


**MEMORANDUM TO:** The Board of Directors  
**FROM:** Doreen R. Eberley   
Director, Division of Risk Management Supervision  
**DATE:** October 6, 2016  
**SUBJECT:** ANPR- Enhanced Cyber Risk Management Standards

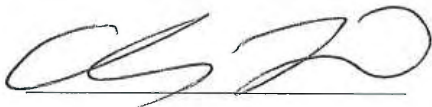
**Summary of Staff Recommendation**

Staff recommends that the Board of Directors (Board) of the Federal Deposit Insurance Corporation (FDIC) approve the attached Advance Notice of Proposed Rulemaking entitled *Enhanced Cyber Risk Management Standards* (ANPR) and authorize publication of the ANPR in the *Federal Register* for a 90-day comment period. The ANPR would be issued jointly by the Board of Governors of the Federal Reserve System (FRB), the Office of the Comptroller of the Currency (OCC), and the FDIC (collectively, the Agencies).

The ANPR would invite comment on the Agencies' consideration of enhanced cyber risk management standards (enhanced standards) for the largest and most interconnected entities under their supervision and those entities' service providers. The enhanced standards would be intended to increase the entities' operational resilience and reduce the impact on the financial system in the event of a failure, cyber attack, or the failure to implement appropriate cyber risk management. The enhanced standards would cover five categories: (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.

At the end of each section of the ANPR, the Agencies have included specific questions on which they are requesting comment.

**Concur:**



Charles Yi, General Counsel

## **Background**

Financial institutions and consumers have become increasingly dependent on information technology (IT) to facilitate financial transactions. The largest and most complex financial institutions rely heavily on IT to engage in national and international banking activities and to provide critical services to the financial sector and the U.S. economy. As this dependence grows, so does the opportunity for high-impact IT failures and cyber-attacks. Due to the increasing interconnectedness of the U.S. financial system, a cyber incident or IT failure at one entity may impact the safety and soundness of other financial entities and introduce potentially systemic consequences.

Depository institutions and depository institution holding companies play an important role in U.S. payment, clearing, and settlement arrangements, and provide access to credit for businesses and households. Non-bank financial companies supervised by the FRB perform critical functions for the U.S. financial system, and financial market infrastructures (FMIs) facilitate the payment, clearing, and recording of monetary and other financial transactions and services and play critical roles in fostering financial stability in the U.S. Non-financial institution third parties that provide payments processing, core banking (e.g., transactional account, loan, and mortgage processing), and other IT services to the foregoing also play a vital role in the financial sector.

For these reasons, the Agencies wish to publish this ANPR to solicit public comment on a series of specific proposed standards for certain large and interconnected financial entities, relating to how those entities identify, measure, mitigate, and monitor various types of cyber risks. 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, and should already be broadly familiar to most of the entities that fall within the proposed scope. Through a series of questions posed in connection with each aspect of the proposed standards, the ANPR solicits public comment in several areas, including the stringency of various proposed standards; their comprehensiveness and effectiveness in achieving the Agencies' objectives; the feasibility of compliance; costs and benefits to the covered entities; practical challenges in implementing controls that address the standards; current practices that may already address the risks identified by the Agencies; and alternative proposals and standards that the Agencies may not have considered.

The enhanced standards would be integrated into the existing IT supervisory framework. The Agencies are considering implementing the standards in a tiered manner:

- *Enhanced standards* would apply to all systems of covered entities.
- *Sector critical standards*, the highest level, would apply to systems of covered entities determined by the Agencies to be critical to the financial sector.

## **Scope**

The Agencies are proposing that the enhanced standards apply to the following:

- Those U.S. bank holding companies, U.S. operations of foreign banking organizations, and U.S. savings and loan holding companies with total consolidated assets of \$50 billion or more;

- Non-bank subsidiaries of covered bank holding companies;
- Non-bank financial companies supervised by the FRB pursuant to section 165 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act);
- Financial market utilities (FMUs) designated by the FSOC for which the FRB is the supervisory agency pursuant to sections 805 and 810 of the Dodd-Frank Act;
- Financial market infrastructures (FMIs) over which the FRB has primary supervisory authority;
- FMIs that are operated by the Federal Reserve Banks;
- Depository institutions and any subsidiaries thereof with total consolidated assets of \$50 billion or more, under the respective jurisdictions of each of the Agencies; and
- Third-party service providers with respect to services provided to covered depository institutions and their affiliates.

