Derek B. Dorn
Managing Director, Regulatory Affairs and Policy |
Associate General Counsel

730 Third Avenue | 12th Floor
New York, NY 10017

212 913-1038
Derek.Dorn@tiaa.org

February 17, 2017

Robert deV. Frierson
Secretary
Board of Governors of the
Federal Reserve System
20th Street & Constitution Avenue, N.W.
Washington, DC 20551

Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
400 7th Street, S.W.
Suite 3E-218
Mail Stop 9W-11
Washington, DC 20219

Robert E. Feldman
Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, DC 20429

Re: Advance Notice of Proposed Rulemaking for Enhanced Cyber Risk Management Standards (Federal Reserve Docket No. R-1550, RIN 7100-AE-61; OCC Docket ID OCC-2016-0016; FDIC RIN 3064-AE45)

Ladies and Gentlemen:

Teachers Insurance and Annuity Association of America ("TIAA") appreciates the opportunity to comment on the Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards released by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency (collectively the "Agencies") on October 19, 2016 and published in the *Federal Register* on October 26, 2016 (the "ANPR").[1]

We agree with the Agencies that robust cybersecurity programs are vital to protecting consumers and upholding the integrity of our nation's financial infrastructure.

---

[1] Capitalized terms not otherwise defined herein correspond to the definitions in the ANPR; similarly, numbered or lettered sections and clauses herein correspond to the sections and clauses so referenced in the ANPR.

We believe the optimal cybersecurity program is a risk-based system of layered controls that are overlapping and reinforce each other. As part of a virtuous cycle of increasing overall security, these controls should adjust, individually or in tandem, to emerging risks. However, any standard that prescribes specific controls will become obsolete over time, and in the particularly dynamic world of cybersecurity this obsolescence may develop quickly.

We also agree with the Agencies that regulatory supervision plays a vital role in encouraging firms to adopt and maintain robust cybersecurity programs. We respectfully submit that rather than mandating specific controls, the most effective regulatory framework emphasizes regulatory examinations to assess whether a regulated firm's controls are adequate to address risks posed by cybersecurity breaches.

Background on TIAA.

Founded in 1918, TIAA is the leading provider of retirement services for those in academic, research, medical, and cultural fields. Over our nearly century-long history, TIAA's mission has always been to aid and strengthen the institutions and participants we serve and to provide financial products that meet their needs. To carry out this mission, we have evolved to include a range of financial services, including asset management and retail services. Today, TIAA manages over $915 billion in assets, and our investment model and long-term approach aim to benefit the 5 million retirement plan participants we serve across more than 16,000 institutions.[2] With our strong nonprofit heritage, the mission we embarked on in 1918 still rings true as we remain dedicated to serving the financial needs of those who serve the greater good.

By virtue of its ownership of TIAA-CREF Trust Company, FSB ("TIAA-FSB"), TIAA is subject to regulation by the Board of Governors of the Federal Reserve System as a savings and loan holding company ("SLHC"). TIAA-FSB was chartered in 1998 for the limited purpose of exercising trust powers. In 2010, TIAA-FSB received regulatory approval to expand its activities to include deposit-taking and lending. As of November 30, 2016, TIAA-FSB had total assets of $4.3 billion and total deposits of $3.4 billion. TIAA-FSB's headquarters are in St. Louis, Missouri, and it has no branch offices. TIAA-FSB's retail deposit products and services are primarily offered through the internet and through referrals from registered representatives of its affiliate TIAA-CREF Individual & Institutional Services, LLC.

---

[2] Asset, participant, and employee data are as of September 30, 2016.

Support for the Agencies' Efforts.

We commend the Agencies for their focus on protecting consumers and bolstering the stability of our nation's financial infrastructure through robust cybersecurity practices in the financial-services industry. We further appreciate that the Agencies have taken a deliberative approach, soliciting an initial round of comments to the ANPR from stakeholders and the public, with additional opportunities for comment to come if and when the Agencies issue a notice of proposed rulemaking. Our comments are offered in the spirit of fortifying the resiliency of all firms across the financial-services industry.

We agree that all financial-services firms should maintain a robust and regularly tested cybersecurity program managed by experienced professional staff with technical expertise, and overseen by senior management and the board of directors. Such a program must include risk assessments of business processes, as well as layered controls to address such risks. But unduly prescriptive mandates could undermine such an approach, as the effectiveness of cybersecurity controls cannot be known outside the context of a tailored risk-assessment.

Accordingly, we respectfully submit that the most effective regulatory framework should emphasize supervisory examinations to assess whether a regulated firm's controls are adequate to address risks posed by cybersecurity breaches.

Risk-Based System of Layered Security.

