U.S. CHAMBER OF COMMERCE

1615 H Street, NW
Washington, DC 20062-2000
www.uschamber.com

January 18, 2017

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

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

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

Re: Enhanced Cyber Risk Management Standards, Dkt. R 1550, RIN 7100-AE-61 (Federal Reserve System), Dkt. ID OCC-2016-0016, RIN 1557-AE06 (OCC), RIN 3064-AE45 (FDIC).

Dear Sirs and Madams:

The U.S. Chamber of Commerce (the "Chamber") is the world's largest business federation, representing the interests of more than three million companies of every size, sector, and region. Appropriate cybersecurity protections are an important and necessary component of efficient capital markets, and we are grateful for the opportunities we have had to partner with 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") on the cybersecurity challenges facing American financial institutions and related entities.

We appreciate the opportunity to respond to the Agencies' request for public comment regarding their joint advance notice of proposed rulemaking on "Enhanced Cyber Risk Management Standards" (the "ANPR").[1] We are particularly glad that the

[1] *See Enhanced Cyber Risk Management Standards*, 81 Fed. Reg. 74315 (October 26, 2016).

Agencies have chosen to solicit comment before issuing a specific proposal in such a complex area.

To be clear, we agree that large financial institutions should have appropriate cyber risk management programs. That view is widely accepted across the industry. The Agencies, moreover, already oversee such programs through their supervisory authority. Financial institutions have played a leading role in improving our nation's cybersecurity and are keenly aware of the enormous risks that cyber threats pose to them individually and, by extension, the financial sector, and the broader economy. The Agencies should encourage and support those entities' continued cybersecurity leadership and collaboration by pursuing a flexible and risk-based approach. We consequently write to emphasize three points:

- **The Agencies should encourage continued cybersecurity leadership by the financial services industry.**

- **The Agencies should support the collaborative development of risk-based approaches rather than impose prescriptive requirements.**

- **The Agencies should pursue regulatory harmonization and avoid creating additional regulatory duplication or confusion.**

We share the important goal of ensuring effective cybersecurity risk management in the financial sector, including to the extent that cyber threats could cause harm to interconnected entities and the sector more broadly. It is our strong belief that cybersecurity should be managed in a risk-based manner based on the unique threats that an enterprise faces, the data it holds and systems it operates, and its culture and capabilities. Although we recognize that some services or systems may be critical to a sector or the broader economy, any effort to address associated risks requires extensive collaboration with industry and flexibility due to the complexity and diversity of the financial services sector. Thus, while the Agencies have identified cybersecurity measures that may make sense for some financial institutions, we would urge them to avoid imposing prescriptive cybersecurity standards on financial sector entities. Pursuit of such an approach would lead to standards that may become rapidly obsolete, an emphasis on compliance rather than security, and the potential undermining of existing public-private collaboration to mitigate cyber threats. The Agencies instead should work collaboratively with financial institutions as they continue to develop risk-based programs to mitigate cyber threats across the sector.

We share the Agencies' appreciation of the scale of the cyber threats facing the financial sector. We believe that we must work together to address these challenges and that a risk-based approach to cybersecurity continues to be the most effective way

to pursue our shared goals. The Chamber and the financial sector have worked closely with federal and state stakeholders to develop and adopt these risk-based approaches, and we have been encouraged by the broad agreement on such best practices. But we are concerned that we face a possible tipping point in the wrong direction in the financial services industry. The Agencies' ANPR comes in the context of a misguided rulemaking by the New York State Department of Financial Services and a request for comment by the Federal Trade Commission on possible amendments to the Safeguards Rule. We urge the Agencies not to create momentum for an effort to regulate away cyber risk. Such an approach would be a mistake: there is no regulatory silver bullet for cybersecurity. The complex, dynamic nature of cyber risk makes pursuing flexible, tailored approaches critical. Instead of focusing on prescriptive approaches, the Agencies should leverage the innovative and collaborative efforts of the financial sector to help further enhance cybersecurity across the industry.

(1) The Agencies Should Encourage Continued Cybersecurity Leadership by the Financial Services Industry.

The financial services industry long has recognized the importance of protecting the financial system against cyber threats. As a result, the financial sector has led the way on many cybersecurity initiatives, becoming a leader for other industries as it develops innovative tools and approaches to managing cyber risk. The Agencies should encourage the financial industry to continue its cybersecurity leadership.

