ALSTON&BIRD

CYBER ALERT

A Publication of the Cybersecurity Preparedness & Response Team

ALSTONSECURITY.COM NOVEMBER 8, 2016

Major Bank Regulators Propose Expanded Cybersecurity Regulations

By Jim Harvey, Kim Peretti and Jason Wool

On October 19, 2016, the Board of Governors of the Federal Reserve System ("Board"), the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC) (the "agencies") issued a joint advance notice of proposed rulemaking (ANOPR), titled "Enhanced Cyber Risk Management Standards," that would constitute a marked expansion of the agencies' cybersecurity regulations. The proposed rules, which would apply a robust set of cyber risk management standards to large jurisdictional entities, are premised on the notion that "the interconnectedness of the U.S. financial system" means 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."

While none of the concepts embodied in the ANOPR are new, the depth and breadth of the potential regulations and their potential applicability not only to banks but to service providers as well is unprecedented in the context of cyber risk management. Indeed, until now, government regulation of cyber risk management has primarily been of the "light touch" variety, such as voluntary standards, e.g., the NIST Framework for Improving Critical Infrastructure Cybersecurity, or regulatory guidance, such as FINRA's 2015 Report on Cybersecurity Practices. For the financial services sector, while the Federal Financial Institutions Examination Council's (FFIEC) IT Handbook has long addressed many topics covered in the ANOPR to provide guidance on bank examinations, the proposed rule would convert these topics into formal regulations, similar to the Interagency Guidelines Establishing Information Security Standards.

The agencies are requesting comments on all aspects of the ANOPR by January 17, 2017.

Scope

The agencies are considering applying the new requirements on an *enterprise-wide basis* to large jurisdictional institutions, specifically those with total consolidated assets of $50 billion or more, as well as "third-party service providers with respect to services provided to depository institutions and their affiliates that are covered entities (covered services)." This would include, for example, bank holding companies, U.S. operations of foreign banking organizations, savings and loan holding companies, nonbank financial companies supervised by the board, national banks, federal savings associations, state nonmember banks and more. These covered entities would need to apply the new "enhanced standards" to *all systems* at the enterprise.

The agencies are also considering a second tier of enhanced standards, which would apply to so-called "sector-critical systems," which are systems that are "critical to the financial sector." The agencies are considering defining these systems as those "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 "systems that support the clearing or settlement of at least five percent of the value of transactions (on a consistent basis) in other markets (for example, exchange-traded and over-the-counter derivatives), or 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." The agencies are also considering additional factors that could cause a system to be considered sector-critical, such as substitutability and interconnectedness.

Proposed Enhanced Standards

The agencies are considering requiring covered entities to implement enterprise-wide, enhanced cyber risk management standards that fall under five categories: cyber risk governance, cyber risk management, internal dependency management, external dependency management and incident response, cyber resilience and situational awareness.

Cyber risk governance

These standards would be similar to the governance standards generally expected for large, complex financial organizations, such as:

- The board of directors, or an appropriate board committee, of a covered entity must be responsible for approving the entity's cyber risk management strategy and holding senior management accountable for establishing and implementing appropriate policies consistent with the strategy.
- The 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.
- A requirement that the entity's board establish cyber risk tolerances consistent with the firm's risk appetite and strategy, and manage cyber risk appropriate to the nature of the operations of the firm.
- A requirement that the entity's board review and approve the enterprise-wide cyber risk appetite and tolerances of the covered entity.
- A requirement to reduce residual cyber risk to the appropriate level approved by the board of directors.
- A requirement that the board of directors have adequate expertise in cybersecurity or maintain access to resources or staff with such expertise so as to be able to provide credible challenge to management in matters related to cybersecurity and the evaluation of cyber risks and resilience.
- A requirement that senior leaders with responsibility for cyber risk oversight be independent of business line management.
- A requirement to establish an enterprise-wide cyber risk management framework that would include policies and reporting structures to support and implement the entity's cyber risk management strategy.

Cyber risk management

These standards would require integration of cyber risk management into the responsibilities of at least three independent functions – business units, an independent risk management function and an audit function – with appropriate checks and balances.

