BRACEWELL

INSIGHTS

Federal Regulators Unveil Proposed Cybersecurity Standards for Large Financial Firms

November 18, 2016

On October 19, 2016, federal regulators issued an Advance Notice of Proposed Rulemaking titled "Enhanced Cyber Risk Management Standards."[1] The draft standards, jointly released by the Federal Reserve, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency, seek to enhance existing cybersecurity standards for large financial institutions and, in particular, supplement existing obligations for financial firms that are the most critical to the U.S. financial system. The plan is open for public comment until January 17, 2017.

Financial institutions with $50 billion or more in assets would be considered "covered entities" and subject to the proposed standards. The proposed standards include a two-tiered framework in which all covered entities would have to meet a minimum standard, and "those entities that are critical to the functioning of the financial sector," referred to as "sector-critical systems," would have to meet "more stringent standards."

Minimum Standards Applicable to All Covered Entities

The proposed standards fall within five different categories: (1) cyber risk governance; (2) cyber risk management; (3) internal dependency management; (4) external dependency management; and (5) incident response, cyber resilience, and situational awareness. The Proposed Standards require covered entities to develop written, board-approved cybersecurity plans that delineate procedures on independent auditing and how issues are reported to the company's chief risk officer. Under the proposed standards, covered entities also must identify and address internal and external cyber risks and adopt plans to ensure continued operation of core business functions during a cyber incident.

Sector-Critical Standards

Entities that have certain systems that would profoundly affect the security and operation of the U.S. financial system are considered "sector-critical." The proposed standards list several types of "sector-critical" systems:

- "systems that support the clearing or settlement of at least five percent of the value of transactions (on a consistent basis) in one or more of the markets for federal funds, foreign exchange, commercial paper, U.S. Government and agency securities, and corporate debt and equity securities";

- "systems that support the clearing or settlement of at least five percent of the value of transactions (on a consistent basis) in other markets (for example, exchange-traded and

over the-counter derivatives)";

- systems "that support the maintenance of a significant share (for example, five percent) of the total U.S. deposits or balances due from other depository institutions in the United States";

- "systems that provide key functionality to the financial sector for which alternatives are limited or nonexistent, or would take excessive time to implement (for example, due to incompatibility)"; and

- "systems that act as key nodes to the financial sector due to their extensive interconnectedness to other financial entities."

Sector-critical systems would be required to adopt the "most effective, commercially available controls." In addition, sector-critical entities must have the capacity to "recover from a disruptive, corruptive, or destructive cyber event" within two hours, and periodically verify their capacity through quantitative testing.

Should you require additional information please contact Glen Kopp at (212) 508-6123.

---

[1] The notice of proposed rulemaking is available ***here.***