WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

Federal Banking Regulators Seek Comment on Enhanced Cyber Risk Management Standards

November 9, 2016

AUTHORS

Daniel Alvarez | Elizabeth Bower | James Burns | Elizabeth Gray | David Katz | Katherine Doty Hanniford

The Board of Governors of the Federal Reserve ("Fed"), the Office of the Comptroller of the Currency ("OCC"), and the Federal Deposit Insurance Corporation ("FDIC," and collectively "the agencies") have issued a joint advance notice of proposed rulemaking ("Notice") related to enhanced cyber risk management, and are seeking comments by January 17, 2017.[1] Citing the interdependence of the U.S. financial system and its reliance on technology, the agencies have set forth a proposed regulatory framework that would transform existing cybersecurity-related guidance into binding standards to which certain entities would be required to adhere. Under this proposal, the agencies would apply the enhanced standards on an enterprise-wide basis to entities with total consolidated assets of $50 billion or more ("covered entities").[2] The Notice contemplates a set of standards that implicate roles and responsibilities from the board and C-suites to specific business units, including internal audit, compliance, and risk management personnel at multiple levels throughout a covered entity.

[1] Enhanced Cyber Risk Management Standards, U.S. Department of The Treasury, Office of the Comptroller of the Currency, 12 C.F.R. Part 30; Docket ID OCC-2016-0016; RIN 1557-AE06; *available* here.

[2] Certain U.S. operations of foreign banking organizations, federal branches of foreign banks, and certain non-bank financial companies supervised by the Fed pursuant to Dodd-Frank would also be considered "covered entities."

Scope and Approach of Application

The Notice evinces a clear intention on the part of the agencies to require robust cybersecurity standards on an enterprise-wide basis that will apply to the lifecycle of assets and functions under the covered entities' control, including covered entities' relationships with third-party service providers. Nevertheless, the agencies' request for comments on thirty-nine separate points throughout the Notice presents a noteworthy opportunity to shape what has the potential to be a sweeping set of regulatory standards, which could reconfigure covered entities' management and reporting structures as well as certain key roles and responsibilities, including of the board of directors, and transform how covered entities interact with third-party service providers. Comments on the Notice are due by January 17, 2017, and the agencies will seek public comment on a detailed proposal before adopting any final rule.

The Notice outlines a two-tiered approach to the application of standards to covered entities. As currently contemplated, all covered entities would be bound by a set of enhanced standards delineated in five categories: (i) cyber risk governance; (ii) cyber risk management; (iii) internal dependency management; (iv) external dependency management; and (v) incident response, cyber resilience, and situational awareness. In addition, the Notice introduces the concept of "sector-critical systems" at covered entities that the agencies deem to be "critical to the functioning of the financial sector."[3] Sector-critical systems would be subject to a second, tougher set of standards in addition to the standards articulated under the five categories.

Enhanced Cyber Risk Management Standards

The stated purpose of the enhanced standards is to "increase the entities' operational resilience and reduce the potential impact on the financial system as a result of, for example, a cyber attack at a firm or the failure to implement appropriate cyber risk management."[4] The standards would require covered entities to demonstrate effective cyber risk governance and management, at risk tolerance levels approved by the entities' respective boards of directors. The cyber risk governance and management standards are intended to serve as the foundation for an entity's risk-based decision-making. Covered entities also would be expected to develop and institute strategies, policies, and procedures for dependency management, incident response, and cyber resilience, including "secure, immutable, and transferable storage of critical records,"[5] and to maintain ongoing situational awareness on an enterprise-wide basis. The standards relating to dependency management, cyber resilience, incident response, and situational awareness are designed to work in tandem and mutually reinforce one another across the enterprise.

---

[3] According to the Notice, the agencies intend to apply the designation at more specific, system levels within a covered entity.

[4] Notice at 21.

[5] Notice at 22.

1. Cyber risk governance

Among the more notable aspects of the proposed standards is their formalization of the board of directors' ultimate responsibility for a covered entity's cyber risk management strategy, which would require directors to have or retain sufficient expertise in cyber risk and resilience issues in order "to provide credible challenge to management" regarding cyber issues.[6] The agencies are considering whether to require boards of directors to review and approve enterprise-wide cyber risk tolerances, and require covered entities to bring their respective risk levels below the level set by the boards of directors. These board-specific requirements are predicated on a covered entity's ability to measure and aggregate cyber risk across the enterprise, and to formally adopt and implement an enterprise-wide cyber risk management framework, including supporting policies and procedures. The Notice characterizes the internal controls and internal audit functions as important to this effort. The Notice also contemplates requiring senior personnel responsible for cyber risk oversight to report directly and independently to the boards of directors.