Business units

- Assess, on an ongoing basis, the cyber risks associated with the activities of the business unit, including assessing the cyber risks and potential vulnerabilities associated with every business asset (that is, their workforce, data, technology and facilities), service and IT connection point for the respective unit, and update these assessments as threats, technology and processes evolve.
- Share information on identified risks with senior management in a timely manner.
- Adhere to procedures and processes necessary to comply with the entity's cyber risk management framework, including those designed to identify, measure, monitor and control cyber risk consistent with risk appetite and tolerance.

Independent risk management

- Incorporate enterprise-wide cyber risk management into the responsibilities of an independent risk management function, which would report to the chief risk officer and board of directors concerning the entity's implementation of its cyber risk management framework.
- Analyze cyber risk at the enterprise level to identify and ensure effective response to events with the potential to impact one or multiple operating units.
- Continually assess the firm's overall exposure to cyber risk and promptly notify the CEO and board of directors, as appropriate, when its assessment of a particular cyber risk differs from that of a business unit, as well as any instances when a unit of the covered entity has exceeded the entity's established cyber risk tolerances.
- Continually identify, measure and monitor cyber risk across the enterprise and determine whether cyber risk controls are appropriately in place across the enterprise consistent with the entity's established risk appetite and tolerances.
- Identify and assess the covered entity's material aggregate risks on an ongoing basis and determine whether actions need to be taken to strengthen risk management or reduce risk given changes in the covered entity's risk profile or other conditions, placing particular emphasis on sector-critical systems.
- Assess the completeness, effectiveness and timeliness with which the firm reduces the aggregate residual cyber risk of their systems to the appropriate, board-of-directors-approved level.
    - The Board, in particular, is considering requiring covered entities at the holding company level to quantitatively measure the completeness, effectiveness and timeliness with which they reduce aggregate residual cyber risk.

Audit function

- Assess whether the cyber risk management framework of a covered entity complies with applicable laws and regulations and is appropriate for its size, complexity, interconnectedness and risk profile.
- Incorporate an assessment of cyber risk management into the overall audit plan of the covered entity, including an evaluation of the adequacy of compliance with the board-approved cyber risk management framework and cyber risk policies, procedures and processes established by the firm's business units or independent risk management.

Internal dependency management

- Integrate an internal dependency management strategy into the entity's overall strategic risk management plan.
- Maintain 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, including mappings to other assets and other business functions, information flows and interconnections.
- Track connections among assets and cyber risk levels throughout the life cycles of the assets and support relevant data collection and analysis across the organization.
- Provide timely notification of internal cyber risk management issues to designated internal stakeholders.
- Establish and apply appropriate controls to address the inherent cyber risk of a covered entity's assets (taking into account the prioritization of the entity's business assets and the cyber risks they pose to the entity). This includes:
  - Assessing the cyber risk of assets and their operating environments before deployment.
  - Continually applying controls and monitoring assets and their operating environments (including deviations from baseline cybersecurity configurations) over the life cycle of the assets.
  - Assessing relevant cyber risks to the assets (including insider threats to systems and data) and mitigating identified deviations, granted exceptions and known violations to internal dependency cyber risk management policies, standards and procedures.
- Periodically conduct tests of backups to business assets to achieve resilience.

External dependency management

- Integrate an external dependency management strategy into the entity's overall strategic risk management plan to address and reduce cyber risks associated with external dependencies and interconnection risks, which would ensure that roles and responsibilities for external dependency management are well defined; establish and regularly update policies, standards and procedures for external dependency management throughout the lifespan of the relationship (for example, due diligence, contracting and subcontracting, onboarding, ongoing monitoring, change management, off-boarding); put appropriate metrics in place to measure effectiveness in reducing cyber risks associated with external dependencies; and put appropriate compliance mechanisms in place.
- Establish effective 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, throughout their lifespans.

- Have 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.
- Prioritize monitoring, incident response and recovery of systems critical to the enterprise and the financial sector; support the continued reduction of the cyber risk exposure of external dependencies to the enterprise and the sector until the board-approved cyber risk appetite and tolerances are achieved; support timely responses to cyber risks to the enterprise and the sector; monitor the universe of external dependencies that connect to assets supporting systems critical to the enterprise and the sector; support relevant data collection and analysis across the organization; and track connections among external dependencies, organizational assets and cyber risk levels throughout their lifespans.
- Establish and apply appropriate controls to address the cyber risk presented by each external partner throughout the lifespan of the relationship.
- Analyze and address the cyber risks that emerge from reviews of external relationships, and identify and periodically test alternative solutions in case an external partner fails to perform as expected.
- Continually apply and evaluate appropriate controls to reduce the cyber risk of external dependencies to the enterprise and the sector.

