THE RISK MANAGEMENT ASSOCIATION

1801 Market Street, Suite 300 • Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

January 13, 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, D.C. 20219

Robert deV. Frierson, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, D.C. 20551

Robert E. Feldman, Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, D.C. 20429

Re: **Enhanced Cyber Risk Management Standards** (the "ANPR"): **Office of the Comptroller of the Currency** 12 CFR Part 30, Docket No. OCC-2016-0016, RIN 1557-AE06; **Federal Reserve System**, 12 CFR Chapter II, Docket No. R-1550, RIN 7100 AE-61; **Federal Deposit Insurance Corporation**, 12 CFR Part 364, RIN 3064-AE45

Ladies and Gentlemen:

This letter is submitted by The Risk Management Association ("RMA" or the "Association") in respect of the Advanced Notice of Proposed Rulemaking, "Enhanced Cyber Risk Management Standards" (the "ANPR"), which is intended to increase the operational resiliency of large institutions and reduce the impact on the financial system in the event that any such institution were to experience a cyber-attack.

Background

RMA is a 501(c) (6) not-for-profit, member-driven professional association whose sole purpose is to advance the use of sound risk management principles in the financial services industry. RMA helps its members use sound risk management principles to improve institutional performance and financial stability and enhance the risk competency of individuals through information, education, peer-sharing and networking. RMA has 2,500 institutional members that include banks of all sizes as well as nonbank financial institutions. They are represented in the Association by more than 18,000 risk management professionals who are chapter members in financial centers throughout North America, Europe, and Asia/Pacific.

THE RISK MANAGEMENT ASSOCIATION

1801 Market Street, Suite 300 • Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

One of the most important components of RMA's mission is to provide independent analysis on matters pertaining to risk management and capital regulation. In this regard, the comments contained herein are informed by subject matter experts from member institutions of the Association having $50 billion or more in assets, including risk practitioners, information security experts, and internal legal counsel of member institutions.

Commentary

RMA is generally supportive of the agencies' work to determine whether to establish enhanced standards for the largest and most interconnected entities under their supervision. We respectfully submit that the agencies consider clearly defining the relationship between cyber risk and information security in any forthcoming guidance or rulemaking and mapping any resulting guidance or regulation to the NIST Framework given that most, if not all, of the institutions which would be covered by such guidance or rule align with the NIST Framework.

Principles-Based Approach

The ANPR presents an opportunity for the agencies to establish a principles-based national standard in the financial services industry for regulators in other industries and jurisdictions to follow.

RMA respectfully submits that the agencies consider not simply whether there is a need for enhanced standards, but the outcome intended to be achieved by covered institutions in the event of a cyber event. RMA notes that the industry, while having access to threat information through FS-ISAC, is at a disadvantage because it does not necessarily have timely access to the threat intelligence generated by law enforcement. RMA believes that there should be a mechanism to permit the sharing of credible threat intelligence by law enforcement in order for institutions to take such actions as may be necessary to deter the resulting threat. In that regard, RMA respectfully suggests that any resulting enhanced standards developed by the agencies should be issued as guidance as opposed to a rule-making given the rapid speed by which the industry is changing, the concomitant pressure to innovate, and the evolving nature of cyber threats, including, but not limited to, the intentions of the actors.

Further, RMA respectfully submits that recent experience has demonstrated that the nature of cyber risk continually evolves. Early trends in cyber risk were associated with theft of financial account information or other personally identifiable information. While those threats continue to exist, new threats have evolved to include the business interruption, loss of access to data, and potential corruption of data that can result from ransomware attacks; the theft of money from accounts seen in recent attacks on the SWIFT interbank system; the increasing use of "business executive compromise" schemes involving spoofed emails; the use of stolen emails and strategic planning information for competitive purposes such as causing embarrassment or undermining confidence in an organization; and the looming risks of personal injury and property damage that could be associated with attacks on devices in the Internet of Things. These changes in the threat landscape are occurring rapidly and unpredictably, making it extremely difficult for any organization to fully assess and plan for cyber risk. Further the federal government has more

THE RISK MANAGEMENT ASSOCIATION

1801 Market Street, Suite 300 • Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

comprehensive knowledge of current and expected trends in cybersecurity risks, and how those risks may be defended against.