TIAA utilizes a risk-based system of layered controls that aims to prevent, detect, and resolve issues relating to data security. This program includes physical, administrative, and technological controls to (i) protect the security and confidentiality of information belonging to both customers and TIAA, (ii) defend against anticipated threats or hazards to the secrecy or integrity of customer and company information, and (iii) protect against unauthorized access to or use of customer or company information. The controls described in our information technology policy and standards are tailored to the severity of potential financial and reputational impacts to TIAA associated with data security risks.

As it is statistically impossible to eliminate risk altogether, a sophisticated information security program such as TIAA's manages risks according to the sensitivity of information assets. Here, we briefly describe the principles that inform our program.

TIAA's robust risk-based information security program begins with a disciplined qualitative or quantitative determination of foreseeable risks that specific business processes pose to information assets' integrity and security. Inherent risk, without regard to any mitigating controls, is determined by assessing the likelihood or probability of a specific attack against a known or foreseeable vulnerability, multiplied by the magnitude of loss that would result. For instance, if an attack were to compromise highly sensitive information assets, the resulting damage would be

far greater than a successful attack on information assets consisting solely of public information.

After determining inherent risk, TIAA's program designs a combination of physical, administrative, and technical controls to mitigate identified vulnerabilities to an acceptable level. The acceptable level varies depending on the nature of the information – an acceptable level of residual risk should certainly be lower for sensitive information assets than for non-sensitive, public information assets. Accordingly, different controls may be designed for information assets of differing sensitivity. If controls do not reduce residual risk to the desired level, then the controls must be re-designed until they do. Thereafter, such controls' residual risk should be monitored and assessed as business conditions change, and based upon the risk of the information asset.

Absent this continuous risk-assessment and control monitoring process, it is impossible to determine whether a particular control will over-protect or under-protect a specific asset. In fact, a single control may be more costly and less effective in reducing residual risk than layers of different types of controls. Mandating a single, specific control, therefore, may not have the intended result of mitigating the damage a cyberattack would cause – and a single control may divert needed resources from designing and implementing a more effective alternative control(s).

In TIAA's view, regulatory examiners are already well-positioned to assess whether a firm's chosen controls are adequate to address inherent risks and reduce overall residual risk within the firm's complete environment of layered controls. Moreover, any gaps in a specific firm's information security program are best addressed after exams. For these reasons, TIAA recommends a risk-based system of layered security and regulatory oversight that emphasizes supervisory examination over strictly codified mandates.

Against this backdrop, we offer below our responses to the Agencies' questions posed in the ANPR. The responses are organized by Section within the ANPR.

Scope of Application.

The Agencies have invited comment regarding enhanced cyber-risk management standards ("enhanced standards") for large and interconnected entities under the Agencies' supervision. The Agencies are considering applying enhanced standards to certain entities with total consolidated assets exceeding $50 billion.

Our foremost concern is the proposed reliance on a consolidated-asset threshold to apply enhanced cybersecurity requirements. In our view, reliance on such a threshold does not sufficiently account for a particular firm's individual risk characteristics. In particular, we encourage the Agencies to adopt a principles-based approach that accounts for the lower risk profile of covered entities that are

insurance companies – particularly life insurance companies like TIAA. If the Agencies do not tailor their approach, and instead adhere to a bright-line test focused solely on consolidated assets, insurance companies will be negatively impacted solely by virtue of general-account assets they maintain under insurance regulatory requirements designed to mitigate risk.

To underscore this point, it bears briefly recalling certain fundamental aspects of life insurance companies' investment and risk profiles. Insurance investments rarely entail the risk of mismatch of assets and liabilities often present in other financial institutions such as banks. And because the payment of benefits is tied to the occurrence of specific events (*e.g.*, annuities begin payment at a specified age or date), insurance liabilities tend to operate independent of the business cycle and are not a function of economic conditions. In fact, life insurers' stable liability profiles provide them greater freedom to choose to sell assets, and they are unlikely to be forced to liquidate assets to satisfy short-term obligations. Extensive regulation of the safety of insurance assets further limits any inappropriate risk-taking in which an insurance company might engage.

Moreover, insurance companies tend not to be interconnected with systemically important financial institutions to the degree banks are. For interconnected entities, a cyberattack or failure poses a threat not only to the entity itself but to other financial institutions with which the entity is connected. This spillover effect could have potentially systemic consequences if the affected firms play an important role in U.S. payment, clearing, and settlement arrangements, or provide access to credit for businesses and households. Insurers, on the other hand, do not provide payment, clearing, or settlement arrangements, nor do they provide credit the way banks do. They are usually not interconnected with other systemically important financial institutions such that a failure at the insurer would have systemic consequences. Whereas the interconnectedness of depository institutions means that a failure at one bank has the potential to amplify risk across the financial sector, insurers by their very nature absorb risk – they accept policyholder premiums, invest those premiums for stable (sometimes long-term) duration, and pay out claims over time, in direct contrast to the potential run risk inherent to depository institutions.

