COVINGTON

Federal Banking Agencies Request Comment on Enhanced Cybersecurity Standards

October 20, 2016

Financial Institutions, Cybersecurity

On October 19, 2016, the Board of Governors of the Federal Reserve System (Federal Reserve), Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC) (collectively the "Agencies") released a joint Advance Notice of Proposed Rulemaking (ANPR)[1] requesting public comment on enhanced cybersecurity standards that would apply to certain large, interconnected financial entities ("covered entities") as well as the third parties that provide services ("covered services") to such entities.[2]

The ANPR describes enhanced cybersecurity risk management standards that would apply to covered entities in five areas:

1. Cyber Risk Governance
2. Cyber Risk Management
3. Internal Dependency Management
4. External Dependency Management
5. Incident Response

In addition to enhanced standards in these five areas that would apply to all covered entities and covered services, the ANPR proposes applying an even more stringent set of requirements called "sector-critical standards" to the most critical systems of covered entities.

Our perception is that the enhanced cybersecurity standards being considered by the Agencies, if implemented in the form described in the ANPR, would have a substantial effect on the financial services industry and require very significant new efforts from covered entities and their service providers to both implement compliant processes and manage these processes on an ongoing basis.

The Agencies will evaluate public comments with respect to the ANPR in developing a more detailed proposal, which also will be issued for public comment. The ANPR requests comments

[1] The ANPR is available at: https://www.fdic.gov/news/board/2016/2016-10-19_notice_dis_a_fr.pdf.
[2] The ANPR also provides a helpful recitation of the various laws, regulations, and guidance that currently establish cybersecurity requirements for banking organizations, including the Gramm-Leach-Bliley Act, Uniform Rating System for Information Technology, FFIEC Information Technology Manual and FFIEC Cybersecurity Assessment Tool, and the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (2003).

in response to 39 questions relating to all aspects of the standards being considered. The deadline for submitting comments is January 17, 2017.

This alert summarizes the requirements described in the ANPR and identifies key questions among the 39 questions in the ANPR that should be evaluated carefully by the financial services industry.

Covered Entities and Services

The Agencies are considering applying the enhanced cybersecurity standards on an enterprise-wide basis to the following entities:

- U.S. bank holding companies and saving and loan holding companies with total consolidated assets of $50 billion or more, including their non-bank subsidiaries;
- U.S. operations of foreign banking organizations with total U.S. assets of $50 billion or more;
- Non-bank financial companies designated by the Financial Stability Oversight Council and supervised by the Federal Reserve;
- National banks and federal savings associations with total consolidated assets of $50 billion or more (and national banks and federal savings associations that are subsidiaries of a parent holding company with total consolidated assets of $50 billion or more);
- Federal branches of a foreign bank that has total consolidated assets of $50 billion or more;
- State-chartered banks with total consolidated assets of $50 billion or more (and state-chartered banks that are subsidiaries of a parent holding company with total consolidated assets of $50 billion or more);
- Financial market utilities designated as systemically important by the Financial Stability Oversight Council that are supervised by the Federal Reserve;
- Financial market infrastructures that are members of the Federal Reserve or that are operated by the Federal Reserve Banks.[3]

The Agencies also are considering applying the standards to third-party service providers with respect to services they provide to depository institutions and their affiliates that are covered entities—i.e., covered services.

[3] ANPR at 13-16.

Key ANPR Questions

1. How should the agencies consider broadening or narrowing the scope of entities to which the proposed standards would apply? What, if any, alternative size thresholds or measures of risk to the safety and soundness of the financial sector and the U.S. economy should the agencies consider in determining the scope of application of the standards? For example, should "covered entity" be defined according to the number of connections an entity (including its service providers) has to other entities in the financial sector, rather than asset size? If so, how should the agencies define "connections" for this purpose?

4. What are the most effective ways to ensure that services provided by third-party service providers to covered entities are performed in such a manner as to minimize cyber risk? What are the advantages and disadvantages of applying the standards to services by requiring covered entities to maintain appropriate service agreements or otherwise receive services only from third-party service providers that meet the standards with regard to the services provided, rather than applying the requirements directly to third-party service providers?

Enhanced Cyber Risk Management Standards

As noted, the enhanced cybersecurity standards under consideration by the Agencies would address the following areas for covered entities: (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.

