October 21, 2016

Federal Banking Agencies Issue Advanced Notice of Proposed Rulemaking on Enhanced Cybersecurity Standards

Enhanced Standards Would Require Certain Large Financial Institutions to Implement Policies and Procedures to Prevent, Contain, and Quickly Recover from Cyberattacks

On October 19, the Federal Reserve Board ("Board"), the Federal Deposit Insurance Corporation ("FDIC"), and the Office of the Comptroller of the Currency ("OCC") jointly issued an advanced notice of proposed rulemaking ("ANPR") seeking comment on a new set of enhanced cybersecurity standards for certain institutions under their supervision.[1] Comments on the ANPR and the various questions posed by the agencies are due by January 17, 2017. The final standards may take the form of a policy statement or guidance or a "detailed regulation."

The agencies are considering applying the enhanced standards to the following "covered entities" and seek comment on whether this scope should be broadened or narrowed:

- U.S. depository institutions and depository institution holding companies (on an enterprise-wide basis, including their subsidiaries) with total consolidated assets of $50 billion or more,
- U.S. operations of foreign banking organizations with total U.S. assets of $50 billion or more,
- Financial market utilities and nonbank financial companies supervised by the Board (*i.e.*, those designated by the Financial Stability Oversight Council),
- Third-party service providers, with respect to services provided to depository institutions and their affiliates that are covered entities.[2]

The agencies recognize that, due to the interconnectedness of the U.S. financial system, a cyber incident at one entity may not only "impact the safety and soundness of the entity, but also other financial entities with potentially systemic consequences."[3] The enhanced standards aim to "increase the operational resilience" of covered entities and reduce the impact of a cyber event on the financial system by establishing enhanced cybersecurity practices in five areas: (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.[4]

The ANPR follows about a month after the New York Department of Financial Services ("DFS") issued its own proposed rules on cybersecurity. It appears that if the federal agencies' and DFS's efforts are

eventually finalized, both sets of rules could apply simultaneously to most New York branches of foreign banks with over $50 billion in U.S. assets, absent an accommodation by one of the regulators.

Application of the Enhanced Standards

The enhanced standards would be integrated into the existing supervisory framework of cybersecurity standards for financial institutions and third-party service providers, which is summarized in the ANPR.[5]

The ANPR reflects a two-tiered structure, with enhanced standards for covered entities and an even higher set of standards for an entity's "sector-critical systems"—that is, systems that are "critical to the financial sector," as explained in more detail below.[6]

Summary of the Enhanced Standards

The enhanced standards would "emphasize the need for covered entities to demonstrate effective cyber risk governance; continuously monitor and manage their cyber risk within the risk appetite and tolerance levels approved by their boards 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 and cybersecurity posture on an enterprise-wide basis."[7]

Key provisions of the enhanced standards include the following:

1. ***Cyber risk governance.*** The enhanced standards would require a covered entity to develop and maintain a formal cyber risk management strategy, which the ANPR proposes would be similar to standards already in place for complex financial institutions, as well as a reporting structure to implement the strategy and a supporting framework of policies and procedures. Among other things, the standards would provide that the board of directors or an appropriate board committee would be responsible for approving an entity's cyber risk management strategy. The standards would include a requirement that covered entities develop written, board-approved, enterprise-wide cyber risk management strategies articulating how entities would address inherent cyber risks and maintain an acceptable level of residual cyber risk after mitigating controls and other factors are considered, as well as how entities would respond to cyber incidents and threats. The standards would require senior leaders with responsibility for cyber risk oversight to be independent of the business line management and have direct access to the board of directors to deliver periodic updates on the firm's cyber risk exposure and risk management practices.[8]

2. ***Cyber risk management.*** The standards would require covered entities to integrate cyber risk management into the responsibilities of at least three independent functions with appropriate checks and balances: business units, independent risk management, and an audit function.[9]

   - *Business units.* Under the standards, units responsible for the day-to-day business functions of a covered entity would be required to assess, on an ongoing basis, the cyber risks associated with the activities of the business unit, and share that information with senior management as appropriate. Business units would be required to adhere to procedures and processes necessary to comply with the entity's cyber risk management framework.

   - *Independent risk management.* Under the standards, covered entities would be required to incorporate enterprise-wide risk management into the responsibilities of an independent risk management function. The function would report to the entity's chief risk officer and board of directors as appropriate regarding implementation of the entity's cyber risk management framework throughout the organization.

   - *Audit function.* Under the standards, a covered entity's audit function would be required to assess whether the entity's cyber risk management framework complies with the applicable laws and regulations and is appropriate for the entity's size, complexity, interconnectedness, and risk profile. The audit function would advise management and the board of directors on whether the entity's policies and procedures are adequate to keep up with emerging risks and industry requirements.

