JONES DAY

NOVEMBER 2016

COMMENTARY

Federal Banking Agencies Propose Enhanced Cyber Risk Management Standards

The Board of Governors of the Federal Reserve System ("Federal Reserve Board"), the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency (collectively, "the agencies") recently issued a joint advance notice of proposed rulemaking ("ANPR") inviting public comment on enhanced cyber risk management standards ("Enhanced Cyber Standards") for large and interconnected financial institutions under their supervision and their third-party service providers.[1]

The ANPR proposes adopting a two-tiered approach for applying a robust set of cyber risk management standards to all covered financial institutions and their service providers and a more stringent set of standards to systems that are critical to the functioning of the financial sector and the U.S. economy. The ANPR asks 39 discrete questions that cover all aspects of the Enhanced Cyber Standards, including appropriate regulatory approaches for applying the Enhanced Cyber Standards. The agencies intend to develop and publish for public comment a notice of proposed rulemaking based upon the comments received in response to the ANPR.

The Enhanced Cyber Standards reflect the agencies' increasing focus on cyber risks as a regulatory priority and may signal the agencies' intent to move away from general guidelines toward binding rules with a greater level of specificity. Cyber risks are ubiquitous, and the agencies' ANPR demonstrates the importance of cyber preparedness, governance, and response at a time when no company and no sector-critical system is immune from cyberattacks.

In light of the heightened threat environment and the agencies' intense focus on cybersecurity, covered financial institutions and their service providers should conduct a careful enterprise-wide examination of their existing cybersecurity policies and procedures against the proposed Enhanced Cyber Standards. This examination should include risks posed by the interconnectedness of financial institutions and systems and the potential consequences of a successful cyber-attack that compromises critical systems of the financial institution or its third-party service providers.

Covered entities and their service providers should consider submitting comments directly to the agencies and/or through their representative industry associations to assist the agencies in developing sound Enhanced Cyber Standards that can be integrated effectively into business operations. The deadline for submitting comments is January 17, 2017.

CYBERSECURITY IS A REGULATORY PRIORITY

The agencies have long recognized cyberattacks as one of the greatest threats facing the financial services industry, and the agencies' supervisory programs have addressed the cybersecurity practices of financial institutions for several years. The agencies are proposing the Enhanced Cyber Standards as part of their ongoing efforts to develop a comprehensive response to the constant and enduring reality of cyberattacks.[2]

Cyberattacks on the U.S. financial system create a serious risk of high-impact technology failures with systemic consequences. The agencies' ANPR points out that the interconnectedness of the U.S. financial system creates the risk that a cyber incident or failure at one interconnected entity "may not only impact the safety and soundness of the entity, but also other financial entities with potentially systemic consequences."[3] The agencies intend for the Enhanced Cyber Standards to "increase the operational resilience" of interconnected entities and reduce negative impacts on the financial system.

The Enhanced Cyber Standards ultimately would be integrated into the existing cybersecurity frameworks that financial institutions already employ, such as the Cybersecurity Assessment Tool adopted by the Federal Financial Institutions Examination Council ("FFIEC"), the FFIEC Information Technology Handbook, the Interagency Guidelines Establishing Information Security Standards on safeguarding the confidentiality and security of customer information, and the National Institute of Standards and Technology Cybersecurity Framework.[4] The proposed Enhanced Cyber Standards, however, would move beyond these tools and guidelines toward the adoption of mandatory requirements.

TWO-TIER FRAMEWORK FOR APPLICATION OF ENHANCED CYBER-RISK MANAGEMENT STANDARDS

The Enhanced Cyber Standards would apply to certain regulated institutions with total consolidated assets of $50 billion or more on an enterprise-wide basis.[5] The Enhanced Cyber Standards also would apply to nonbank financial companies supervised by the Federal Reserve Board, to financial market utilities designated by the Financial Stability Oversight Council, and to financial market infrastructures ("FMIs") that perform critical functions for the U.S. financial system and for which the Board is the supervisory agency.