Cyber Risk Governance

The cyber risk governance standards would address how a covered entity develops and maintains its formal cyber risk management strategy, as well as the allocation of responsibility within the entity for approving and implementing the strategy and overseeing its execution. The standards would be similar to those governance standards that large, complex financial organizations are expected to employ.[4] Standards in this area could include:

- Development of a written, board-approved, enterprise-wide cyber risk management strategy that is incorporated into the overall business strategy and risk management of the firm.
- Establishment of board-approved cyber risk tolerances consistent with the firm's risk appetite and strategy and management of cyber risk appropriate to the firm's operations.
- Requirement for the board of directors to have adequate cybersecurity expertise or to maintain access to resources or staff with such expertise.
- Requirement for the board of directors to have and maintain the ability to provide credible challenge to management in matters related to cybersecurity.
- Requirement for senior leaders with responsibility for cyber risk to be independent of business line management and to have direct, independent access to the board of directors.

[4] For an example of governance expectations established by the OCC, see 12 C.F.R. Part 30 Appendix D.

- Establishment of an enterprise-wide cyber risk management framework, including policies and reporting structures to support and implement the firm's cyber risk management strategy; reporting structures and expectations for independent risk management, internal control, and internal audit personnel; mechanisms for identifying and responding to cyber incidents and threats, and procedures for testing the effectiveness of the firm's cybersecurity protocol and updating them according to the evolving threat landscape.[5]

Key ANPR Questions

13. How would a covered entity determine that it is managing cyber risk consistent with its stated risk appetite and tolerances? What other implementation challenges does managing cyber risk consistent with a covered entity's risk appetite and tolerances present?

14. What are the incremental costs and benefits of establishing the contemplated standards for the roles, responsibilities, and adequate cybersecurity expertise (or access to adequate cybersecurity expertise) of the board of directors? To what extent do covered entities already have governance structures in place that are broadly consistent with the proposed cyber risk governance standards?

Cyber Risk Management

The enhanced standards would require, to the greatest extent possible and consistent with organizational structure, covered entities to integrate cyber risk management into three independent functions: (1) business units; (2) independent risk management; and (3) audit.

Business Units

Business units of covered entities would be responsible for assessing the cyber risks associated with their activities on an ongoing basis, and for sharing such information with senior management, including the CEO, in a timely manner. Business units would be required to assess the cyber risks associated with every business asset (i.e., workforce, data, technology, and facilities), service, and IT connection point for the respective unit and update these assessments as threats evolve.

Independent Risk Management

Covered entities would be required to incorporate enterprise-wide cyber risk management into the responsibilities of an independent risk management function. This function would report to the entity's Chief Risk Officer and board of directors regarding implementation of the cyber risk management framework. This function would also continuously monitor cyber risk on an enterprise-wide basis, and determine whether cyber risk management controls are consistent with the firm's cyber risk tolerances. The function would notify the CEO and board of directors when its assessment of a particular cyber risk differs from that of a business unit.

[5] ANPR at 23-26.

As a part of satisfying these requirements and other requirements set forth in the ANPR, the covered entity's independent risk management function would be required to have and maintain sufficient independence, stature, authority, resources, and access to the board of directors.

Audit

The audit function of covered entities would be responsible for evaluating the effectiveness of risk management, internal controls, and governance processes and advising the board of directors on whether those controls are keeping up with emerging risks. The audit function of a covered entity would be required to assess the cyber risk management framework for compliance with applicable laws and regulations, and to ensure the framework is appropriate for the size, complexity, interconnectedness, and risk profile of the firm. The audit function would also be required to incorporate an assessment of the entity's cyber risk management into its overall audit plan.[6] This assessment would entail an evaluation of the adequacy of the board-approved cyber risk management framework, including the entire security lifecycle, penetration testing, and other vulnerability assessment activities. Audit would additionally be responsible for assessing the business units' and independent risk management function's capabilities to adapt and remain in compliance with the firm's cyber risk management framework.

Key ANPR Question

15. The agencies seek comment on the appropriateness of requiring covered entities to regularly report data on identified cyber risks and vulnerabilities directly to the CEO and board of directors and, if warranted, the frequency with which such reports should be made to various levels of management? What policies do covered entities currently follow in reporting material cyber risks and vulnerabilities to the CEO and board of directors?

Internal Dependency Management

An "internal dependency" refers to the business assets (i.e., workforce, data, technology, and facilities) of a covered entity upon which the entity depends to deliver services and the information flows and interconnectedness among those assets. Standards for managing cyber risk with respect to an entity's internal dependencies could include:

- Development of an internal dependency management strategy, including policies, standards, and procedures to identify and manage cyber risks from internal assets, and integration of the strategy into the entity's overall strategic risk management plan.
- Maintenance of 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.
- Establishment of appropriate controls to address the inherent cyber risk of the firm's assets by assessing cyber risk prior to deployment, continually applying controls and monitoring assets and their operating environments over the lifecycle of the assets, and by mitigating identified deviations, granted exceptions, and known violations to internal dependency cyber risk management policies, standards, and procedures.

[6] Id. at 27-30.

