American Institute of CPAs
1211 Avenue of the Americas
New York, NY 10036-8775

September 9, 2016

Ms. Nakia Grayson
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

RE: Input to the Commission on Enhancing National Cybersecurity

Dear Ms. Grayson:

The American Institute of CPAs (AICPA) is pleased to offer its comments regarding the current and future states of cybersecurity in the digital economy.

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.

We applaud the Commission's efforts and believe that today's marketplace is driving the need for strengthened cybersecurity in all types of organizations. We have drafted this letter to provide some background and context to the Commission regarding the CPA profession's efforts in the cybersecurity space, which we believe will help to provide a common foundation for meaningful enterprise-wide cybersecurity risk management and reporting.

Overview

As you know, high profile attacks on major entities have resulted in an increased focus on cybersecurity by boards of directors, management, customers, business partners, regulators, analysts, and investors who have expressed a desire for decision-useful information about an entity's cybersecurity risk management program. Directors and senior management of entities are evaluating the design and effectiveness of their cybersecurity risk management programs and discussing options for communicating to stakeholders. In our view, innovation driven by the private sector significantly increases the opportunity to produce meaningful and timely improvements in current practice.

Decision makers, however, seek confidence that the information provided by entities is reliable. Because involvement of an independent, highly-qualified professional can increase the credibility of entity-prepared information, CPAs who have a long history of independently evaluating and reporting on controls over IT security are uniquely positioned to play such a role. Accordingly, we believe a CPA's opinion on the design and

operating effectiveness of an entity's cybersecurity risk management program could enhance the confidence that decision makers place in the entity's cybersecurity reporting.

The Role of CPAs in Facilitating a Consistent, Holistic Approach to Cybersecurity Risk Management

Currently, CPAs provide cybersecurity examination services under a variety of generally accepted professional standards and approaches. However, the AICPA believes adoption of a more consistent profession and market-wide approach for CPAs to examine and report on an entity's cybersecurity measures would address the informational needs of a broad range of users. Further, it would introduce a level of consistency that does not exist at present in the context of cybersecurity reporting and related assurance.

We are in the process of developing criteria that will give management the ability to consistently describe its cyber risk management program, and related guidance to enable the CPA professional to provide independent assurance on the effectiveness of the program's design via a report designed to meet the needs of a variety of potential users. Importantly, we believe that the decision to utilize such a service should be market driven, resting with the board and management of each company, and not be dictated by a government regulation or mandate.

Specifically we are developing the following:

- Suitable criteria (measuring benchmarks) for the cybersecurity examination engagement including:
    - Proposed Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program (description criteria), which are intended for use by management in designing and describing their cybersecurity risk management program, and by public accounting firms to report on management's description.
    - Proposed Revision of Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (control criteria), which are intended for use by public accounting firms that provide advisory or attestation services to evaluate the controls within an entity's cyber risk management program, or for SOC 2® engagements. Management also may use the trust services control criteria to evaluate the suitability of design and operating effectiveness of controls.
- A cybersecurity attestation guide to provide CPAs with performance and reporting guidance for an examination-level attestation engagement. The proposed cybersecurity examination-level attestation engagement reporting package includes:
    - A narrative description, prepared by management, describing the entity's cybersecurity risk management program;
    - Management's assertion that the narrative is presented in accordance with the description criteria and that the controls described within that program were effective to achieve the entity's cybersecurity objectives based on the control criteria; and
    - A CPA's independent opinion on whether the description is presented in accordance with the description criteria and the controls within that program were effective.

Management's description of their cybersecurity risk management program is designed to provide users with decision-useful information about how the entity identifies its sensitive information and systems, the ways in which the entity identifies and manages cybersecurity risks that threaten it, and a summary of controls implemented and operated to protect the information and systems against risk. This information provides the context users need to understand the conclusions expressed by management in its assertion, and by the CPA in his or her report about the effectiveness of the controls included in the entity's cybersecurity risk management program.

In order to promote consistency and comparability of cybersecurity information provided by different entities, the AICPA is developing the aforementioned description criteria for use by entities in preparing their descriptions. In developing the description criteria, we are considering information about cybersecurity published by industry experts, as well as cybersecurity information currently being requested by regulators and other potential report users. Elements from a variety of these sources are incorporated in the proposed description criteria to address the cybersecurity-related information that a range of users would find beneficial in their decision-making. Examples of the information considered include the following:

- National Institute of Standards and Technology Framework for Improving Critical Infrastructure (NIST Cybersecurity Framework or NIST CSF)
- ISO/IEC 27001/27002 and related standards
- US Dept. of Homeland Security requirements for annual FISMA reporting
- FFIEC questionnaires
- COBIT 5
- COSO's 2013 Internal Control – Integrated Framework
- HIPAA Security Rule
- HITRUST CSF
- PCI DSS 3.1
- NIST Special Publication 800 series

In particular, to facilitate management use, both the description criteria and the control criteria are organized in line with the points of focus of the 2013 COSO Internal Control – Integrated Framework, and have been mapped to the most widely-accepted industry security management and control frameworks, including the NIST Critical Infrastructure Cybersecurity Framework and ISO/IEC 27001 and 27002.

Our goal is for the criteria we are developing to be relevant for management application regardless of the frameworks they may already have implemented internally for cybersecurity risk management purposes. At the same time, the use of the criteria we have developed is voluntary, and the AICPA supports flexibility for entities in selecting which description criteria and control criteria are used in the examination. Ultimately, management is responsible for selecting both the description criteria and the control criteria to be used in an engagement, which could include any criteria deemed suitable by management and the auditor. This may include the criteria we are developing, or other

criteria embedded in widely-accepted industry security management and control frameworks, such as the NIST Cybersecurity Framework and ISO/IEC 27001.

Next Steps

Because the AICPA strongly believes in the importance of allowing the markets to lead on cyber issues, we have solicited feedback on the proposed engagement from multiple stakeholders. Later this month, the AICPA also plans to expose for public comment the proposed description criteria and proposed revisions to the trust services control criteria. We will forward the links to these exposure drafts for your consideration upon publication.

As cybersecurity risk management continues to evolve, the AICPA will adapt and advance the criteria and the assurance guidance we are developing based on user feedback and implementation evaluations. The AICPA is seeking to improve the usefulness of information in the marketplace, while enhancing efficiency and reducing compliance burdens of entities, and therefore cautions against additional regulations that could impact the constructive, market-driven conversations (and related solutions) that are currently being held around cybersecurity risk management and related information needs.

The CPA profession appreciates the opportunity to provide comments. We would be pleased to discuss these comments with you at your convenience. If you have any questions in the meantime, please don't hesitate to contact Amy Pawlicki, the AICPA's Director of Business Reporting, Assurance & Advisory Services, at apawlicki@aicpa.org or 212-596-6083.

Sincerely,

Susan C. Coffey, CPA, CGMA
Executive Vice President for Public Practice
AICPA