current revision is timely and will assist states with communicating cybersecurity risk to government stakeholders and enable state CIOs and CISOs to better address risk gaps through commensurate investment in budgets and strategies. Currently, there is a confidence gap between state CISOs and other state officials; 66 percent of state officials say they are very or extremely confident that adequate measures are in place to protect information assets from externally originating cyberthreats, compared with only 27 percent of CISOs. As such, NASCIO has recommended that states enhance their communications ability to tell a compelling story about cyber risk especially given the impact to state budgets and policy. *4.0*

Measuring and Demonstrating Cybersecurity in the current revision will guide states as they develop communications strategies to appropriately portray the risk profile for state officials, leaders, and business stakeholders. In future revisions, additional examples of measurement and their application in a mission-driven environment, like that of state government, would be helpful.

NASCIO is also pleased to see the inclusion of supply chain risk management (SCRM) and its application in procurement or purchase environments. NASCIO data suggest that CISOs remain largely doubtful of third parties such as contractors, service providers, and business partners; 22 percent of CISOs report being "not very confident" and 65 percent of CISOs are only "somewhat confident" in the cybersecurity practices followed by third parties. In response, CISOs have adopted several measures to combat potential threats from third parties by: addressing cybersecurity issues in the contract (84%), impose cybersecurity policy and controls on third parties (71%), and monitor and control third-party access to systems and data (61%) among others. The SCRM sections in the current Framework revision will assist and guide states as they incorporate cybersecurity strategies and goals beyond their immediate operational environment.

Cybersecurity remains a priority for state CIOs and NASCIO applauds NIST for their commitment to guiding and assisting state government stakeholders as they mature in their enterprise risk management approaches. We look forward to working with you on this and future revisions of the NIST Cybersecurity Framework. Please contact Yejin Cooke, NASCIO Director of Government Affairs, should you have any questions.

Sincerely, Mark Raymond
President, NASCIO
Chief Information Officer, State of
Connecticut

Doug Robinson
Executive Director, NASCIO