Banking Regulators Release Advanced Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards

OCTOBER 20, 2016

Yesterday, the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (Fed), and the Federal Deposit Insurance Corporation (FDIC) issued a joint advanced notice of proposed rulemaking (ANPRM) seeking comment on possible enhanced cybersecurity risk management standards for (i) institutions under their supervision with total consolidated assets of $50 billion or more; (ii) "sector-critical firms," i.e., firms whose systems support the clearing or settlement of at least five percent of the value of transactions 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; and "other large, interconnected financial systems where a cyber-attack or disruption also could have a significant impact on the U.S. financial sector"; and (iii) service providers to companies in the first two categories. The ANPRM is available here.[1] The agencies are considering establishing two tiers of enhanced standards—basic enhanced standards for all covered firms and even more stringent enhanced standards for systems that are "sector-critical."

Although the agencies are proceeding through an ANPRM, they remain undecided about the regulatory approach they will use to put the enhanced standards in place. The possible approaches "range from establishing the standards through a policy statement or guidance to imposing the standards through a detailed regulation." The ANPRM seeks responses to 39 questions. Comments are due by January 17, 2017.

Categories of Enhanced Cyber Risk Management Standards

The agencies are considering establishing enhanced standards in five areas.

Cyber risk governance. The agencies are considering requiring covered firms to develop a written, board-approved, enterprise-wide cyber risk management strategy that is incorporated into the overall business strategy and risk management of the firm. Elements of the proposal under consideration would include requirements for:

- articulating how the entity intends to address its inherent cyber risk (that is, its cyber risk before mitigating controls or other factors are taken into consideration), how the entity would maintain an acceptable level of residual cyber risk through mitigation, and how the

entity would maintain resilience going forward;

- Board approval of the strategy and of policies and procedures to carry it out;
- Board approval of the enterprise-wide cyber risk appetite and tolerances of the covered entity;
- reducing the firm's cyber risk to the appropriate level approved by the Board;
- having senior leaders with responsibility for cybersecurity who are independent of business line management and who have direct reporting access to the Board; and
- Board development of sufficient cyber expertise or independent access to such expertise to challenge management effectively on oversight of cyber risk.

Cyber risk management. The ANPRM considers risk management standards that would require at least three independent functions of covered entities to include cyber risk management as part of their responsibilities, serving as "three lines of defense." Covered firms' independent risk management function would be required to report to the chief risk officer or the Board, as appropriate, on implementation of the firm's cyber risk management framework. Covered firms' audit function would be required to assess whether the firm's cyber risk management framework complies with applicable laws and regulations and is appropriate for the firm's size, complexity, interconnectedness, and risk profile. The audit function would also be required to incorporate an assessment of cyber risk management into the overall audit plan of the covered entity.

Internal dependency management. The internal dependency management considerations in the ANPRM address the cyber risks related to a company's internal assets, such as employees, data, technology, and facilities. The ANPRM notes that this type of management would be designed to address risks arising from a wide range of sources, including data transmission errors and the use of legacy systems integrated with the company through a merger. Elements of the proposal would include requirements for:

- ensuring that covered entities continually assess and improve, as necessary, their effectiveness in reducing the cyber risks associated with internal dependencies on an enterprise-wide basis;
- maintaining an inventory of all business assets on an enterprise-wide basis prioritized according to the assets' criticality to the business functions they support, the firm's mission and the financial sector;
- establishing and applying appropriate controls to address the inherent cyber risk of their assets; and
- periodically testing back-ups to business assets to achieve resilience.

External dependency management. The external dependency management considerations in the ANPRM address cyber risks arising from "an entity's relationships with outside vendors, suppliers, customers, utilities, and other external organizations and service providers that the entity depends on to deliver services, as well as the information flows and interconnections between the entity and those external parties." Elements of the proposal would include requirements for:

- integrating 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;

- maintaining a current, accurate, and complete awareness of, and prioritizing, all enterprise-wide external dependencies and trusted connections based on their criticality to the business functions they support, the firm's mission, and the financial sector; and
- establishing and applying appropriate controls to address the cyber risk presented by each external partner throughout the lifespan of the relationship.

Incident response, cyber resilience, and situational awareness. Elements of the response, resilience, and awareness standards under consideration would include requirements for:

- establishing and implementing plans to identify and mitigate the cyber risks they pose through interconnectedness to sector partners and external stakeholders to prevent cyber contagion, including effective escalation protocols linked to organizational decision levels, cyber contagion containment procedures, communication strategies and processes to incorporate lessons learned back into the program;
- establishing and implementing strategies to meet the entity's obligations for performing core business functions in the event of a disruption, including the potential for multiple concurrent or widespread interruptions and cyber-attacks on multiple elements of interconnected critical infrastructure, such as energy and telecommunications;
- establishing protocols for secure, immutable, off-line storage of critical records, including financial records of the institution, loan data, asset management account information, and daily deposit account records, including balances and ownership details, formatted using certain defined data standards to allow for restoration of these records by another financial institution;
- establishing plans and mechanisms to transfer business, where feasible, to another entity or service provider with minimal disruption and within prescribed time frames if the original covered entity or service provider is unable to perform; and
- maintaining an ongoing situational awareness of their operational status and cybersecurity posture to pre-empt cyber events and respond rapidly to them, including through the maintenance of threat profiles and threat modeling.

Standards for Sector-Critical Systems

The higher tier standards applicable to sector-critical systems would require covered entities:

- to implement “the most effective, commercially available controls” to minimize residual cyber risk;
- to establish a recovery time objective (RTO) of two hours for sector-critical systems to return to normal after a cyber-attack, validated by testing; and
- to measure quantitatively the ability of the firm, at the holding company level, to reduce cyber risk to minimal levels.

Approach to Quantifying Cyber Risk

Finally, the agencies are seeking to develop a consistent, repeatable methodology for measuring cyber risk in covered firms. The ANPRM notes the existence of the FAIR Institute's Factor Analysis of

Information Risk standard and Carnegie Mellon's Goal-Question-Indicator-Metric process, but states that the agencies “are not aware of any consistent methodologies to measure cyber risk across the financial sector using specific cyber risk objectives.” The agencies appear to be particularly eager for private-sector input on this score.

---

[1] Office of the Comptroller of the Currency, Federal Reserve System, and the Federal Deposit Insurance Corporation, *Enhanced Cyber Risk Management Standards, Joint Advance Notice of Proposed Rulemaking* (October 19, 2016), *available at* https://www.fdic.gov/news/board/2016/2016-10-19_notice_dis_a_fr.pdf. The definition of sector-critical firms and systems draws on the 2003 *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* (published by the Fed, OCC, and Securities and Exchange Commission), *available at* http://www.sec.gov/news/studies/34-47638.htm.

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Franca Harris Gutierrez

PARTNER

Chair, Financial Institutions Practice

Co-Chair, Securities and Financial Regulation Practice

franca.gutierrez@wilmerhale.com

+1 202 663 6557