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

Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
400 7th Street SW, Suite 3E-218
Mail Stop 9W-11
Washington, DC 20219
Docket ID OCC-2016-0016
RIN 1557-AE06

Robert deV. Frierson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW.
Washington, DC 20551
Docket No. R-1550
RIN 7100-AE61

Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street N.W.
Washington, DC 20429
RIN 3064-AE45

Re: Enhanced Cyber Risk Management Standards Joint Advance Notice of Proposed Rule Making

Dear Agencies:

The Association of International Certified Professional Accountants (the Association) is pleased to offer its comments on the advance notice of proposed rulemaking (ANPR) regarding enhanced cyber risk management standards for large and interconnected entities and their service providers.

The Association combines the strengths of the American Institute of CPAs (AICPA) and The Chartered Institute of Management Accountants (CIMA) to power opportunity, trust and prosperity for people, businesses and economies worldwide. It represents 650,000 members and students in public and management accounting and advocates for the public interest and business sustainability on current and emerging issues. With broad reach, rigor and resources, the Association advances the reputation, employability and quality of CPAs, CGMAs and accounting and finance professionals globally.
We applaud the agencies' efforts to increase the operational resilience of entities and reduce the impact of cyber events. The Association believes 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 agencies regarding the accounting profession's efforts in the cybersecurity space, which we believe supports many of the ANPR objectives and will help to provide a common foundation for meaningful enterprise-wide cybersecurity risk management and reporting.

Background

CPAs have a long history of performing specialized audits of information technology internal controls. Since 1974, CPAs have been required to consider the effects of information technology on financial statements and reporting. Recognizing that customers' need for assurance extended beyond financial objectives, we developed the Trust Service Principles and Criteria (TSPC) in 2002 to provide a framework for CPAs to report on the design and operating effectiveness of security, confidentiality, availability, privacy and processing integrity controls (SOC 2 reports). As the use of outsourced services increased in the marketplace, the need for information to address risks associated with those outsourced services grew.

SOC 2 reports were developed to meet the needs of these users by providing information and assurance on the controls at a service organization that affect the security, availability, and processing integrity of the systems the service organization uses to process users' data, and the confidentiality and privacy of the information processed by these systems. Examples of stakeholders who rely on these reports include management or those charged with governance of the user entities and of the service organization, customers of the service organization, regulators, business partners, suppliers, and others who have an understanding of the service organization and its controls. These reports play an important role in oversight of the organization, vendor management programs, internal corporate governance and risk management processes, and regulatory oversight.

As the use of SOC 2 reports expanded throughout the marketplace, we noted a need for, and developed, guidance that allows SOC 2 reports to include other criteria related to HIPAA, FISMA, HITRUST, and other IT (security) requirements. Over time, SOC reports by CPA firms have become the standard for reporting on internal controls at a service organization as required by the U.S. Government, Security and Exchange Commission (SEC), the financial services industry, and standard contract terms with service organization users.
Building on the foundation of the SOC 2 service, we have also developed an entity-wide, examination-level cybersecurity risk management program attestation engagement, which is discussed in detail later in this document. Additionally, there are plans underway to develop attestation guidance for reporting to customers of manufacturers and distributors on cybersecurity risk in their supply chains.

Challenges Encountered

Our members regularly provide feedback to us regarding challenges they have encountered with respect to security and cybersecurity. Information about a few of those challenges that may be useful to you in the rule making process are as follows:

- Security standards and requirements created for a specific set of organizations regularly become contractual requirements for their service providers. Most organizations rely on service providers to perform critical business functions. Because of this dependency, organizations try to obtain, from service providers, contractual commitments to comply with the standards and requirements of the organization. Consequently, while the proposed rules are intended to be directly applicable to only a limited number of organizations, compliance with the rules will likely be required for numerous smaller service providers.
- As a result of customers contractually requiring compliance with security standards and requirements, most service providers are now required to comply with many different security standards and requirements established by various governments, agencies and industry associations.
- Current security standards and requirements take different approaches. Depending on the point of view of the party establishing the security standards or requirements, they may:
  - Necessitate the implementation of specific controls
  - Necessitate the implementation of specific processes

  Such approaches may not permit service providers the flexibility needed to implement an efficient and effective set of processes and controls that best address their individual risks and business objectives that are unique to their organizations and the environments in which they operate.

Many of these challenges may be mitigated or avoided by the proposed principles-based rules. The impact to service providers can also be lessened by providing for the use of any acceptable security framework that adequately addresses the principles. Security standards and requirements, of necessity, demand that organizations assess the risks arising from the use of service providers and interactions with other external parties, and manage those risks through the implementation of controls and monitoring. Many organizations address these requirements by making individual inquiries or performing compliance assessment procedures at service providers. Because many service providers serve numerous organizations across multiple industries and legal jurisdictions, the providers experience significant costs in addressing the procedures. This creates "audit fatigue" for the service providers' employees, and diverts security resources from operational duties to addressing customers' procedures. In establishing the requirements for assessing and managing risks by external parties, the agencies should consider how the use of independent third-party reporting, such as SOC 2 reports, in conjunction with other monitoring procedures, can reduce the additional burden that the rules will have on service providers and other external parities.

The SOC 2 reporting framework provides an effective means for service providers to communicate with users and provide them the transparency needed to make critical decisions. It utilizes a principles based approach that meets the needs of various users by (1) allowing management of organizations the flexibility to develop processes, procedures, and controls for risk management programs that address the risks that are unique to their organizations and the environments in which they operate, and (2) providing a consistent framework for evaluating those risk management programs.

Such flexibility and consistency has been the cornerstone for the success of SOC 2 and its usefulness to organizations in understanding how controls at service providers are integrated into their own frameworks, and is the premise behind our new entity-wide cybersecurity examination engagement. We believe both of these frameworks are supportive of, and compatible with, the agencies efforts.