2. Cyber risk management

The agencies appear to be focused on two key aspects of cyber risk management: (i) reporting to the CEO and board of directors; and (ii) organizational approaches to effectively monitor, measure, manage, and report on cyber risk. The Notice includes consideration of proposals that would require additional, timely, and, in some cases, independent reporting lines to the CEO and board of directors for cyber risk. The Notice also repeatedly underscores the importance of continuous, ongoing cyber risk assessment and monitoring, and the communication of these risks and threat status to the senior-most levels of a covered entity's governance structure.

In terms of organizational approaches to risk management, the Notice references the three lines of defense model as an example for implementing an appropriate cyber risk management framework.[7] Under this model as contemplated by the Notice, enhanced cyber risk management responsibilities would be assigned to three organizational functions: (i) business units; (ii) independent risk management; and (iii) internal audit. Each business function would retain responsibility for certain identification, measurement, monitoring, and mitigation efforts, and corresponding internal reporting or information-sharing obligations.

The agencies also are considering whether to require the creation of an independent risk management function, comprised of individuals sufficiently senior and independent to report directly to the covered entity's chief risk officer and board of directors. In addition to continuously assessing the entity's overall exposure to cyber risk, the independent risk function would be required to promptly notify the CEO and board of directors if its cyber risk assessment differs from that of a business unit or when a business unit has exceeded the board-approved cyber risk tolerance level. The independent

---

6 Notice at 25.

7 *See, e.g.*, "IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control," January 2013, *available* here.

risk management function would also be expected to quantitatively assess a covered entity's ability to reduce its aggregate residual cyber risk, and how efficiently, effectively, and completely it can do so.

3. Internal dependency management

The Notice defines "internal dependency" as the business assets of a covered entity upon which such entity depends to deliver services, as well as the information flows and connections among those assets. The agencies are considering a requirement to integrate an internal dependency management strategy into a covered entity's overall cyber risk management framework. The purpose of such a strategy would be to ensure that the covered entity has a comprehensive and accurate understanding of all internal assets and business functions that bear on its overall cyber risk management framework. The agencies are considering requiring a complete listing of all assets and functions and how they connect or communicate with one another, throughout the assets' lifecycles, in order to promote monitoring, incident response, and systems recovery. Required permanent controls and periodic back up testing are contemplated under this provision.

4. External dependency management

The Notice defines "external dependency" as an entity's relationships with third-party vendors, suppliers, customers, telecommunications or power utility providers, and other external organizations and service providers upon which such entity depends to deliver services, as well as the information flows and connections among those third parties. The agencies are focused on a covered entity's ability to effectively monitor third-party service providers in order to limit the cyber risks associated with external parties. To that end, the agencies are considering a requirement that a covered entity maintain a comprehensive list of third parties and external connections, and that they prioritize that list based on which third parties are critical to the business functions they support, the entity's mission, and the financial sector more broadly. The agencies are also focused on a covered entity's dependence on third parties within the context of a cyber event or disruption, and the covered entity's and third parties' abilities to withstand such a threat and recover quickly from a disruption.

5. Incident response, cyber resilience, and situational awareness

The Notice contemplates that covered entities will be required (i) to be capable of sustaining critical business functions in the face of cyber attacks and (ii) to maintain sufficient situational awareness to be continually improving their cyber-readiness. The Notice contemplates requiring covered entities to develop, maintain, and test cyber resilience and incident response programs, on an enterprise-wide basis. The agencies appear to be especially focused on the threat of cyber contagion, given the interconnected nature of the U.S. financial and banking system. Accordingly, cyber resilience and incident response exercises would be required to consider wide-scale scenarios. These scenarios would stretch beyond institutional considerations to those of third parties, and to the overall resilience of the U.S. financial sector. The preservation of critical records and ability to perform core business functions are among the key considerations included in the Notice. The agencies are also considering requirements relating to vulnerability analyses and security analytics,

such as whether to require covered entities to establish and maintain threat profiles, threat modeling capabilities, and threat intelligence gathering.

Sector-Critical Systems

Consistent with other cyber-related regulations,[8] covered entities with systems deemed to be "sector-critical" would be required to establish a recovery time objective ("RTO") of two hours. The two-hour RTO would be required to be tested under a range of severe scenarios, and such testing would encompass communications, governance, resumption, and recovery aspects of resiliency. The agencies' consideration of the sector-critical systems standard explicitly surpasses the guidance that the Fed, OCC, and Securities and Exchange Commission ("SEC") previously set forth.[9] While that guidance focused on clearing and settlement organizations following the September 11, 2001 attacks, here the agencies are contemplating the broader effects of advances in technology on other large, interconnected financial systems, and the potential impact of a cyber-based disruption on the U.S. financial sector.