(a) Financial Institutions Have Helped to Lead the Way on Cybersecurity Risk Management.

Private-sector businesses own and operate the substantial majority of the critical infrastructure in the United States, including in the financial services industry. While the government has an important role to play in supporting private sector cybersecurity, financial institutions and other businesses ultimately are responsible for protecting their networks, systems, and data. This includes not only preventing financial crimes or theft of personal information, but also stopping attacks on critical assets and networks that could disrupt the financial system as a whole.

Financial institutions recognize the scale and severity of the cyber risks they face and the vital importance of mitigating these risks to customers, institutions, and to the financial system more broadly. The financial services industry accordingly has invested heavily in cybersecurity risk management. It has led the way on cyber risk management by:

- Developing sophisticated risk management protocols and procedures, and seeing them widely adopted across the industry;

- Developing robust internal cybersecurity resources, tools, and capabilities;

- Developing strong cybersecurity governance programs, including at the board of directors level;

- Developing a leading information sharing organization, the Financial Services Information Sharing and Analysis Center, that shares cyber threat information, provides education, performs readiness exercises, and has created mechanisms for identifying and managing systemic cybersecurity risks;

- Helping to lead the development of the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v. 1.0 and supporting its use;[2] and

- Developing strong relationships with law enforcement agencies and other relevant government entities.

The financial sector's work on cybersecurity is ongoing: financial institutions and related entities continue to work hard to strengthen their cyber risk management programs. Many of these efforts began organically and have thrived as collaborative, consensus-based efforts. The Agencies will be well served to build on these successes and further empower the initiative, capability, and momentum of the industry going forward.

(b) Public-Private Collaboration Has Strengthened Financial Sector Cybersecurity.

The Agencies and the federal government more broadly have an important role to play in advancing the nation's cybersecurity. It has become a truism that the government and the private sector must work together to enhance our nation's cybersecurity. Federal cybersecurity efforts have been centered on this basic premise. Three initiatives merit special focus:

First, the NIST Framework has been a notable success and a prime example of the benefits of public-private collaboration on cybersecurity challenges. The

[2] *See* NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (Feb. 12, 2014). *See also* Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2013).

Chamber, sector-based coordinating councils and associations, companies, and other entities have collaborated closely with NIST in creating the framework from the first workshop in April 2013 to its ongoing implementation. Financial sector institutions and other critical infrastructure entities are very supportive of the NIST Framework. Indeed, businesses across the U.S. economy have incorporated the NIST Framework and similar risk management tools into their cybersecurity programs. This is because NIST has created a broadly-applicable platform for strengthening cyber defenses, rather than static checklists that could become quickly outdated.

Second, the government and the financial sector agree that the timely sharing of actionable cyber threat data offers an important first line of defense against cyber threats. Following a bipartisan push in the House of Representatives and the Senate in 2015, President Obama signed the Cybersecurity Act of 2015 into law. This landmark legislation gives businesses important legal protections when voluntarily sharing threat data with or receiving such information from industry peers and the government. The Chamber and other financial sector stakeholders now are working with the government to leverage this legal framework and expand and improve real-time information sharing.

Third, President Obama provided additional clarity on how the federal government will participate in the response to cybersecurity incidents in the private sector by issuing a Presidential Policy Directive on cyber incident coordination.[3] As Michael Daniel, special assistant to the president and White House cybersecurity coordinator, said at a U.S. Chamber roundtable on the topic, the directive "brings together the lessons learned from responding to cyber events over the last eight years," and provides additional clarity and guidance to the private sector "about the federal government's roles and responsibilities" in responding to incidents that affect the private sector.[4] As a result, companies now have more clarity about what they can expect from the government, allowing the development of more effective working relationships.

(c) The Agencies Should Support Continued Industry Leadership on Cybersecurity.

The Agencies should work with industry stakeholders to help them in their substantial and ongoing efforts to protect the systems on which the financial sector depends. The Agencies have played an important role in efforts to strengthen financial sector cybersecurity, and they will have a substantial part to play in determining whether industry stakeholders continue to lead cybersecurity advances

[3] Presidential Policy Directive/PPD-41, United States Cyber Incident Coordination (July 26, 2016).
[4] Ann M. Beauchesne, *Government, Business Staying in Step to Put Out Cyber Fires*, U.S. Chamber of Commerce: Above the Fold (Aug. 8, 2016).

going forward. As Commerce Department Secretary Penny Pritzker recently said at the Chamber's Cybersecurity Forum, "we still need more strategic, real-world cooperation between government and industry."[5] To that end, we would ask the Agencies to adopt policies that support public-private collaboration and that encourage financial sector entities to continue pursuing risk-based cybersecurity programs.