RMA believes that the regulatory agencies should take a principles-based, as opposed to a prescriptive, approach to the supervisory oversight of enhanced cyber risk management standards consistent with the enterprise-wide approach to risk management articulated by the agencies in heightened standards, enhanced prudential standards, and other applicable regulation and guidance. RMA believes that the regulatory agencies should focus attention on the "outcome" of effective cyber risk management programs rather than attempting to harmonize the "method" of designing and implementing such programs by each covered institution.

Scope

We submit that standards premised on asset size alone are inconsistent with the broader threat to institutions and the financial system generally. For example, the agencies have prescribed a 5% threshold for determining whether institutions would be required to comply with the higher set of expectations for "sector critical standards." The 5% threshold is an arbitrary setting and is not necessarily appropriate because it is not risk-based. Accordingly, RMA submits that prior agency promulgations to consider size, scale, complexity, risk profile and nature of operations should also inform the establishment of any guidance or rulemaking in respect of enhanced cyber risk management standards. In addition, to the extent that standards are imposed based upon asset size, an unintended consequence could be that the marketplace believes, perhaps incorrectly so, that institutions below any such threshold are less resilient, which could result in a loss of business or increased cost of capital. Additionally, there is a concern that the wide scope of this proposed guidance could potentially capture several entities for whom regulation is both prohibitively expensive and burdensome.

A related point that the agencies should consider is that all institutions should be held accountable to maintain robust risk management standards that evolve with the evolving nature of cyber threats by, for example, leveraging the FFIEC cybersecurity assessment tool.

We note that "cyber-attacks continue to target companies that provide cybersecurity risk-mitigation products and services to banks, potentially amplifying the breadth of affected institutions through a common access point."[1] And we note again that institutions frequently do not have the kinds of information available to the federal government that would make it possible to anticipate the ways in which cyber threats may evolve. Consequently, any regulations should anticipate that institutions' risk management approaches are only expected to address known risks, not to anticipate currently unfamiliar ones, and should also provide guidance on which federal agency reports, analyses, or other information institutions are entitled to rely on as the catalogue of cyber risks the institutions are expected to consider as they carry out their risk management activities. RMA respectfully submits that such a catalogue should include federal agency guidance on best practices to mitigate those risks,

[1] OCC Semiannual Risk Perspective, Spring 2016, p. 8.

1801 Market Street, Suite 300 • Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

and that consideration of the catalogue of risks in cyber risk management planning should appropriately be considered a safe harbor of sorts; that institutions that take into account those listed risks cannot be penalized for failing to anticipate a risk that was previously unknown; and that each time that a new type of risk is added to the list, guidelines are issued which allow a reasonable amount of time for institutions to incorporate that particular risk into their overall risk management efforts.

Recovery Time Objective

The ANPR notes that the IT Handbook requires institutions to establish RTOs, recovery and resilience strategies that should address the potential for malware or corrupted data to replicate or propagate through connected systems or high availability solutions. RMA would caution the agencies regarding the mandate of RTOs, noting that it is highly unlikely that an institution would be able to ascertain the scope and impact of a cyber incident, let alone be confident that a system would be clear for all operations within any particular prescribed time.

Third Party Risk Management

RMA's members recognize that the use of third parties increases the risk that a third party could become the gateway to a cyber-attack affecting one or more institutions. Accordingly, we believe that it is important to note that due to the difficulty in monitoring third parties' cyber risk management practices, it is increasingly likely that concentration risk will increase as institutions migrate to third parties that are believed to possess both superior technologies and risk management practices. Several issues could result, such as: (i) widespread contagion should a third party's systems be breached; (ii) certain third parties could become "too big to fail"; and (iii) as third parties increase in size, certain of them will enjoy superior negotiating leverage compared to smaller institutions, which could have the unintended consequence of smaller institutions doing business with such third parties on less favorable terms than larger institutions.

