SULLIVAN & CROMWELL LLP

October 21, 2016

Federal Banking Agencies Solicit Comments on Enhanced Cyber Risk Management Standards

Once Established, Enhanced Cyber Risk Standards Would Apply to "Large and Interconnected" Banking Organizations and Certain Non-Bank Service Providers

SUMMARY

On October 19, 2016, the Board of Governors of the Federal Reserve System ("the Board"), the Office of the Comptroller of the Currency ("the OCC"), and the Federal Deposit Insurance Corporation ("the FDIC", and the three agencies collectively, "the Agencies") jointly issued an advance notice of proposed rulemaking ("the ANPR") soliciting public comment on enhanced cyber risk management standards. The Agencies are considering enhanced standards designed to increase the operational resilience of large and interconnected entities under their supervision and certain of their service providers and to reduce the potential impact of a cyber-attack or other cyber-related failure on the financial system. Once established, the enhanced standards would be integrated into the Agencies' existing IT supervisory framework. The Agencies are considering implementing the enhanced standards in a tiered manner, imposing more stringent standards on the systems of entities that are critical to the functioning of the financial sector. The Agencies plan to use the information collected through the ANPR to develop a more detailed proposal and have pledged to invite public comment on such proposal before adopting any final rule.

BACKGROUND

The ANPR arises out of the recognition that, as technology dependence in the financial sector continues to grow, so do the risks of high-impact failures and cyber-attacks. Due to the interconnectedness of the

U.S. financial system, a cyber incident or failure at one interconnected entity may affect not only the safety and soundness of that entity, but also other financial entities with potentially systemic consequences. Furthermore, third-party providers of IT and financial technology services to financial firms, such as payment processing and transactional account, loan and mortgage processing, are also vital to the safety and security of the financial sector. Although the Agencies have incorporated information security into their supervisory reviews for many years, in response to growing cybersecurity risks, the Agencies are now considering enhanced standards for the largest and most interconnected entities under their supervision, as well as certain of their third-party service providers.

DISCUSSION

The Agencies are considering applying the enhanced standards to regulated institutions that have total consolidated assets of $50 billion or more on an enterprise-wide basis, as well as to certain of their third-party service providers. The Board is also considering applying the standards to certain non-bank financial companies, "financial market utilities" and "financial market infrastructures." The ANPR refers to all entities that would be subject to the enhanced standards as "covered entities."

The proposed standards draw significantly on existing guidance and best practices issued by, among others, the federal banking agencies, the National Institute of Standards and Technology, and industry organizations. In its recommendation to the FDIC's Board of Directors, the FDIC staff noted that the enhanced standards should already be broadly familiar to most entities that fall within the scope of the proposal.

The ANPR addresses five categories of cyber standards: (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 particular aspects of such standards are described in the ANPR and the Staff Recommendation to the Board of Directors of the FDIC.[1]

As noted above, the Agencies are also considering a higher set of standards, referred to in the ANPR as "sector-critical standards," that would apply to the systems of covered entities that are deemed critical to the financial sector. These sector-critical standards would require such entities to substantially mitigate the risk of a disruption due to a cyber incident involving their sector-critical systems. Although the ANPR does not provide a definition of "sector-critical systems," it suggests that the definitions presented in the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, issued

[1] *See* ANPR, *available at*: https://www.fdic.gov/news/board/2016/2016-10-19_notice_dis_a_mem.pdf; and the FDIC Staff Recommendation, *available* at: https://www.occ.gov/news-issuances/news-releases/2016/nr-ia-2016-131a.pdf.

by the Board, the OCC and the Securities and Exchange Commission in 2003, provide a good starting point for identifying sector-critical systems that should be subject to the more stringent standards.[2]

The Agencies are considering three mechanisms for implementing the enhanced standards:

- A regulation requiring covered entities to maintain a risk management framework for cyber risks, in conjunction with supervisory guidance that describes minimum expectations for such framework;
- A regulation imposing specific cyber risk management standards on covered entities; or
- A regulation detailing the specific objectives and practices that covered entities would be required to achieve in each area of concern to demonstrate that the entity's cyber risk management program could adapt to changes in the entity's operations and to the evolving cybersecurity environment.

The Agencies are seeking public comment on, and ask a number of questions regarding, all aspects of the enhanced standards described in the ANPR.

The ANPR demonstrates the increasing importance that financial industry regulators are assigning to cybersecurity risks, particularly the risks posed by the interconnectedness of the largest financial institutions and the potential consequences should critical systems within these financial institutions be compromised by a cyber-attack. Also noteworthy is the Agencies' proposal to apply the enhanced standards to third-party service providers of such institutions. The ANPR is another indication that financial sector regulators are increasingly willing to consider much more detailed regulation of cybersecurity practices, rather than the less prescriptive approach that has prevailed until now.[3]

Institutions that would be subject to the enhanced standards should evaluate their cybersecurity policies, procedures and programs and compare them against the enhanced standards. Such institutions should also consider participating in the 90-day public comment period, whether directly or through their industry trade associations.

* * *

---

[2] *See* ANPR, *supra* note 1, at pg. 18 ("While there are different ways to gauge significance of such firms in critical markets, as a guideline, the agencies consider a firm significant in a particular critical market if it consistently clears or settles at least five percent of the value of transactions in that critical market.").

[3] *See* our memo entitled *New York Department of Financial Services Issues Proposed Cybersecurity Regulations: Regulated Institutions to be Required to Establish Cybersecurity Program and Policies, Appoint CISO, and Certify Compliance* (September 19, 2016), *available at* https://www.sullcrom.com/new-york-department-of-financial-services-issues-proposed-cybersecurity-regulations.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, three offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future related publications from Michael Soleta (+1-212-558-3974; soletam@sullcrom.com) in our New York office.

CONTACTS

New York		
Jay Clayton	+1-212-558-3445	claytonwj@sullcrom.com
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
Mitchell S. Eitel	+1-212-558-4960	eitelm@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
Nicole Friedlander	+1-212-558-4332	friedlandern@sullcrom.com
C. Andrew Gerlach	+1-212-558-4789	gerlacha@sullcrom.com
Scott D. Miller	+1-212-558-3109	millersc@sullcrom.com
Alexander J. Willscher	+1-212-558-4104	willschera@sullcrom.com
Michael M. Wiseman	+1-212-558-3846	wisemanm@sullcrom.com
Washington, D.C.		
Eric J. Kadel, Jr.	+1-202-956-7640	kadelej@sullcrom.com
Brent J. McIntosh	+1-202-956-6930	mcintoshb@sullcrom.com
Stephen H. Meyer	+1-202-956-7605	meyerst@sullcrom.com
Jennifer L. Sutton	+1-202-956-7060	suttonj@sullcrom.com
Samuel R. Woodall III	+1-202-956-7584	woodalls@sullcrom.com
Palo Alto		
Nader A. Mousavi	+1-650-461-5660	mousavin@sullcrom.com