(2) The Agencies Should Support the Collaborative Development of Risk-Based Approaches Rather than Impose Prescriptive Requirements.

The Agencies should not drive the financial services industry to a compliance-based approach to cybersecurity built around static checklists. Such requirements – some of which we highlight below – are likely to distract or divert financial institutions away from measures that will more effectively protect the financial system from the most critical cyber risks.

(a) The Agencies Should Empower Financial Institutions to Identify Appropriate, Risk-Based Approaches to Achieve Cybersecurity Goals.

Cybersecurity is not a one-size-fits-all proposition. Companies must develop cybersecurity programs that are tailored to the risks that they face and their unique operational requirements. Likewise, attempts to create prescriptive cybersecurity rules risk becoming out-of-date, diverting resources from enhancing security to ensuring compliance, and inhibiting innovation. Moreover, regulation could undermine the collaboration we need for effective cybersecurity. As Secretary Pritzker put it, "[t]he problem is that relationships between regulators and the businesses they regulate are inherently adversarial – not collaborative."[6]

Thus, if the Agencies ultimately conclude that further steps are necessary, they should focus on identifying security objectives and providing covered entities with the flexibility to meet them in the context of their particular cyber risk profile. This approach would ensure that private sector entities are able to maintain cybersecurity programs that are appropriately tailored to the specific risks that they face and can be quickly adjusted over time to respond to evolving threats, new systems, or changing policies. This approach also would empower private-sector innovation while allowing the Agencies to provide further clarity about the expectations that they will bring to supervisory examinations.

---

[5] U.S. Secretary of Commerce Penny Pritzker, Address to U.S. Chamber of Commerce's Cybersecurity Summit (Sept. 27, 2016).

[6] *Id.*

(b) The Agencies Should Avoid Turning Generally Accepted Principles Into Prescriptive Requirements.

More specifically, the Agencies identify a wide range of common elements of many risk-based cybersecurity programs. However, the proposed standards do not provide the required flexibility that entities require for their unique business organizational needs, operations, or risk profiles. For example, the Agencies should not impose prescriptive requirements in the following areas:

- Cybersecurity Governance: Cyber risks have become critical areas of focus for senior leadership at large financial institutions and related entities. Indeed, these entities have developed a variety of different measures and tools for ensuring that their senior executives and boards of directors oversee cybersecurity programs effectively. However, approaches vary based on the risks that an individual entity faces, the systems it operates and data it holds, the maturity and design of its cybersecurity program, and its culture. Mandating a particular governance structure—including with respect to the expertise a board must itself possess or the board's role—is likely to disrupt current efforts and isolate cyber from an entities' overall risk management approach. Consider, for example, an institution in which each member of the audit committee already has engaged heavily on cybersecurity issues. Appointment of a "cyber expert" to the board could disincentivize the existing audit committee members from continuing to engage on cybersecurity issues by concentrating attention to cybersecurity in a single board member.

- Internal Allocation of Responsibilities: It is widely accepted that an independent risk management function can provide substantial value to internal management of cyber risks. Likewise, the value of auditing a cybersecurity program is broadly recognized. Nonetheless, mandating a particular approach would make each function less effective by not accounting for the particular risk profile, business needs, and organizational structures of different entities. Financial institutions and related entities should be empowered to develop models that work best within their enterprises.

    - The internal audit function should be allowed to focus its attention where it identifies the greatest risks. It should not be required, for example, to stretch or divert its resources to

undertake a deep review of every business unit, regardless of risk, or prognosticate about future ability to "remain in compliance."

- The risk management function likewise should not generally be required to maintain catalogs of cybersecurity programs and "relationships to the evolving cyber threat landscape," but should be permitted to perform its function in a manner that reflects the assessed risks facing the various individual business units. Moreover, it is unclear why cybersecurity should differ from other enterprise risks in a way that would require a different, independent reporting structure.