As insurance companies tend to have lower risk profiles and a limited degree of interconnectedness with other systemically important financial institutions, a principles-based approach is far more appropriate. Such an approach would enable the Agencies to determine when an entity's business model and activities pose sufficient risk to warrant application of enhanced cybersecurity standards.

Sector-Critical Systems.

The Agencies are considering implementing enhanced standards in a tiered manner, imposing more stringent standards on the systems of covered entities that are critical to the functioning of the financial sector. As discussed above, the breach of a covered entity that engages mostly in life and annuities insurance activities, such as

TIAA, would likely not pose systemic risk – and therefore such entities should not be considered to have sector-critical systems.

Governance.

We respectfully submit that the governance provisions within the ANPR are overly prescriptive. The Agencies are already well-positioned to assess the adequacy of governance through the examination process, which renders unnecessary prescriptive mandates.

The Agencies are considering a requirement that covered entities develop a written, board-approved, enterprise-wide cyber-risk management strategy that is incorporated into the entity's overall business strategy and risk management. TIAA respectfully submits that a board's role is to approve strategy, commit resources to implement that strategy, and be informed of the maturity of the financial institution's cybersecurity program in general, rather than to review and implicitly approve the myriad technical aspects of a written cybersecurity program. It is not customary for a board to adopt technical policies and procedures of this sort or review changes to them. Rather, this is generally a management function delegated by the board.[3] Along these lines, TIAA respectfully submits that the oversight and implementation of a covered entity's cybersecurity program is best entrusted to senior management as opposed to the board, as management is more knowledgeable of the covered entity's operations and risk factors.

The Agencies also are considering requiring senior leaders with responsibility for cyber-risk oversight to be independent of business-line management and have direct, independent access to the board of directors. TIAA respectfully recommends against a mandate that imposes specific reporting structures bringing all elements of a covered entity's cybersecurity program under one common manager. In many financial institutions, the business continuity function is separate from cybersecurity – yet cybersecurity is a crucial aspect of business continuity. While these two functions must work together seamlessly, it seems unnecessary to require that both be housed within the same reporting structure.

The ANPR appears also to require that a covered entity's cybersecurity policies be drafted as a *single* policy. But many information security programs consist of a framework that links together various policies and procedures. This practice allows for staggered review and revisions of relevant policies and procedures, either annually or as business conditions change. We urge the Agencies to preserve flexibility for such frameworks.

---

[3] Elevated board supervision of cybersecurity policies may be required for OCC-regulated depository institutions. That requirement should not extend beyond the depository institution to the parent or other affiliated entities.

Risk Management.

The Agencies appear to favor a "three lines of defense" risk management model composed of (i) business units, (ii) independent risk management with reporting lines that "must be clear and separate from those for other operations and business units," and (iii) an audit function. TIAA recognizes that the three lines of defense model may be a prudent and wise approach for many firms, and we support the goal of ensuring multiple lines of defense. But an overly prescriptive requirement in favor of three lines of defense may force covered entities to undergo a corporate reorganization and encroach upon management's duties. Rather, TIAA recommends a flexible, risk-based system of layered security, including flexible reporting structures that are able to adjust as needs arise. Furthermore, any concerns regarding reporting structures can be addressed through the Agencies' extant examination authority.

Internal & External Dependency Management.

The Agencies are considering several requirements pertaining to enterprise-wide internal dependency management, among them inventorying and prioritizing all business assets (defined as "workforce data, technology, and facilities") throughout their lifespans, including threats posed by insiders, and mapping these dependencies.

The Agencies are also considering several requirements pertaining to external dependency management (*e.g.*, "outside vendors, suppliers, customers, utilities, and other external organizations and service providers"), including real-time monitoring throughout the lifespan of the relationship and considerations of alternative solutions in case an external partner is ever unable to perform. The ANPR imagines a situation in which financial institutions obtain "complete awareness" in "real time" of all external dependencies enterprise-wide and the extent or priority of their criticality.

These requirements are too stringent. TIAA agrees that financial-services firms must maintain a robust and regularly tested cybersecurity program managed by experienced professional staff with technical expertise, and that such a program must include risk assessments of business processes, including vendor relationships, as well as layered controls to address such risks. However, the scope of the ANPR's external dependency management requirements is far too broad, and requires an impractical level of awareness on the part of covered entities.

And while practically infeasible, these proposed requirements are also needlessly prescriptive. TIAA respectfully submits that the most effective regulatory paradigm should emphasize regulatory examinations to assess whether a regulated firm's controls are adequate within the complete environment of multiple layered reinforcing controls, rather than mandate specific controls. For instance, penetration testing and other assessment exercises (*e.g.*, Red Team, table top) are invaluable

tools for testing programs' resilience and effectiveness, and the adequacy of this testing can be assessed through supervisory examination.