In addition, RMA notes that the agencies have issued guidance on outsourcing and third party risk management. RMA respectfully suggests that great care be given to harmonize any resulting guidance on enhanced cyber risk management standards with such third party risk management guidance in order to avoid gaps in coverage and overlapping and potentially inconsistent standards.

Risk Management and Governance

In the United States, corporate governance traditionally has been carefully balanced between the board of directors, which is charged with policy formulation and oversight, and senior management which is charged with execution of policy and strategy and the day-to-day operations of the business. The agencies are considering a requirement that the board of directors have "adequate expertise" in cybersecurity or maintain access to staff or resources with such expertise. We note that there is a recognition that directors have difficulty in engaging in credible challenge with respect to cyber risk and applaud the agencies for adding the caveat that boards may discharge their duties under the enhanced standards by having access to staff or resources. We would suggest that in any guidance or rule that the agencies make clear that the board is entitled to rely upon the advice or judgment of an

1801 Market Street, Suite 300 • Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

institution's Chief Information Security Officer or outside consultant in discharging its obligations regarding cyber risk management.

In addition, we note that the three lines of defense model articulated in the ANPR calls for cyber risk management to be embedded in the first line of defense, which would not typically apply to institutions that are not regulated by the OCC. Participants observed that the ANPR introduces non-OCC-regulated institutions to the concepts articulated in the "Heightened Standards" guidance, but only as such standards apply to cyber risk. RMA believes this to be a fragmentary approach in singling out cyber risk for this regulatory framework as it applies to non-OCC banks.
A related point is that while internal audit is a key component of the three lines of defense model, internal audit may lack the expertise to assess whether an institution's cyber risk management framework is appropriate or effective for its size, complexity, interconnectedness, and risk profile.

Quantification of Risk

The ANPR provides that the agencies are seeking to develop a consistent, repeatable method to support the ongoing measurement of cyber risk. As you know, RMA's AMA Group has worked for more than a decade on AMA implementation and related issues and we draw from that general experience in connection with the following comment. RMA believes that basic metrics regarding cyber risk quantification are possible (e.g., number of unpatched known vulnerabilities; percentage of third party software that has been scanned prior to deployment), but that more robust quantification would rely on scenario analysis. Cyber risk, like third party risk, is a subset of operational risk, and cyber risk, like operational risk generally, would be very difficult to model. We respectfully suggest that were the agencies to prescribe modelling (as opposed to measuring basis metrics as noted above), there would be a significant resulting misallocation of resources whereby institutions would focus on quantification and measurement instead of risk management.

* * * * *

Conclusion

While there appear to be some signs of convergence on certain aspects of cyber risk management programs, RMA believes that there should not be an expectation that all aspects of practice will or should eventually converge. Accordingly, the supervisory community should apply a principles-based approach, as opposed to a prescriptive one, to ensure that institutions have the freedom and flexibility to independently innovate to respond to evolving cyber risks. In other words, RMA believes that the industry should not move in lockstep to a particular state of readiness which may have the unintended consequence of creating a large scale and common vulnerability which could be exploited by bad actors. In short, the supervisory community does not want to inadvertently thwart ingenuity and problem solving brought to bear by diverse industry participants through a prescriptive, by-rote approach to the promulgation of enhanced standards.

1801 Market Street, Suite 300 • Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

Should there be any questions concerning the comments above, kindly contact Edward J. DeMarco Jr., General Counsel and Director of Regulatory Relations at (215) 446-4052 or edemarco@rmahq.org.

Very truly yours,

Edward J. DeMarco, Jr.,
General Counsel and
Director of Regulatory Relations