- Recovery Time Objective: We agree that the ability to return sector-critical systems to operation in a timely manner is an important element of mitigating the effects of a cyber attack. However, imposing a specific, broadly applicable recovery time objective after a cyber incident would be unworkable in many scenarios and could exacerbate the impact of an incident. Without the time to appropriately diagnose or mitigate critical systems, rushing to return to operations could lead to catastrophic consequences for the institution and the financial system more broadly. Financial institutions need no further incentive to return to operations in an expeditious fashion. The Agencies should encourage them to do so in a prudent and careful manner based on an appropriate understanding of the underlying incident and any necessary remediation. They should not require financial entities to meet fixed deadlines that could lead to further compromise of the systems and data of the entity or the system more broadly.

- Quantitative Risk Management: The ANPR reflects the Agencies' desire to develop quantitative tools for assessing and managing cyber risk. We share this goal, but we submit that such tools are not sufficiently mature for broad, much less mandatory, use. Certain quantitative metrics can inform cybersecurity oversight, and there is likely additional value to be achieved through the further development of metrics. However, such metrics currently provide a general heuristic about the state of an enterprise's cybersecurity at best. There is unlikely to ever be a single set of quantitative metrics that allows ready assessment of an enterprise's cybersecurity or straight-forward comparison with other entities. Relying on cybersecurity scores or metrics risks relying on inaccurate assessments of cyber risks—and thus inappropriate allocation of resources and focus. Cybersecurity risk management best practices

involve core qualitative elements, especially as different entities give due consideration to the unique aspect of their operations, systems, and threat profile. The Agencies consequently should not task financial entities with creating an unproven scoring or other rating system in recognition that such systems are only one part of assessing cybersecurity.

- Implementing the "Most Effective Commercially Available Controls": The ANPR indicates that the Agencies are contemplating requiring that sector-critical systems be protected by the "most effective commercially available controls." Although the private sector broadly seeks to leverage state-of-the-art commercial tools, the implementation of such a requirement would not be feasible and may have unintended consequences. The effectiveness of cybersecurity controls cannot be readily measured and is highly dependent upon other factors, such as the nature of an entity's environment and the control's function within a broader cybersecurity framework. As a result, it would be unclear how to comply with such a requirement. Affected institutions are likely to ask, for example, whether they should always choose the most expensive option on the market or whether the Agencies intend to produce lists of the best controls. Additionally, it is not clear how this proposed standard would apply to the many entities that use proprietary security controls. The implementation of this requirement as proposed would disrupt sound risk-based practices, depart from longstanding principles of technological neutrality, and discourage innovation in favor of technical compliance.

- Mitigating Systemic Risks: Given the interconnectedness of existing networks, risks to individual financial institutions are risks to the financial system. Likewise, risks to the financial system are risks to individual financial institutions. Despite this fact, individual financial institutions are not well-placed to identify and to mitigate overarching risks to the financial system writ large. Such a requirement also risks being interpreted differently by each financial institution, which would further complicate efforts to address the shared risks of the sector. The Agencies thus should work collaboratively with industry to: (a) identify systemic cyber risks; and (b) develop approaches by which an industry participant can integrate an understanding of those risks into that particular entity's operations.

In addition, we note that the ANPR is too prescriptive with respect to insurers and fails to recognize many of the unique features of the insurance business model, especially the lack of interconnectedness of insurers to the broader financial system. As we have stated with respect to other standards that apply to insurers designated as systemically important financial institutions, we believe that any proposal should be properly calibrated to the business of insurance and should not employ a "one size fits all" approach that would also apply to other financial institutions.

- Asset and External Dependency Mapping: The ANPR emphasizes the importance of situational awareness. While we agree that an institution should base its cybersecurity program on an informed understanding of its data, systems, and external dependencies, there is likely to be a point where such an exercise yields substantially diminished returns. Assets, external dependencies, and business units should be managed an enterprise-wide, risk-based basis. A financial institution should not be required to take a one-size-fits-all approach and dedicate resources to exhaustively cataloging data, systems or dependencies that pose little or no risk to the institution or the sector more broadly.[7]

(3) The Agencies Should Pursue Regulatory Harmonization and Avoid Creating Additional Regulatory Duplication or Confusion.

The Agencies should focus, both in this process and more broadly, on eliminating regulatory duplication and harmonizing cybersecurity standards under a risk-based approach, including the NIST Cybersecurity Framework. Moreover, we would urge the Agencies to ensure that any final product is clear and readily understandable by covered entities.

