North American
CRO Council

January 17th, 2017

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

Re: Advanced Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards

Dear Mr. deV. Frierson,

The CRO Council is a professional association of Chief Risk Officers ("CROs") from leading insurers based in the United States, Canada, and Bermuda. Member CROs currently represent 30 of the largest Life, and Property and Casualty insurers in North America. As a body formed to promote sound practices in risk management, the CRO Council appreciates the opportunity to submit its comments and concerns regarding the ANPR for Enhanced Cyber Risk Management Standards.

Ensuring that the financial services sector is resilient to cyber-attacks is a monumental task given the ever increasing number and sophistication of potential attackers, difficulty in hiring/retaining top talent, and continued digitization of financial services companies. To have a chance at being successful, leaders need to ensure that they focus their resources on the top risks. It is in this context that the CRO Council provides its comments to the ANPR for Enhanced Cyber Risk Management Standards. Our comments below represent objectives that should be considered if there is a decision to move forward with enhanced standards.

Avoid legislating obsolescence
Prescriptive detailed rule-making creates the risk of inflexibility in the face of rapidly evolving threats and a divergence of regulation from what is actually required to manage the risks. This prescriptive approach potentially puts the regulator in the position of having to be the cyber security expert and/or having the industry have two streams of activity, one to satisfy the regulations and another to address the real and evolving risks – which will be more expensive and less effective.

Ensure the risk is clearly defined
As noted in the Scope of Application section of the ANPR, the objectives of the proposed rules are to address operational resilience for entities in which a cyber-attack or disruption at one or more of these entities could have a significant impact on the safety and soundness of the entity, other financial entities, or the U.S. financial sector. The scope of the proposed guidelines is very broad and may not result in entities collectively focusing on the highest risk areas. Additional clarity is needed to identify threats and risk scenarios for the business activities that have the most significant impact on safety and soundness. For example, in the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, the scope was focused on the systemic risk from a wide-scale disruption and the associated rapid recovery and resumption of clearing and settlement activities that support critical financial markets.

North American
CRO Council

Ensure the proposed solutions address the risk

The proposed solutions within the ANPR involve a more detailed role for the Board, more independence in the oversight of Cybersecurity Risk, a more rigorous standard for risk assessment and controls (including quantifying cyber risks), and the identification and monitoring of all internal and external connections. Given the level of detail the ANPR is set at and the detailed responses to 39 questions requested, the CRO Council is concerned that the conversation is taking place at too granular a level of detail, too early in the process and ahead of a discussion around more specific threats, risk scenarios, and associated defenses. There may be more effective ways of mitigating these cyber risks than by having all "covered entities" adhere to these enhanced standards. The enhanced standards, if approved in a similar form to the proposal, will require a significant commitment of resources and board and management focus – it is critical that this effort is precisely directed at the areas of highest risk versus distracting attention away from them.

Ensure the proposed solutions are feasible

In order to make some aspects of the ANPR feasible, further regulatory and industry leadership will be required. As an example, without a coordinated industry approach, critical 3rd parties will receive separate requests for information from each and every covered entity that they transact with. Another example is that, on page 40, the ANPR mentions that the agencies are considering a requirement that covered entities minimize the residual cyber risk of sector-critical systems by implementing the most effective commercially available controls. Defining the "most effective commercially available solutions" requires some degree of industry leadership. A final example, is the requirement of monitoring, in real time all external dependencies and trusted connections. Most organizations would not allow another organization to monitor their systems in real time. The key element for managing external dependencies is collaboration on threats as is done through the FS-ISAC and other organizations.

The process around any ANPR may be more efficient and effective if the Industry leadership mechanism is addressed up front, then plays an active role in the risk assessment, and appropriate rule making that might follow.

Sincerely,

Mark Verheyen, Chair
North American CRO Council

Tammy Roou, Lead
North American CRO Council, Cyber Risk Working Group