Incident response, cyber resilience and situational awareness

- Establish and maintain effective incident response and cyber resilience governance, strategies and capacities that enable the organizations to anticipate, withstand, contain and rapidly recover from a disruption caused by a significant cyber event.
- Establish and implement plans to identify and mitigate the cyber risks they pose through interconnectedness to sector partners and external stakeholders to prevent cyber contagion.
- Establish and maintain enterprise-wide cyber resilience and incident response programs, based on enterprise-wide cyber risk management strategies and supported by appropriate policies, procedures, governance, staffing and independent review.
- Establish and implement strategies to meet the entity's obligations for performing core business functions in the event of a disruption, including the potential for multiple concurrent or widespread interruptions and cyber-attacks on multiple elements of interconnected critical infrastructure, such as energy and telecommunications.
- Establish protocols for secure, immutable, off-line storage of critical records, including financial records of the institution, loan data, asset management account information and daily deposit account records, including balances and ownership details, formatted using certain defined data standards to allow for restoration of these records by another financial institution, service provider or the FDIC in the event of resolution.
- Establish plans and mechanisms to transfer business, where feasible, to another entity or service provider with minimal disruption and within prescribed timeframes if the original covered entity or service provider is unable to perform.

- Conduct specific testing that addresses disruptive, destructive, corruptive or any other cyber event that could affect the ability to service clients and create significant downtime that would threaten the business resilience of clients.
  - The testing would need to address external interdependencies, such as connectivity to markets, payment systems, clearing entities, messaging services and other critical service providers or partners; be undertaken jointly where critical dependencies exist; and validate the effectiveness of internal and external communication protocols with stakeholders.
- Maintain an ongoing situational awareness of their operational status and cybersecurity posture to preempt cyber events and respond rapidly to them.
- Establish and maintain threat profiles for identified threats to the firm, establish and maintain threat modeling capabilities, gather actionable cyber threat intelligence and perform security analytics on an ongoing basis, and establish and maintain capabilities for ongoing vulnerability management.

Proposed Sector-Critical Standards

For entities with sector-critical systems, the agencies are considering the following requirements, which would apply only to the sector-critical systems and not across the enterprise (unlike the other enhanced cyber risk management standards):

- Minimize the residual cyber risk of sector-critical systems by implementing the most effective commercially available controls.
- Establish a recovery time objective (RTO) of two hours for sector-critical systems, validated by testing, to recover from a disruptive, destructive or corruptive cyber event.
- The Board is specifically considering requiring, at the holding company level, jurisdictional entities to measure (quantitatively) their ability to reduce the aggregate residual cyber risk of their sector-critical systems and their ability to reduce such risk to a minimal level.

Implementation of Enhanced Standards

The agencies state that they are considering a number of paths forward to implement the enhanced standards requirements. They specifically identify the following possible options:

- The agencies could propose the standards as a combination of a regulatory requirement to maintain a risk management framework for cyber risks along with a policy statement or guidance that describes minimum expectations for the framework, such as policies, procedures and practices commensurate with the inherent cyber risk level of the covered entity.
- The agencies could propose regulations that impose specific cyber risk management standards, but without specifying the required activities in detail.
- The agencies could propose a regulatory framework that is more detailed than the second approach.

Given that the format of the proposed standards could have a significant impact on entities' compliance activities, potential covered entities may wish to comment on this section in particular.

If you have any questions or would like additional information, please contact Kimberly Peretti, Jim Harvey or Jason Wool.

Cybersecurity Preparedness & Response Team Co-Chairs

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com

Follow us: @AlstonPrivacy | www.AlstonPrivacy.com

www.alstonsecurity.com

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: 2828 North Harwood Street ■ 18th Floor ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RESEARCH TRIANGLE: 4721 Emperor Blvd. ■ Suite 400 ■ Durham, North Carolina, USA, 27703-85802 ■ 919.862.2200 ■ Fax: 919.862.2260
SILICON VALLEY: 1950 University Avenue ■ 5th Floor ■ East Palo Alto, California, USA, 94303-2282 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333