CENTER FOR AUDIT QUALITY

Serving Investors, Public Company Auditors & the Markets

January 17, 2017

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-XXXX
RIN 7100-AD16

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 Rulemaking

Dear Agencies:

The Center for Audit Quality (CAQ) is an autonomous public policy organization dedicated to enhancing investor confidence and public trust in the global capital markets. The CAQ fosters high quality performance by public company auditors, convenes and collaborates with other stakeholders to advance the discussion of critical issues requiring action and intervention, and advocates policies and standards that promote public company auditors' objectivity, effectiveness, and responsiveness to dynamic market conditions. Based in Washington, DC, the CAQ is affiliated with the American Institute of CPAs (AICPA).

The CAQ welcomes the opportunity provided by the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation (collectively, the agencies) to comment on an advance notice of proposed rulemaking regarding enhanced cyber risk management standards for large interconnected entities under their supervision

and those entities' service providers (the ANPR). This letter represents the observations of the CAQ, but not necessarily the views of any specific firm, individual, or CAQ Governing Board member.

CAQ Background and Auditing Profession Perspective

The CAQ's members are audit and consulting firms that perform financial statement audits of public companies. Many of these firms also provide a wide range of audit and consulting services across all industry sectors, providing them with the opportunity to observe cyber readiness in a variety of entities and contexts.

Accordingly, our observations in this letter are drawn from many stakeholder groups and various industry sectors. Indeed, the auditing profession is in a strong position to play an important role in fostering instructive conversations about cybersecurity risk management, bringing to bear its core values—including independence, objectivity, and skepticism—as well as its deep expertise in providing independent evaluations in a variety of contexts.

CPAs have been actively engaged in information security for decades, and already provide valued cybersecurity risk management support to their advisory clients. Beginning in 1974, CPAs were required to consider the effects of information technology on financial statements. This evolved into the development of attestation engagements dealing with controls at a service organization, as well as other information security consulting services offered to the market. Today, four of the leading 10 information security/cybersecurity consultancies are CPA firms and CAQ members. From the broad perspective we have gained through direct contact with our member firms and our own interaction with interested parties (e.g., chief information officers, internal auditors, audit committee members, academics and financial reporting executives), we have summarized a number of key observations with the current state of readiness and response by the public company community to cyber risks.

Key Considerations from the Auditor's Vantage Point

Cyber Risk Governance

We agree with the agencies that "a key aspect of cyber risk governance is developing and maintaining a formal cyber risk management strategy, as well as a supporting framework of policies and procedures to implement the strategy, that is integrated into the overall strategic plans and risk governance structures of covered entities."[1] Effective governance in this critical area requires appropriate oversight of management's strategy and its implementation. We believe all stakeholders, including regulatory authorities, benefit when the board of directors has oversight responsibility related to how a company is dealing with its cyber risks. Each company is unique, and therefore a 'one-size-fits all' approach to cybersecurity risk management would not be sufficiently agile to adapt to the variety of cyber risks each company faces. Accordingly, we believe boards should have flexibility as to how they approach and execute that oversight.

No matter how a board chooses to structure its cybersecurity risk oversight, there are some things that we believe all boards should consider. In June 2014, the National Association of Corporate Directors (NACD) released the *Cyber-Risk Oversight Handbook* (the Handbook) for directors.[2] The Handbook outlines five key principles for directors to consider in executing their oversight responsibilities related to cybersecurity. Those principles are:

1. Approaching cybersecurity as an enterprise-wide risk issue;

[1] See page 23 of the ANPR.

[2] https://www.nacdonline.org/Resources/Article.cfm?ItemNumber=10688

2. Understanding the legal implications of cyber risk as they relate to the company;

3. Giving cyber regular time on the board's agenda;

4. Expecting management to establish a cyber-risk management framework; and

5. Recognizing that discussion of cyber risks should include identification of which risks to avoid, accept, mitigate or transfer through insurance, as well as specific plans associated with each approach.

As part of the third principle listed above, the *Handbook* suggests that boards should have adequate access to cybersecurity expertise. In today's marketplace, generally speaking, two perspectives on the level of cyber expertise needed on a board have emerged. One is that there should be a cyber-expert on the board (or the audit or risk committee —wherever the responsibility for cyber risk oversight lies). The other is that the board would not have a cyber-expert resident on the board but would have sufficient access to cybersecurity expertise in order to fulfill its oversight role.

We believe that it is more important for cyber expertise to reside within the company and that the oversight role of the board or audit or risk committee can be best served by the use of outside consultants when and if it is needed. The thinking here is that rather than serving as a repository of cyber expertise, directors should excel at their core role of overseeing management. In other words, the director's job is to understand the company's cybersecurity risks broadly, and ask probing questions about how management is dealing with those risks as part of its overall enterprise risk management program. The dynamic nature of technology and cyber threats, as well as the limited number of resources who may be considered "cyber experts," also makes the case for utilizing a combination of company and external resources.

No matter which of these alternative approaches prevails, audit and risk committees and other board members may need additional resources, tools, or training to help them get up to speed in this dynamic area so they can best discharge their responsibilities. We believe it should be the board's decision how to best organize the talent and expertise needed on the board, or one of their committees, to best serve shareholders.

Resources

We agree in principle that covered entities subject to the ANPR should work to "effectively identify, monitor, measure, manage and report on cyber risk."[3] The enhanced standards would require integrating cyber risk management into the responsibilities of at least three independent functions (such as the three lines of defense risk management model).[4] In addition, it appears that the ANPR would require each of these three functions to assess or test cybersecurity controls. This would likely result in companies needing to hire additional experts in cybersecurity and could potentially result in a redundancy of efforts already under the purview of internal audit. It could also have an unintended consequence of potentially distracting existing cybersecurity experts from their core mission.