In order to ensure consistent application of the Enhanced Cyber Standards and to facilitate supervisory action, the agencies are proposing to apply the Enhanced Cyber Standards to third-party service providers with respect to the services they provide to covered depository institutions and their affiliates. In this way, third-party service providers would have the same obligation to meet the Enhanced Cyber Standards as the depository institutions or affiliates to which they provide services. Further, the Federal Reserve Board is considering requiring nonbank financial companies and Board-supervised FMIs to verify that any services they receive from a third party are subject to the same standards that would apply if those services were conducted directly by those entities.

The agencies are proposing a two-tiered approach for applying the Enhanced Cyber Standards to substantially mitigate the risk of disruption in the event of a cyber event. The first tier of Enhanced Cyber Standards would apply to all covered entities, and the second tier would apply additional, more stringent standards to so-called "sector-critical systems" that are essential to the functioning of the financial sector.

Standards that Would Apply to All Covered Entities

The Enhanced Cyber Standards emphasize the need for all covered entities to demonstrate effective cyber risk governance; continuously monitor and manage their cyber risk within the risk and tolerance levels approved by their boards of directors or executive management; establish and implement strategies for cyber resilience and business continuity in the event of a disruption; establish protocols for secure, immutable, and transferable storage of critical records; and maintain continuing situational awareness of their operational status and cybersecurity posture on an enterprise-wide basis.

The Enhanced Cyber Standards are organized into five categories to emphasize the core cyber risk governance and cyber risk management standards the agencies would expect a covered entity to develop to establish a foundation for making informed risk-based decisions in support of its business objectives.

C**yber-Risk Governance**. Consistent with other cyber risk guidance for financial institutions, the ANPR emphasizes the importance of developing a formal cyber risk management strategy that involves the highest levels of the organization. Covered entities would be required to develop a written, enterprise-wide cyber risk strategy; develop policies and plans to implement the cyber risk strategy into the overall business strategy for the entity; establish formal cyber risk tolerance levels; and reduce the entity's cyber risk levels to appropriate levels. Each of these actions would require review and approval by the board of directors. The board of directors would oversee and hold senior management responsible for implementing the entity's cyber risk management framework. Given the level of board involvement contemplated, the agencies envision that boards will have adequate cybersecurity expertise, or at least retain their own cyber experts to manage cyber risks. The agencies' focus on board involvement is aligned with the Securities and Exchange Commission's recognition of the importance of board oversight and risk management against cyberattacks and cyber crimes.[6]

Cyber-Risk Management. Covered entities would be required to integrate cyber risk management across at least three independent functions, serving as "three lines of defense."

- **Business Units**. The business unit function would be required to assess major cyber risks and potential vulnerabilities associated with every business asset, such as workforce, data, technology and facilities, on a regular basis and to adhere to policies designed to mitigate and manage those risks. The business unit, therefore, must be tooled with the resources and staff to comply with the unit's cyber risk responsibilities so that it can identify and report any threats to senior management in a timely manner.
- **Independent Risk Management**. The independent risk management function would be required to continuously identify, measure, and monitor risk across the enterprise and directly report to the entity's chief risk officer and board of directors the implementation of cyber risk management throughout the organization. To satisfy these requirements, the ANPR emphasizes that a covered entity's independent risk management function should have sufficient independence, resources, and access to the board and, furthermore, should have separate reporting lines from the business unit, as appropriate, when its assessment of a particular cyber risk differs from that of the business unit.
- **Audits**. The audit function evaluates the effectiveness of the entire cyber risk management strategy, internal controls, and governance. The audit function would further advise the board on whether the existing policies and procedures are sufficient to keep up with emerging risks in the industry.

Internal Dependency Management. "Internal dependency" refers to the business assets upon which the entity depends to deliver services, such as workforce, data, technology, and facilities, and the interconnectedness of those assets. A key purpose of internal dependency management is to ensure that covered entities continually assess and improve their effectiveness in reducing cyber risk associated with internal dependencies. The ANPR would require covered entities to adopt practices to identify and assess the cyber risks of their business assets, establish policies to manage the risks, maintain an inventory of all business assets, and apply appropriate controls to address the cyber risks of the assets.