Incident Response, Cyber Resilience, and Situational Awareness.

The Agencies are considering a requirement that covered entities establish and maintain effective incident response and cyber resilience governance, strategies, and capacities that enable entities to anticipate, withstand, contain, and rapidly recover from a disruption caused by a significant cyber event. As it is statistically impossible to eliminate risk altogether, a sophisticated information security program like TIAA's manages risks according to the sensitivity of information assets. Determined and sophisticated attackers will eventually develop new methods for infiltrating financial institutions. Thus, it is critical that covered entities retain flexibility in their means for detection, response, and resilience. Continuous risk-assessment and control monitoring through multiple means is effective and regulatory examiners are well-positioned to assess the adequacy of these measures.

RTO for Sector-Critical Systems of Covered Entities.

The Agencies are considering requiring covered entities to establish a recovery time objective ("RTO") of two hours for their sector-critical systems, validated by testing, to recover from a disruptive, corruptive, or destructive cyber event. TIAA believes that the best approach to managing availability and recovery requirements is for organizations to design their own RTOs based upon customer needs and in accordance with a risk-based approach. This approach preserves needed flexibility for covered entities to provide responsive services to customers. The validity of this approach can be validated through supervisory assessments.

Further, as noted above, life and annuities insurers are not sector-critical. As such, life and annuity insurers should not be subject to any higher tier beyond the base enhanced standards applicable to all SLHCs or other covered entities.

Quantifying Cyber Risk.

The Agencies are seeking to develop a consistent, repeatable methodology to support the ongoing measurement of cyber risk within covered entities. The Agencies acknowledge that they are not aware of any consistent methodologies to measure cyber risk across the financial sector, though they are familiar with the FAIR Institute's Factor Analysis of Information Risk Standard and Carnegie Mellon's Goal-Question-Indicator-Metric process. In TIAA's experience, risk analysis using FAIR has been an invaluable contribution to our management of IT risk. While TIAA intends to continue to utilize FAIR, we recommend against mandating it or codifying any other specific methodology, in line with our belief in a flexible, risk-based system of layered security that is able to adjust as needs arise. And as emphasized above, the adequacy of this testing can be assessed through supervisory examination.

Implementation.

The Agencies are considering three approaches (separately or in combination) to establish enhanced standards for covered entities. We interpret these strategies as: (i) a combination of guidance and other policy statements providing minimum expectations for a cyber-risk management framework, (ii) the imposition of prescriptive cyber-risk management strategies that are commensurate with covered entities' size, structure, and complexity while emphasizing the risk categories described above (governance, risk management, internal dependencies, external dependencies, incident response/resilience/situational awareness), and/or (iii) an even more prescriptive regulation mandating specific controls in each risk category. Among these three potential approaches, TIAA recommends the first, as it appears to better preserve the flexibility that diverse entities will need to meet their diverse risk profiles. Common tools and frameworks (*e.g.*, FFIEC Cyber Assessment Tool) are helpful, as are information sharing forums, so long as they do not become prescriptive standards. Any standard that prescribes specific controls will become obsolete over time, and in the particularly dynamic world of cybersecurity this obsolescence may develop quickly. As outlined above, TIAA respectfully submits that the most effective regulatory paradigm should emphasize supervisory examinations to assess whether a regulated firm's controls are adequate within the complete environment of multiple layered reinforcing controls, rather than mandate specific controls.

Conclusion.

TIAA commends the Agencies for their focus on cybersecurity in the financial-services sector. We believe that the protection of both customer information and the operational integrity of firms' information-technology systems are paramount to a well-functioning economy and are integral to the financial security of our participants. We share the Agencies' belief that regulation plays an important role in bolstering the cybersecurity practices of regulated entities. But in an environment of ceaselessly evolving cybersecurity threats, we respectfully submit that unduly prescriptive mandates are counterproductive and draw needed resources away from more effective means of countering cybersecurity threats. Instead, we advocate for a risk-based system of layered security and regulatory oversight that emphasizes examination over strictly codified mandates that can quickly become outdated.

TIAA appreciates the sensitivity the Agencies have shown to differences among types of regulated entities, and urges the Agencies to reconsider the often bank-centric approach that underlies much of the ANPR. As explained above, insurance companies do not provide payment, clearing, or settlement arrangements, nor do they provide credit the way banks do. Furthermore, unlike banks, insurers are usually not interconnected such that the failure of an insurer would pose systemic risk to the larger financial sector; this is especially true for insurers that engage primarily in the life and annuities business. Accordingly, we respectfully recommend that the Agencies take a principles-based approach that accounts for the lower risk

profile and limited interconnectedness of covered entities that are insurance companies when applying enhanced cybersecurity standards.

We would welcome the opportunity to engage further on any aspects of this comment letter.

Sincerely yours,

Derek B. Dorn