Other requirements of the ANPR likely would require the ramp-up of cyber expertise in other areas as well (e.g., within business units and risk management)—a challenge given a workforce where qualified cyber experts are in relatively short supply.[5] The ANPR states that "the agencies are considering [whether] to apply the standards to third party service providers with respect to services provided to depository institutions and

[3] See page 27 of the ANPR.
[4] See page 26 of the ANPR.
[5] Cisco 2016 Annual Security Report, Cisco, Jan. 2016

their affiliates that are covered entities (covered services)."[6] We believe it is important that entities have the ability to scale their resource needs according to assessed risks, including third-party risks, and any guidance put forth by the agencies should allow entities the flexibility to be responsive to their own risk assessment and response plans.

Compliance Environment

Cybersecurity, like other new and challenging business and compliance risks, has already spawned a multitude of responses and proposed solutions. One goal of the agencies should be to align and focus the range of response to cybersecurity risks—and to avoid exacerbating compliance efforts with yet another layer of prescribed activities. Policymakers at all levels of government and industry should prioritize harmonizing cybersecurity regulations.

The demand for effective organizational cybersecurity risk management and information on organizations' cybersecurity risk management efforts has led to the development of numerous risk management frameworks that provide guidance to organizations on how to manage cybersecurity risk (e.g., ISO/IEC 27001, NIST Cybersecurity Framework).[7]

The existence of multiple, disparate frameworks and programs—and different stakeholders' preferences for each—has created a challenging environment for organizations trying to design and implement an effective cybersecurity risk management program. We encourage the agencies to give full consideration as to how any additional requirements would align with existing frameworks.

As written, the ANPR runs the risk of establishing yet another framework in a long line of prescriptive policies that have emerged domestically and internationally. In October 2016, the Department of Treasury publicly supported the publication of the Group of 7 (G-7) Fundamental Elements of Cybersecurity for the Financial Sector (the G-7 Elements).[8] Released by finance ministers and central bank governors of the G-7 countries, the G-7 Elements provide a concise set of principles on best practices in cybersecurity for public and private entities in the financial sector.

The ANPR does not provide clear indication about how those G-7 Elements are to be considered, if at all, in relation to the proposed rule. It is also not clear what current compliance requirements, if any, would be replaced or superseded by requirements contemplated by the ANPR. Any rulemaking in the cybersecurity space should endeavor to reduce the compliance and communication burdens companies face and reduce the number of information requests from stakeholders and the amount of information sought if such requests are made. The end result should not be compliance with a process, but the establishment of a cybersecurity risk management program that provides an appropriate level of cybersecurity risk management tailored to the company and its risk tolerance.

We recognize that monitoring is an important aspect of cybersecurity risk management. Organizations and their stakeholders need timely, useful information on cybersecurity risk management efforts to drive decision making. Corporate directors and senior management have begun requesting reports on the effectiveness of their cybersecurity risk management programs from independent third-party assessors. Yet until now there has been no widely accepted approach or professional standard for providing cybersecurity assessments in response to regulator or other stakeholder requests.

---

[6] See page 15 of the ANPR.

[7] AICPA's Cybersecurity Reporting: A Backgrounder, http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/Cybersecurity/AICPA_Brief_Cybersecurity.pdf

[8] https://www.treasury.gov/press-center/press-releases/Pages/ l0570.aspx

The Value of a Principles-Based Approach

The AICPA is working to develop a voluntary, market-based solution to report on cybersecurity risk management that could enhance public trust in the effectiveness of a company's cybersecurity risk management programs.[9] Implementing fundamental principles related to cyber hygiene and examining the effectiveness of their implementation could better arm boards, senior management, and other key stakeholders to drive forward their company's cybersecurity and resiliency. We believe this approach, which establishes the policies, processes and controls that should be addressed for cybersecurity risk management, rather than additional compliance procedures focused on a static set of minimum requirements, could better serve the needs of stakeholders, including regulators. As cybersecurity maturity increases, it will also serve as the requisite foundation for high quality, independent third-party assurance services, which will necessarily evolve over time to address changing market dynamics and needs.[10]

We agree that it is in the public's best interest to protect and promote financial stability and mitigate cyber risk within the most critical sectors and entities, and their service providers. We believe there would be benefits to a principles-based, converged approach among financial and other regulators related to cybersecurity and resilience. The G-7 Elements provide a good example of high level, guiding principles for effective cybersecurity risk management. Principles provide the building blocks upon which a company can design and implement its cybersecurity strategy and operating framework, informed by its approach to risk management and culture. Companies would then be allowed to choose from the myriad frameworks and criteria available (e.g., COSO, NIST, ISO 27001, AICPA Trust Services Criteria and Cybersecurity Description Criteria) and determine what best suits their needs and risk appetite to satisfy the principles. Having a principles-based approach also allows for a more dynamic process through which a company can systematically re-evaluate its cybersecurity strategy and framework as the operational and threat environment evolves.

***

The CAQ appreciates the opportunity to comment on the ANPR and would be pleased to discuss our comments or answer any questions that the agencies may have regarding the views expressed in this letter.

Sincerely,

Cynthia M. Fornelli
Executive Director
Center for Audit Quality

[9] http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPACybersecurityInitiative.aspx

[10] http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/Cybersecurity/Fact_Sheet_Cybersecurity_Risk_Management.pdf