January 26, 2016

National Institute of Standards and Technology
ATTN: Diane Honeycutt
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

Dear Ms. Honeycutt:

The American Institute of Certified Public Accountants (AICPA) is pleased to comment on the National Institute of Standards and Technology's (NIST's) "Views on the Framework for Improving Critical Infrastructure Cybersecurity." The AICPA is the world's largest member association representing the accounting profession, with more than 412,000 members in 144 countries, and a history of serving the public interest since 1887. AICPA members represent many areas of practice, including business and industry, public practice, government, education and consulting. The AICPA sets ethical standards for the profession and U.S. auditing standards for private companies, nonprofit organizations, federal, state and local governments. It develops and grades the Uniform CPA Examination, and offers specialty credentials for CPAs who concentrate on personal financial planning; forensic accounting; business valuation; and information management and technology assurance. Through a joint venture with the Chartered Institute of Management Accountants, it has established the Chartered Global Management Accountant designation, which sets a new standard for global recognition of management accounting.

Since the introduction of computers into the business environment, the AICPA has provided technology related risk management thought leadership guidance to businesses ranging from Fortune 10 corporations to sole proprietors on Main Street. As trusted advisers to businesses, our members have obtained a unique perspective of the impact of technology and its threats on business viability and security. Our members have designed controls to help businesses manage these threats, and when a threat is realized, provide financial and technical guidance that enables businesses to recover.

In 2000, the AICPA developed Trust Services Principles and Criteria (TSP&C). This resource presents measurement criteria for use when providing attestation or consulting services to evaluate controls relevant to the security, availability, and processing integrity of a system, and the confidentiality and privacy of the information processed by the system. In 2015, the AICPA developed the *SOC 2 + HITRUST Illustrative Report* in collaboration with HITRUST. The illustrative report assists CPAs in reporting on the fairness of the presentation of a description of a service organization's system relevant to security, availability and confidentiality, and the suitability of the design and operating effectiveness of controls over those aspects of the system based on the criteria for the security, availability, and confidentiality principles included in the *AICPA Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria) and the requirements in Health Information Trust Alliance Common Security Framework. The AICPA has collaborated with various organizations such as the Cloud Security Alliance and HITRUST to use SOC 2, demonstrating compliance with other security frameworks. Also, the AICPA is currently developing guidance for CPAs for performing and reporting on attestation engagements related to cybersecurity, and the NIST Framework is an integral part of the service.

One of the AICPA's largest contributions to the economic environment with publicly registered companies is through our active involvement with partners, audit committees and boards of directors. The CPA, acting as the trusted business advisor, provides insight and support into how shareholder concerns related to information security are addressed through various corporate governance initiatives.

We recognize the considerable work NIST has undertaken in establishing the Framework to strengthen the resilience of critical infrastructure. We applaud NIST for its inclusive approach, use of best practices, existing standards and guidance, and collaboration with industry and professional organizations and its willingness to ensure a fluid Framework, adapting to evolving cyber and business risks.

Our review and comments focus on two of NIST's questions for reviewers:

> ***Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?***

There is a greater need for transparency and understanding in the governance of the board and executive management. While the Framework does highlight communication to key stakeholders, there should be a heightened, driven criteria component set at what level of transparency should be delivered to stakeholders. It's general. It would have greater value if it set better expectations on what many boards of directors and steering committees really need to be aware of. The Framework should provide additional background around cybersecurity threats and their impact to an organization's objectives. For example, boards of directors should receive plain language, non-technical summaries of current threats regarding data integrity, the effectiveness of counter measures, and the potential reputational impact and financial loss. By providing clarity on the level at which cybersecurity objectives integrate into an organizations' Enterprise Risk Management (ERM) framework, the relationship between cybersecurity and business objectives can be better understood. For example, many organizations use the Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Enterprise Risk Management – Integrated Framework* (COSO Risk Management Framework) or similar framework.

Further, the Framework may not provide senior executives with appropriate tools to enable effective execution of their responsibilities in the realm of ERM. Namely, the Framework does not include a summary addressing the expected impact to critical issues on which business executives and boards of directors often focus. Among these would include reputation, consumer trust, investor or stakeholder responsibilities, required Securities and Exchange Commission disclosures outlining discussion of risks and breach costs, calculating and evaluating security metrics, operation leadership related to customer service delivery, and business opportunity. The Framework should translate the issues identified to a senior management level perspective as to facilitate executive understanding of the issues to be addressed.

> ***What portions of the Framework (if any) should be changed, or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.***

The Framework is helpful in identifying ways for larger organizations to benchmark their security posture, however, NIST should find a way to be relevant to smaller organizations (understanding that the resources are different) and convey the importance of information security awareness. While smaller organizations may not have all of the resources (e.g. staff, technology, skill set, etc.) that their larger counterparts have, the Framework can help smaller organizations focus on more direct threats like zero-day attacks by adding more references and resources to support them.

NIST may also want to consider adding to the Framework some criteria around the 2015 Cybersecurity Information Sharing Act which loosened the reins on what is considered private or confidential data for information sharing for threats that are real time or evolving. While the Framework aligns other standards in one cohesive document, it could better cross-reference with other governmental tools including the Cyber Resilience Review (CRR), a voluntary, non-technical assessment used to evaluate an organization’s operational resilience and cybersecurity practices. Also, some sort of introduction guiding professionals how to use the NIST guidance alongside complementary or even equivalent guidance would be of value to Framework users. For example, most organizations immediately mapped the NIST standard to ISO27001 and very little deviation was found. While this NIST Framework is excellent, how are end users supposed to use NIST with any other frameworks they have already adopted? The introduction should stress the value to be gained from using NIST alongside their own policies and frameworks.

Additionally, the Framework might have greater value if it offered examples of when competitors can share threat data and avoid anti-trust issues. It would also be helpful to suggest some sort of introduction targeting information security professionals and privacy attorneys since they both need to understand how to use the Framework within the context of their respective professions. For example, privacy concerns can conflict with data integrity concerns.

We appreciate the opportunity to comment and welcome the opportunity to serve as a resource to NIST on cybersecurity issues. If we can be of further assistance, please contact Susan Pierce at 919-402-4805 or SPierce@aicpa.org.

Sincerely,

Jeannette Koger

Jeannette Koger, CPA, CGMA
Vice President – Member Specialization and Credentialing
AICPA