Nevertheless, for firms already subject to regulations such as Regulation SCI, the Notice leaves unanswered whether financial institutions that are following other standards will be deemed to be in compliance with the proposed standards, including sector-critical systems, or whether the proposed standards will serve as additional requirements. Presumably, for those institutions whose primary regulator is the Fed, OCC, or FDIC, such institutions will need to comply with the enhanced standards while also complying with regulations issued by other agencies, such as the SEC and the New York Department of Financial Services ("NYDFS").[10] However, the standards discussed in the Notice, the SEC's proposed rules under Regulation BCP,[11] and the NYDFS proposed regulations are not yet final, so there may be an opportunity to work with the regulators to achieve some level of harmonization among these regulations in order to maximize the efficiency of cyber readiness efforts across the U.S. financial sector.

---

8 *See* Willkie Farr Client Memorandum, *SEC Adopts Regulation Systems Compliance and Integrity*, Dec. 2, 2014, *available* here; Regulation Systems Compliance and Integrity, Securities Exchange Act Rel. No. 73639 (Nov. 19, 2014) [79 FR 72251 (December 5, 2014)]. Regulation SCI requires entities to maintain and test back up and recovery plans in order to be capable of resuming critical systems within two hours of a wide-scale disruption.

9 *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* ("Sound Practices Paper") Federal Reserve System Docket No. R-1128 (April 8, 2003), *available* here.

10 *See, e.g.*, Willkie Farr Client Memorandum, *Increased Financial Regulatory Focus for Enhanced Reporting of Cyber-Events and Cyber-Enabled Crime*, Nov. 3, 2016, *available* here.

11 *See, e.g.*, *supra* note 8; Willkie Farr Client Memorandum, *SEC Proposes Rule Requiring Investment Advisers to Adopt Business Continuity and Transition Plans*, July 26, 2016, *available* here.

The agencies also seek comment on tools and practices that can be used consistently and repeatedly in order to assess cyber risk at the entity level. It appears they are especially interested in the development of repeatable methodology as it relates to the mitigation of the residual cyber risk of sector-critical systems at a covered entity.

Conclusion

The agencies' proposed standards stop short of explicitly embracing one approach to cyber risk, and indeed they note the extensive existing guidance developed to date, and also explicitly request comment on what approaches covered entities could take in order to ensure they are effectively monitoring, measuring, managing, and reporting on cyber risk. Yet much of the Notice appears to provide the corporate governance analogue to the approach to cyber security known as layered security or defense in depth. This approach to cyber security contemplates multiple types of security measures, deployed at various levels throughout an entity, such that together they form overlapping sets of defenses around a given asset, reducing the likelihood of success of a cyber threat, and increasing the entity's ability to detect and mitigate a cyber event. The agencies are considering how to require the integration of cyber risk management across multiple independent functions of a covered entity, with appropriate checks and balances, so that the covered entity would be better positioned to identify, monitor, measure, manage, and report on risk. This is consistent with more technical cyber risk management techniques that combine multiple mitigating security controls to protect a covered entity's assets.

By explicitly involving the uppermost echelons of a covered entity's governance structure, the agencies are considering a set of requirements that may impact liability determinations in the event of cyber breaches and may extend responsibility for adverse consequences or the perception of lax governance to senior management and the board of directors at a covered entity.

Finally, the agencies are considering three possible tracks for implementation, which vary by specificity. Under the most principles-based approach, the agencies would propose standards as part of a policy statement or guidance that would be accompanied by the requirement of a covered entity to maintain a cyber risk management framework. Under the middle track, the agencies would propose regulations that impose specific cyber risk management standards along the lines of the five enhanced cyber risk management standards discussed earlier in this memorandum. Under the most prescriptive track, the agencies would propose specific regulations with greater detail than the middle track, and promulgate specific objectives and practices that a covered entity would need to achieve in order to demonstrate the adequacy of its cyber risk management framework. In considering which track to pursue, the agencies will consider relative clarity of standards, implementation effort, cost-benefit analysis, and whether the standards are sufficiently adaptable to meet the dynamic challenges posed by cyber threats.

If you have any questions regarding this memorandum, please contact Daniel Alvarez (202-303-1125; dalvarez@willkie.com), Elizabeth Bower (202-303-1252; ebower@willkie.com), James Burns (202-303-1241; jburns@willkie.com), Elizabeth Gray (202-303-1207; egray@willkie.com), David Katz (202-303-1149; dkatz@willkie.com), Katherine Doty Hanniford (202-303-1157; khanniford@willkie.com) or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

November 9, 2016