- Requirement to continually apply appropriate controls to reduce the cyber risk of business assets to the board-approved levels.
- Requirement to periodically conduct tests of back-ups to business assets to achieve resilience.[7]

External Dependency Management

An "external dependency" is 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. Standards for managing cyber risk with respect to an entity's external dependencies could include:

- Development of an external dependency management strategy, including policies, standards, and procedures to identify and manage cyber risks from external assets, and integration of the strategy into the entity's overall strategic risk management plan.
- Establishment of policies, plans, and procedures to identify and manage real-time cyber risks associated with external dependencies, particularly those connected to or supporting sector-critical systems and operations.
- Development of a current (i.e., real time), accurate, and complete awareness of, and priority to, all external dependencies based on criticality to the business functions supported, the firm's mission, and the financial sector.
- Establishment and application of appropriate controls to address the cyber risk presented by each external partner throughout the lifespan of the relationship.
- Requirement that covered entities analyze and address cyber risks that emerge from reviews of external relationships and periodically test alternative solutions in the event an external partner fails to perform as expected.[8]

[7] Id. at 31-33.
[8] Id. at 33-35.

Key ANPR Questions

17. The agencies request comment on the comprehensiveness and effectiveness of the proposed standards for internal and external dependency management in achieving the agencies' objective of increasing the resilience of covered entities, third-party service providers to covered entities, and the financial sector.

19. How do the proposed internal and external dependency management standards compare with processes already in place at banking organizations?

21. How would the proposed standards for internal and external dependency management impact a covered entity's use of a third-party service provider?

22. What additional issues should the agencies consider related to internal and external dependency management and the covered entities' use of third-party service providers? How should those issues be evaluated by the agencies?

Incident Response, Cyber Resilience, and Situational Awareness

Covered entities would be required to plan for, respond to, contain, and rapidly recover from disruptions caused by cyber incidents, thereby strengthening their cyber resilience as well as that of the financial sector. Standards in this area could include:

- Establishment and maintenance of effective incident response and cyber resilience governance, strategies, and capacities in order to withstand, contain, and rapidly recover from a disruption caused by a significant cyber event.
- Establishment of a plan to identify and mitigate the cyber risks posed by the entity through interconnectedness to sector partners and external stakeholders to prevent cyber contagion.
- Establishment of an enterprise-wide cyber resilience and incident response program, supported by appropriate policies, procedures, governance, staffing, and independent review.
- Establishment and implementation of strategies to meet the entity's obligations for performing core business functions in the event of a disruption.
- Establishment of protocols for secure, immutable, off-line storage of critical records, including financial records, loan data, asset management account information, and daily deposit account records.
- Establishment of 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 provider is unable to perform.
- Conduct of specific testing that addresses disruptive, destructive, corruptive, or any other cyber event that could affect the entity's ability to service clients, including testing external dependencies.

- Maintenance of ongoing situational awareness of the entity's operational status and cybersecurity posture to preempt cyber events and respond rapidly.
- Establishment and maintenance of threat profiles for identified threats to the firm, threat modeling capabilities, actionable cyber threat intelligence, and security analytics on an ongoing basis.[9]

Key ANPR Questions

23. How well do the proposed standards for incident response, cyber resilience, and situational awareness address the safety and soundness of individual financial institutions and potential systemic cyber risk to the financial sector, including with respect to the testing strategies and approaches? How could they be improved?

25. How do covered entities currently evaluate their incident response and cyber resilience capabilities? What factors should the agencies consider essential in considering a covered entity's incident response and cyber response capabilities?

27. What other factors should be included within the incident response, cyber resilience, and situational awareness category?

Sector-Critical Systems

In addition to the above enhanced standards, the ANPR notes that the Agencies are considering even more stringent standards for "sector-critical systems." Sector-critical systems could be those systems that:

- Support the clearing or settlement of at least five percent of the value, on a consistent basis, of transactions in the markets for federal funds, foreign exchange, commercial paper, U.S. government and agency securities, and corporate and debt securities;
- Support the clearing or settlement of at least five percent of the value, on a consistent basis, of transactions in other markets, such as exchange-traded and over-the-counter derivatives, or that support the maintenance of a significant share (at least five percent) of the total U.S. deposits or balances due from other depository institutions in the United States; or
- Provide key functionality to the financial sector for which alternatives are limited or nonexistent or would take excessive time to implement.

Standards applicable to sector-critical systems also would apply to the services provided by third-parties to support covered entities' sector-critical systems.

The more stringent standards applicable to sector-critical systems could include:

- Minimization of the residual cyber risk of sector-critical systems by implementing the most effective, commercially available controls by substantially mitigating the risk of a disruption or failure due to a cyber event.

[9] Id. at 37-40.