3. ***Internal dependency management.*** Internal dependency refers to "the business assets (i.e., workforce, data, technology, and facilities) of a covered entity upon which such entity depends to deliver services, as well as the information flows and interconnections among those assets."[10] Covered entities would be required to continually assess and improve their effectiveness in reducing cyber risks associated with internal dependencies on an enterprise-wide basis. An internal dependency management strategy would be incorporated into a covered entity's overall strategic risk management plan. Covered entities would be required to keep 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. Finally, a covered entity would be required to establish appropriate controls to address the inherent cyber risk of its assets.[11]

4. ***External dependency management.*** External dependency refers to "an entity's relationships with outside vendors, suppliers, customers, utilities (such as power and telecommunications), and other external organizations and service providers that the covered entity depends on to deliver services, as well as the information flows and interconnections between the entity and those external parties."[12] Covered entities would be required to

continually assess and improve their effectiveness in reducing cyber risks associated with external dependencies on an enterprise-wide basis. An external dependency management strategy would be incorporated into a covered entity's overall strategic risk management plan to address and reduce cyber risks associated with external dependencies and interconnection risks. Covered entities would be required to maintain a current, accurate, and complete awareness of, and prioritize, all external dependencies and trusted connections enterprise-wide based on their criticality to the business functions they support, the firm's mission, and the financial sector.[13]

5. ***Incident response, cyber resilience, and situational awareness.*** Standards in this area would be designed to ensure that covered entities plan for, respond to, contain, and rapidly recover from disruptions caused by cyber incidents. Covered entities would need to establish and maintain, among other things, enterprise-wide cyber resilience and incident response programs, based on their enterprise-wide cyber risk management strategies and supported by appropriate policies, procedures, governance, staffing, and independent review. They would also need to implement strategies to meet their obligations for performing core business functions in the event of a disruption, including the potential for multiple or concurrent or widespread interruptions and cyber-attacks on multiple elements of interconnected critical infrastructure, such as energy and telecommunications. Lastly, covered entities would be required to conduct specific testing that addresses disruptive, destructive, corruptive or any other cyber event that could affect their ability to service clients.[14]

Sector-Critical Standards

As noted above, the proposed rules include a higher set of standards for systems of covered entities that are critical to the functioning of the financial sector. The agencies seek comment on whether those critical systems include, among others, 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," as well as perhaps other markets such as exchange-traded and over-the-counter derivatives. The agencies also propose that critical systems might include 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."[15]

Among other requirements, covered entities would be required to minimize the residual cyber risk of sector-critical systems by implementing the most effective, commercially available controls, and to establish a recovery time objective ("RTO") of two hours for their sector-critical systems, validated by testing, to recover from a disruptive, corruptive, or destructive cyber event.[16]

Additional Proposals and Questions

Quantifying cyber risk. In the ANPR, the agencies also seek assistance in developing a consistent, repeatable methodology to support the ongoing measurement of cyber risk within covered entities, including potential methodologies to quantify both inherent and residual cyber risk and to compare entities across the financial sector.[17]

The form of the enhanced standards. The agencies are considering several regulatory approaches for establishing the enhanced standards proposed in the ANPR. The approaches include establishing standards through a policy statement or guidance, and imposing standards through a detailed regulation. The agencies are seeking feedback on possible approaches.[18]

Conclusion

Like the proposed cybersecurity rules issued by the New York Department of Financial Services ("DFS") last month,[19] the enhanced standards proposed in the ANPR would create new cybersecurity requirements for covered entities. While many of these are consistent with existing guidance, overall these standards are indeed "enhanced" and implementing and complying with these standards would likely prove to be costly and complex. Unlike the DFS proposed rules, the enhanced standards would not require a covered entity's board or senior officers to submit an annual certification of compliance.

And for most New York branches of foreign banks with U.S. assets of $50 billion or more, both the new federal standards and the DFS's forthcoming cybersecurity rules could potentially apply concurrently, absent an accommodation by one of the regulators.

The ANPR can be found here and the joint press release can be found here. Paul, Weiss's client memorandum discussing the proposed cybersecurity rules issued by the DFS can be found here.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Jack Baughman
212-373-3021
jbaughman@paulweiss.com

H. Christopher Boehning
212-373-3061
cboehning@paulweiss.com

Susanna M. Buergel
212-373-3553
sbuergel@paulweiss.com

Jessica S. Carey
212-373-3566
jcarey@paulweiss.com

Jay Cohen
212-373-3163
jaycohen@paulweiss.com

Roberto Finzi
212-373-3311
rfinzi@paulweiss.com

Michael E. Gertzman
212-373-3281
mgertzman@paulweiss.com

Roberto J. Gonzalez
202-223-7316
rgonzalez@paulweiss.com

Michele Hirshman
212-373-3747
mhirshman@paulweiss.com

Brad S. Karp
212-373-3316
bkarp@paulweiss.com

Lorin L. Reisner
212-373-3250
lreisner@paulweiss.com

Elizabeth M. Sacksteder
212-373-3505
esacksteder@paulweiss.com

Theodore V. Wells Jr.
212-373-3089
twells@paulweiss.com

Richard C. Tarlowe
212-373-3035
rtarlowe@paulweiss.com

Associate Andrew D. Reich contributed to this client alert.

[1] *See Enhanced Cyber Risk Management Standards*, October 19, 2016, to be codified at 12 CFR Part 30 and 12 CFR Part 364, available at https://www.fdic.gov/news/board/2016/2016-10-19_notice_dis_a_fr.pdf.

[2] *See id.* at 13–15 for a full list of proposed covered entities.

[3] *Id.* at 7.

[4] *Id.* at 1–2.

[5] *Id.* at 8–13.

[6] *Id.* at 17.

[7] *Id.* at 21–22.

[8] *Id.* at 23–27.

[9] *Id.* at 27–31.

[10] *Id.* at 22–23.

[11] *Id.* at 31–33.

[12] *Id.* at 23.

[13] *Id.* at 33–36.

[14] *Id.* at 37–41.

[15] *Id.* at 18–19.

[16] *Id.* at 41–43.

[17] *Id.* at 43–45.

[18] *Id.* at 45–47.

[19] For a more detailed discussion of the DFS proposed cybersecurity rules, see Paul, Weiss's client memorandum on this topic, available at https://www.paulweiss.com/media/3721011/15sept16cyber.pdf.