From: **Kate Kiley**
Date: Mon, Apr 10, 2017 at 1:56 PM
Subject: AICPA response to RFC RE: Cybersecurity Framework v 1.1 draft
To: "cyberframework@nist.gov" <cyberframework@nist.gov>
Cc: Susan Pierce, Iesha Mack

Hello-

Please see the AICPA's comments RE: RFC to the Draft Cybersecurity Framework v1.1. If you have questions, please contact Susan Pierce at 919-402-4805 or Susan.Pierce@aicpa-cima.com
Thank you!

-Kate

Kate Kiley
Director — Congressional and Political Affairs
Association | AICPA | CIMA
Kate.Kiley@aicpa-cima.com
AICPA Member Service: 888.777.7077 or service@aicpa.org
CIMA: cimaglobal.com/Contact-us/

[Attachment Copied Below]

April 10, 2017
To: cyberframework@nist.gov (link sends e-mail)

The American Institute of Certified Public Accountants (AICPA) is pleased to comment on the National Institute of Standards and Technology's (NIST's) "Cybersecurity Framework Draft Version 1.1." The AICPA is the world's largest member association representing the accounting profession, with more than 418,000 members in 143 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 accounting and finance professionals who concentrate on personal financial planning; forensic accounting; business valuation; entity and intangible valuations; 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.

The AICPA has developed an entity-wide, examination-level cybersecurity risk management program attestation engagement including a reporting framework through which organizations can communicate relevant useful information about the effectiveness of their cybersecurity risk management program and CPAs can report on such information to meet the cybersecurity information needs of a broad range of stakeholders. This guide will be available in May of this year. Additionally, the AICPA plans to develop attestation guidance for internal control reports on a vendor's manufacturing processes for customers of manufacturers and distributers to better understand the security risk in their supply chains.

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 in 2014 and the recent update 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:

Does this proposed update adequately reflect advances made in the Roadmap areas?

As stated in the NIST Roadmap for Improving Critical Infrastructure Cybersecurity, "All organizations are part of, and dependent upon, product and service supply chains. Supply chain risk is an essential part of the risk landscape that should be included in organizational risk management programs." The inclusion of "Cyber Supply Chain Risk Management" category under Identify supports adequately reflects Section 4.8 of the Roadmap. However, there are some enhancements that NIST should consider adding to increase the effectiveness of the updated framework.

Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?

In Section 2.2 Framework Implementation Tiers, within the Tier 4's Cyber Supply Chain Risk Management section, it may be helpful to reference sub-vendors and providers of components and sub-services (e.g. risk could come from compromised chips inserted in a network device or computer). In addition to the cyber supply chain risk management activities outlined in Section 3.3 Communicating Cybersecurity Requirements with Stakeholders, when discussing global cybersecurity supply chain risk management activities, NIST may want to add identifying sovereign and regulatory risks to the list of activities. For example, users of the framework may want to consider what risks are involved in sole sourcing (when only one known source exists or that only one single supplier can fulfill the requirements). For instance, there could possibly be risks involved with critical parts from nations with hostile or unstable relations, not to mention, the difficulties with export/import licenses. Lastly, in Section 4.1 Correlation to Business Results, NIST may want to consider adding risks metrics that aren't easily quantified (e.g. reputational risks).

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.

Sincerely,

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