- Establishment of an RTO (i.e., amount of time in which a firm aims to recover clearing and settlement activities after a wide-scale disruption with the overall goal of completing material pending transactions on the scheduled settlement date) of two hours for sector-critical systems.
- Requirement for Federal Reserve-supervised covered entities, at the holding company level, to measure quantitatively their ability to reduce the aggregate residual cyber risk of a sector-critical system and to reduce such risk to a minimal level.[10]

Key ANPR Questions

29. The agencies request comment on the appropriateness and feasibility of establishing a two-hour RTO for all sector-critical systems. What would be the incremental costs to covered entities of moving toward a two-hour RTO objective for these systems?

30. What impact would a two-hour RTO have on covered entities' use of third-party service providers? What challenges or burdens would be presented by the requirement of a two-hour RTO for covered entities who rely on third-party service providers for their critical systems? How would the agencies weigh such costs against other costs associated with implementing the enhanced standards outlined in this ANPR?

31. How should the agencies implement the two-hour RTO objective? For example, would an extended implementation timeline help to mitigate costs, and if so, what timeline would be reasonable?

33. The Federal Reserve requests comment on the benefits of requiring Federal Reserve-supervised covered entities, at the holding company level, to measure the residual cyber risk of their sector-critical systems on a quantitative basis. How would this approach to measuring cyber risk compare with efforts already underway at holding companies to manage and measure their cyber risk? For example, what processes do holding companies already have in place to measure their residual cyber risk? What challenges and costs would holding companies face in measuring their residual cyber risk quantitatively? What are the benefits of requiring holding companies to reduce the residual risk of their sector-critical systems to a minimal level, taking into account the risks associated with internal and external dependencies connected to or supporting their sector-critical systems?

Approach to Quantifying Cyber Risk

The Agencies are interested in receiving comments on potential methodologies to quantify inherent and residual cyber risk and compare entities across the financial sector. The ANPR notes the FAIR Institute's Factor Analysis of Information Risk and the Carnegie Mellon's Goal-Question-Indicator-Metric process, and indicates that the Agencies are considering how to build on these methodologies to measure cyber risk in a consistent, repeatable manner.

[10] Id. at 41-42.

Key ANPR Questions

34. What current tools and practices, if any, do covered entities use to assess the cyber risks that their activities, systems, and operations pose to other entities within the financial sector, and to assess the cyber risks that other entities' activities, systems, and operations pose to them? How is such risk currently identified, measured, and monitored?

36. What methodologies should the agencies consider for the purpose of measuring inherent and residual cyber risk quantitatively and qualitatively? What risk factors should agencies consider incorporating into the measurement of inherent risk? How should the risk factors be consistently measured and weighted?

Approach to Implementing Enhanced Standards

The Agencies are also seeking comment on which of three proposed regulatory approaches is most appropriate to implement the enhanced standards:

- Combination of a regulatory requirement to maintain an appropriate cyber risk management framework, along with a policy statement or guidance that explains the minimum expectations for such a framework (such as the *Interagency Guidelines Establishing Standards for Safety and Soundness* and the *Interagency Guidelines Establishing Information Security Standards*);
- Formal regulations that impose high-level cyber risk management standards addressing each of the five areas of cyber risk management and are to be used as the supervisory basis for the Agencies' examination of covered entities and covered services; or
- Formal regulations with more prescriptive requirements regarding specific objectives and practices a covered entity would need to achieve in each of the five areas of cyber risk management to demonstrate that its cyber risk management program is able to adapt to changes in operations and the evolving cyber environment.

Key ANPR Question

34. What are the potential benefits or drawbacks associated with each of the options for implementing the standards discussed above?

* * *

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Financial Institutions and Cybersecurity practices:

Michael Nonaka	+1 202 662 5727	mnonaka@cov.com
Stuart Stock	+1 202 662 5384	sstock@cov.com
David Fagan	+1 202 662 5291	dfagan@cov.com
Jenny Martin	+1 212 841 1018	jrmartin@cov.com
John Dugan	+1 202 662 5051	jdugan@cov.com
James Garland	+1 202 662 5337	jgarland@cov.com
Mark Plotkin	+1 202 662 5656	mplotkin@cov.com
D. Jean Veta	+1 202 662 5294	jveta@cov.com
Steve Surdu	+1 202 662 5737	ssurdu@cov.com
Lucille Andrzejewski	+1 202 662 5079	landrzejewski@cov.com
Randy Benjenk	+1 202 662 5041	rbenjenk@cov.com
Kate Goodloe	+1 202 662 5505	kgoodloe@cov.com
Nikhil Gore	+1 202 662 5918	ngore@cov.com
Jason Grimes	+1 202 662 5846	jgrimes@cov.com