SCHWARTZ & BALLEN LLP
1990 M STREET, N.W. • SUITE 500
WASHINGTON, DC 20036-3465

WWW.SCHWARTZANDBALLEN.COM

TELEPHONE
(202) 776-0700

FACSIMILE
(202) 776-0700

M E M O R A N D U M

October 25, 2016

To Our Clients and Friends

Re: Agencies Consider Enhanced Cybersecurity Risk Management Standards

The Federal Reserve System Board, the Comptroller of the Currency and the Federal Deposit Insurance Corporation (the "Agencies") have issued an advance notice of proposed rulemaking requesting comment on enhanced cyber risk management standards that would apply to depository institutions, depository institution holding companies and the U.S. operations of foreign banking organizations, with total U.S. assets of $50 billion or more, as well as financial market infrastructure companies and nonbank financial companies supervised by the Board. The Agencies are also considering applying the standards to third-party service providers. Comments are due by January 17, 2017.

The proposed standards emphasize the need for covered entities to continuously monitor and manage their cyber risk within the risk appetite and tolerance levels approved by their board of directors; establish and implement strategies for cyber resilience and business continuity in the event of a disruption; establish protocols for secure, immutable, transferable storage of critical records; and maintain continuing situational awareness of their operational status on an enterprise-wide basis. The standards would be integrated into the Agencies' existing IT supervisory framework.

The Agencies are considering establishing a two-tiered approach, with enhanced standards applying to all covered entities and a more stringent set of expectations on entities that are critical to the financial sector. The enhanced standards would apply in five areas and require covered entities to perform the following tasks:

- **Cyber risk governance.** Develop a written, board-approved, enterprise-wide cyber risk management strategy that is incorporated into the overall business strategy and risk management of the company.
- **Cyber risk management.** Integrate cyber risk management into the responsibilities of at least three independent functions with appropriate checks and balances. Business units would need to ensure that information regarding the cyber risks is shared with senior management in a timely manner.
- **Internal dependency management.** Continually assess and improve, as necessary, the company's effectiveness in reducing cyber risks associated with internal dependencies on an enterprise-wide basis.
- **External dependency management.** Integrate an external dependency management strategy into the entity's overall strategic risk management plan to address and reduce cyber risks associated with external dependencies and interconnection risks.

- **Incident response, cyber resilience, and situational awareness**. Ensure that the entity plans for, responds to, contains, and rapidly recovers from disruptions caused by cyber incidents. Covered entities would be required to be capable of operating critical business functions in the event of cyber-attacks and continuously enhance their cyber resilience. Covered entities would also be required to establish processes designed to maintain effective situational awareness capabilities to reliably predict, analyze, and respond to changes in the operating environment.

A copy of the Agencies' notice is available on our website at http://www.schwartzandballen.com/news.html

If you have any questions, please call Gilbert Schwartz, Robert Ballen, Tom Fox, Heidi Wicker or Magda Gathani at (202) 776-0700.