Business Roundtable℠

300 New Jersey Avenue, NW
Suite 800
Washington, DC 20001

Telephone 202.872.1260
Facsimile 202.466.3509
Website brt.org

February 13, 2017

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).

On behalf of the close to 200 members of Business Roundtable, an association comprised of chief executive officers of leading U.S. companies representing all sectors of the economy, I want to thank you for the opportunity to provide these comments to the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation (the Agencies) advance notice of proposed rulemaking on Enhanced Cyber Risk Management Standards (Notice).

We commend the Agencies for their prioritization of cybersecurity, and we share their concern about escalating cybersecurity threats. We also appreciate the Agencies releasing this document as an Advanced Notice of Proposed Regulation (ANPR), recognizing the complexity of the issue and the need for a robust dialogue on how to best protect the most critical functions of the financial sector. With this in mind, our following comments on the proposed regulations encourage a more flexible and risk-based approach to cybersecurity that complements existing cybersecurity requirements and results in better cybersecurity outcomes for everyone.

Business Roundtable members have prioritized cybersecurity and supported federal efforts to create voluntary, flexible and agile cybersecurity approaches.

In 2013, President Obama directed the creation of "a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[1] The resulting National Institute of Standards and Technology (NIST) Cybersecurity Framework has been heralded by both industry and government, and Business Roundtable members believe that a voluntary and flexible risk-based approach premised on the NIST Cybersecurity Framework is the approach most capable of managing cybersecurity threats as they evolve.

As the Agencies work to refine the concepts in the Notice into the draft language of a Proposed Guideline or Rule, we appreciate the opportunity to provide the following recommendations:

- First, the Proposed Guideline or Rule should be premised on a risk-based approach. Companies operate in dynamic digital environments and their cybersecurity programs must be designed to accommodate this reality. As the Agencies consider the best approach for implementing the Notice, we recommend moving away from a prescriptive, one-size-fits-all approach because it does not provide companies with the flexibility needed to respond to technological changes and evolving cybersecurity threats. As such, we recommend drafting the standards in a manner that defines security objectives. Furthermore, requiring boards of directors to have adequate cybersecurity expertise would force companies to adopt a compliance-based approach to cybersecurity that is driven by a narrow skill-set. Such an approach is ill-suited for the dynamic environment in which companies operate.

- Second, the Proposed Guideline or Rule should complement existing cybersecurity requirements and guidance. Business Roundtable members are increasingly concerned about the uncoordinated and misaligned cybersecurity requirements among and within federal, state and foreign governments. The proliferation of new and uncoordinated cybersecurity requirements at multiple levels of government forces companies to prioritize compliance with individual requirements over the development of more holistic programs that are matched to their individual risk profiles. We believe that greater collaboration between government and critical infrastructure owners and operators, such as the financial sector, can lead to better aligned cybersecurity requirements and guidance.

- Third, the Proposed Guideline or Rule should avoid prescribing new stringent operational resiliency requirements for sector-critical systems, but rather clarify expected outcomes. As currently drafted, the regulation would require companies to establish a two-hour Recovery Time Objective (RTO) capability for sector-critical systems following a cyber-attack – without considering the nature of the attack or the complexity of the affected

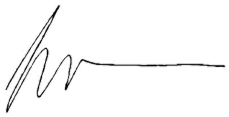
[1] Exec. Order No. 13363, 78 FR 11737 (February 13, 2013), https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.

system. Returning to operations prior to fully understanding and mitigating the attack in order to comply with a defined RTO requirement has the potential to spread the damage throughout the financial system. We would recommend identifying expected RTO capabilities and procedures, instead of mandatory time frames.

We believe that a flexible and risk-based framework will result in the most effective outcome for strengthening cybersecurity for all sectors of the economy. A framework should be intentionally designed to enable companies to customize their cybersecurity programs to their individual risk profiles. We understand that the Agencies want to ensure that the most critical operations in the financial sector maintain the appropriate level of security and resilience in the face of rising cyber threats and encourage the Agencies to bring the Proposed Guideline or Rule in line with a risk-based approach developed through active collaboration with industry, thereby creating a model for other government agencies to follow.

We appreciate the Agencies' consideration of our concerns. Business Roundtable looks forward to collaborating with the Agencies to build upon and improve the proposed standards to manage the risks posed to the most critical operations.

Sincerely,



Julie Sweet
Chief Executive Officer - North America
Accenture
Chair, Technology, Internet and Innovation Committee
Business Roundtable