(a) The Agencies Should Harmonize Standards Using a Risk-based Approach, Leveraging the NIST Cybersecurity Framework.

The ANPR indicates that the Agencies are contemplating establishing standards that could duplicate elements of other standards, best practices, and requirements. The further proliferation of cybersecurity regimes across the financial sector could be counterproductive by creating additional complexity and compliance requirements without a corresponding improvement of outcomes. Financial institutions should be able to build effective cyber risk management programs without

[7] We of course are aware that hostile actors can use a wide range of attack vectors, including those provided by vulnerable third-party systems. But this possibility only speaks to the need to assess and respond to the actual risks that a company faces, not to any need to dedicate resources to exhaustive cataloging without regard to actual risks.

having to navigate multiple overlapping and conflicting requirements. Otherwise, cybersecurity will become a challenge to meet compliance requirements rather than an exercise in making financial services companies more secure.

For example, the proposed new standards would be added to requirements stated in FFIEC guidance, the standards implicit in the FFIEC assessment tool, reporting requirements articulated by the SEC, the Safeguards Rule, and payment card security measures imposed through the PCI DSS requirements. We believe that the Agencies should work with fellow agencies to harmonize relevant standards around risk-based approaches like the NIST Framework. At a minimum, they should ensure that any new standards do not create overlaps or duplications that will render compliance unduly difficult or burdensome with limited cybersecurity benefit.

(b) The Agencies Should Ensure That Any Future Standards, Expectations, or Requirements Are Clear.

We are concerned about the potential diversion of resources from enhancing security to focusing on compliance if the Agencies create new standards, expectations, or requirements in this process that are not risk-based and flexible in their application to a diverse, dynamic sector. A critical aspect of this process is to ensure that any output uses precise terminology and furthers the cyber risk management efforts of covered entities and the broader sector. But the ANPR uses numerous terms that are susceptible to multiple possible meanings or used interchangeably. For example, the ANPR appears to use the terms "critical business functions" and "core business functions" interchangeably, and it does not clearly define "sector partners" and "widespread." The Agencies should ensure that any further steps in this process consistently use appropriately defined terms to avoid confusion about scope and substance.

Further discussion and collaboration will help better define and scope these issues. Indeed, this fact demonstrates the merit of the Agencies' decision to issue an ANPR rather than to jump immediately to issuing a specific proposal. Nonetheless, it merits emphasis that the Agencies should ensure that any future steps in this process are supported by consistent use of appropriately defined terms.

* * * * *

American financial institutions and related entities are well aware of the substantial risks that cyber threats pose to the financial system. To mitigate these risks, they have invested heavily in developing cyber risk management programs, supported by substantial technological and personnel investments. Additionally, they have worked closely with the Agencies and other government partners to develop

collaborative cybersecurity capabilities and relationships to pursue the shared goal of strengthening the security of our financial system.

The cybersecurity of the financial services sector will depend upon the risk-based, outcome-focused efforts of financial entities in collaboration with government partners. Additional standards straying from these principles are likely to inhibit entities' use of best practices and cooperative sector initiatives, dampening cybersecurity innovation and leadership by financial institutions. The Agencies thus should not attempt to impose prescriptive requirements, but support industry efforts to enhance financial sector cybersecurity.

The Chamber is urging policymakers to help agencies harmonize existing regulations with the NIST Cybersecurity Framework.[8] The White House Commission on Enhancing National Cybersecurity report, which was released in December, emphasizes that regulatory agencies should harmonize existing and future regulations with the cyber framework to "reduce industry's cost of complying with prescriptive or conflicting regulations that may not aid cybersecurity and may unintentionally discourage rather than incentivize innovation."[9]

In addition to urging regulatory harmonization, the Chamber believes that it is crucial that the next administration opposes the creation of additional regulatory burdens with respect to cybersecurity. We urge the Agencies to pause and review the ANPR and myriad related regulations in conjunction with industry before moving to the next stage of the rulemaking process.

We thank you for your consideration of these comments and would be happy to discuss these issues further with appropriate staff.

Sincerely,

Tom Quaadman
Executive Vice President
Center for Capital Markets Competitiveness

Ann M. Beauchesne
Senior Vice President
National Security and Emergency Preparedness

[8] *See* http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/20160209_US_Chamber_of_Commerce.pdf
[9] *See* www.nist.gov/sites/default/files/documents/2016/09/15/coc_rfi_response.pdf