External Dependency Management. "External dependency" refers to a covered entity's relationship with outside vendors, suppliers, customers, utilities, and other external organizations and service providers upon which the covered entity depends to deliver services. Consistent with the agencies' focus on third-party risk management, under the external dependency management category, covered entities would be required to integrate an external dependency risk management strategy into overall strategic risk management plans, establish policies to monitor and identify cyber risks in real time, and support timely identification and responses to external disruptions.

Incident Response, Cyber-Resilience, and Situational Awareness. Covered entities must plan for, respond to, contain, and rapidly recover from cyberattacks and disruptions, by adopting measures such as incident response programs, substitute systems and secure offline storage of critical records, periodic threat testing, and the maintenance of threat profiles for identified threats.

Standards that Would Apply to Sector-Critical Systems

The ANPR defines "sector-critical systems" as those that meet one of the following criteria:

- Consistently support the clearing or settlement of at least five percent of the value of transactions in one of more of the markets for federal funds, foreign exchange, commercial paper, U.S. government and agency securities, and corporate debt and equity securities;
- Consistently support the clearing or settlement of at least five percent of the value of transactions in other markets such as exchange-traded and over-the-counter derivatives); or
- 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 addition to the Enhanced Cyber Standards that would apply to all covered entities, the ANPR would require covered entities to identify "sector-critical systems" that would be subject to more stringent standards. The ANPR suggests that covered entities with sector-critical systems must utilize the most effective, commercially available controls and establish a Recovery Time Objective of two hours or less for these systems to recover from a cyberattack.

Notably, the more stringent standards for sector-critical systems also would apply to services provided by third parties to support a covered entity's sector-critical systems.

Regulatory Approaches

The agencies are interested in receiving comments about the regulatory approaches they should adopt to implement the Enhanced Cyber Standards. The agencies are requesting comments on a regulatory approach that would require covered entities to maintain a cyber risk management framework consistent with the agencies' guidance on the minimum expectations for the framework.

The agencies also are interested in comments on an approach that would require covered entities to follow specific cyber risk management standards that are commensurate with the entity's structure, risk profile, complexity, activities, and size, as they have adopted for other guidance such as for safety and soundness standards. To demonstrate that the entity's cyber risk management program could adapt to changes in the entity's operations and the cybersecurity environment, the agencies additionally are interested in receiving comments on an approach that would require covered entities to outline specific objectives and practices the covered entity would be required to achieve in each of the five categories described above.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

Lisa M. Ledbetter
Washington
+1.202.879.3933
lledbetter@jonesday.com

C. Hunter Wiggins
Chicago / Washington
+1.312.269.1554 / +1.202.879.7656
hwiggins@jonesday.com

Todd S. McClelland
Atlanta
+1.404.581.8326
tmcclelland@jonesday.com

Jay Johnson
Dallas
+1.214.969.3788
jjohnson@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Jennifer C. Everett
Washington
+1.202.879.5494
jeverett@jonesday.com

Endnotes

1 Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74315 (proposed Oct. 26, 2016).

2 The New York Department of Financial Services recently proposed a regulatory framework that would require New York-licensed financial institutions to establish stringent cybersecurity compliance programs. *See* Proposed Regulation 23 NYCRR 500.

3 Enhanced Cyber Risk Management Standards, *supra* note 2, at 74317.

4 Other widely employed cybersecurity frameworks include the Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions Guidance on cyber resilience for financial market infrastructures, the Interagency Paper on Sounds Practices to Strengthen the Resilience of the U.S. Financial System, and the G7 Fundamental Elements of Cybersecurity for the Financial Sector.

5 Consequently, the proposed standards would not apply to community banks, which would remain subject to the agencies' existing guidance, standards and examination.

6 *See, e.g.*, Comments by SEC Commissioner Luis A. Aguilar on Boards of Directors, "Corporate Governance and Cyber Risks: Sharpening the Focus," June 10, 2014.