Although the ANPR does not indicate an intent to establish external reporting requirements on the part of covered entities, we wish to emphasize that we believe such a requirement would not be beneficial at this time. Based on discussion with focus groups across a number of industries and the current dynamic nature of cybersecurity, we believe that the establishment of such a requirement is unnecessary and might distract organizations from efforts to improve the management of their cybersecurity risks. We believe that stakeholders are best served by a voluntary system of reporting that is market driven and encourages organizations to adopt an agile, strategic, objectives-based approach to cybersecurity risk management.
We also believe that the needs of the stakeholders for such reporting are materially different than the needs of a customer of a service provider when evaluating cybersecurity risk at that service provider. Whereas users of a service organization need information specific to the controls affecting the systems used at the service provider, entity-wide information is most useful for stakeholders of organizations in evaluating whether cybersecurity risk management programs address the unique cybersecurity risks of the organization as a whole, rather than a particular service.

<u>The Cybersecurity Risk Management Program Examination</u>

To address cybersecurity *within* the boundaries of an organization, we have developed an entity-wide, examination-level cybersecurity risk management program attestation engagement that CPAs can provide for their clients. Currently, CPAs provide cybersecurity examination services under a variety of generally accepted professional standards and approaches. However, we believe adoption of a more consistent, market-wide approach for CPAs to examine and report on an entity's cybersecurity risk management program 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 cybersecurity risk management program using a common language. We are also developing related guidance to enable the CPA professional to provide independent assurance on the effectiveness of an entity's cybersecurity risk management program via a report designed to meet the needs of a variety of potential users.

Specifically, we are developing the following:

- Suitable criteria for the cybersecurity examination engagement including:
  - Criteria, called 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 certified public accounting firms to report on management's description.
    - Criteria, called 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 cybersecurity 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. This examination engagement is intended to provide third-parties with:
    - A narrative description, prepared by management, describing the entity's cybersecurity risk management program using the description criteria described above or another suitable set of criteria;
    - Management's assertion that the narrative is presented in accordance with a defined set of suitable description criteria, and that the controls described within that program are effective to achieve the entity's cybersecurity objectives based on a defined set of suitable control criteria; and
    - The independent certified public accountant's report on the presentation of the description, and the operating effectiveness of the controls.

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 has inherent value to the organization and its stakeholders on its own, and in the context of a voluntary, independent third-party attestation engagement, also 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, we are 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, and to have a strategic, risk management-oriented focus to arm those charged with governance with the information they need for appropriate oversight. Accordingly, the criteria have been drafted with a view to establishing the universe of controls that should be addressed for cybersecurity risk management. We think this will give organizations a level of comfort that they've adequately considered the best practices covered by the most commonly referenced control and cybersecurity frameworks, regardless of which cybersecurity risk management framework(s) they've chosen to implement internally.

Importantly, we believe that the decision to undergo an independent cybersecurity risk management examination should be market driven and voluntary, resting with the board and management of each company, and not be dictated by a government regulation or mandate. We have designed the engagement and related criteria to be both *voluntary* and *flexible* because cybersecurity risk is a complex and rapidly changing challenge. We believe such an approach is preferable to the implementation of specific compliance requirements, which may quickly become obsolete, and worse yet may take a company's focus away from proactively monitoring and addressing their most critical cybersecurity vulnerabilities, which can be expected to change on a regular basis. Companies are in the best position to understand and adapt to evolving vulnerabilities through the design, implementation and monitoring of responsive controls.

We have developed our framework for cybersecurity risk management reporting with a view to improving the usefulness of cybersecurity risk-related information in the marketplace; taking a holistic view of cybersecurity, enhancing consistency and comparability of communication and assessment, while addressing the information needs of a wide variety of stakeholders. We hope that a bi-product of this effort will be a reduction in the number of disparate cybersecurity information requests and compliance requirements placed on companies, thereby enabling companies to take a more strategic and proactive approach to their cybersecurity risk management efforts. We believe that the regulatory community can best serve the public interest and national security by coordinating to establish and implement common, overarching principles related to cybersecurity risk management. A consistent set of high-level principles or best practices (as opposed to specific, detailed, prescriptive rules or requirements), would keep the focus on agility and responsiveness to an ever-evolving challenge, to stay one step ahead of, not behind, current and future risks. Such

principles could lay out minimum expectations with respect to the five categories laid out in the ANPR, however any detailed or prescriptive requirements are likely to either be of limited ongoing value, or may be duplicative to existing cybersecurity risk management frameworks. These principles would be most useful to the extent that they encourage the meaningful application of existing frameworks and standards, which are maintained and updated on a regular basis by the organizations that publish them. As noted above there are already a number of strong voluntary cybersecurity risk management frameworks available to companies to follow in designing effective cybersecurity risk management programs. We believe that the cybersecurity risk management *reporting* framework that we have developed complements these frameworks and serves as a critical step to enabling a consistent, market-based, business-based mechanism for companies to effectively communicate with key stakeholders on how they're managing cybersecurity risk. It is well understood that it is impossible to guarantee the prevention of a cybersecurity breach, however this framework will enable companies to demonstrate and communicate due diligence and due care in their management of cybersecurity risk in a consistent manner, serving the needs of multiple stakeholders with a single approach.

The accounting 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 contact Amy Pawlicki, the Director of Business Reporting, Assurance & Advisory Services, at Amy.Pawlicki@aicpa-cima.com or 212-596-6083.

Sincerely,

Susan S. Coffey, CPA, CGMA

Executive Vice President - Public Practice

Association of International Certified Professional Accountants

AICPA / CIMA