The Agencies are also considering requiring nonbank financial companies and Board-supervised FMIs to verify that any services received from third parties are subject to the same standards that would apply if the services were being conducted by those entities directly.

### **Cyber Risk Management Standards**

The Agencies are considering organizing the enhanced standards into 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:*** This entails developing and maintaining a formal cyber risk management strategy, as well as a framework of policies and procedures to implement the strategy, that are integrated into the overall strategic plans and governance structures of covered entities. These standards would provide that the board of directors of a covered entity be responsible for approving the entity's cyber risk management strategy and for holding senior management accountable for establishing and implementing appropriate policies consistent with the strategy.

Specifically, the Agencies are considering requiring covered entities to develop a written, board-approved, enterprise-wide cyber risk management strategy that is incorporated into the overall business strategy and risk management of the firm. Further, the board would be expected to review and approve an enterprise-wide cyber risk appetite and tolerances. The Agencies are considering requiring the board of a covered entity to have adequate expertise in cybersecurity or to maintain access to personnel with such expertise. Also, the Agencies are considering requiring senior leaders with responsibility for cyber risk oversight to be independent of business line management and have direct independent access to the board.

***Cyber risk management:*** The enhanced standards being considered would require covered entities to integrate cyber risk management into at least three independent functions: (1) business units, (2) independent risk management, and (3) audit.



Business units responsible for day-to-day business functions would be required to assess cyber risks associated with business activities on an ongoing basis and share that information with senior management, including the chief executive officer. Business units would also be required to adhere to procedures and processes to effectively identify, measure, monitor, and control cyber risk consistent with the entity's risk appetite and tolerances. They would also be expected to ensure that they maintain, or have access to, resources and staff with the skill sets needed to comply with the unit's cybersecurity responsibilities.

The Agencies are considering requiring covered entities 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 regarding implementation of the cyber risk management framework. Independent risk management would be required to continuously identify, measure, and monitor cyber risk across the enterprise, and determine whether controls are consistent with established risk tolerances. Entities would be required to assess the completeness, effectiveness, and timeliness with which they achieve aggregate residual risk levels established by the board.

The Agencies are considering requiring the audit function to assess whether a covered entity's cyber risk management framework complies with applicable laws and regulations and is appropriate for its size, complexity, interconnectedness, and risk profile. Further, audit would be required to incorporate an assessment of cyber risk management into the entity's overall audit plan. More specifically, the audit would be required to include an evaluation of penetration testing and other vulnerability assessment activities, as appropriate to the covered entity.

**Internal dependency management:** The Agencies are considering requiring covered entities to integrate an internal dependency management strategy into the overall strategic plan to ensure that roles and responsibilities for internal dependency management are well defined; to establish and update policies, standards, and procedures to identify and manage cyber risks associated with internal assets throughout the assets' lifespans; to ensure appropriate oversight to monitor effectiveness in reducing cyber risks associated with internal dependencies; and to adopt appropriate compliance mechanisms.

The Agencies are considering requiring covered entities to 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. The Agencies are also considering requiring covered entities to establish and apply appropriate controls to address the inherent cyber risk of their assets, taking into account the prioritization of the entity's business assets and the cyber risks they pose to the entity.

**External dependency management:** The Agencies are considering requiring covered entities to integrate an external dependency management strategy into the overall strategic management plan to ensure that roles and responsibilities for external dependency management are well-defined; to establish and update policies, standards and procedures throughout the lifespan of the relationship; and to adopt appropriate metrics to measure effectiveness and compliance.

The Agencies are also considering requiring covered entities to have a current, accurate, complete, and prioritized awareness of 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. Entities should support the continued reduction of the cyber risk exposure of external dependencies until the board-approved cyber risk tolerance level is achieved.

In addition, the Agencies are considering requiring covered entities to analyze and address the cyber risks that emerge from reviews of their external relationships, and identify and periodically test alternative solutions in case an external partner fails to perform as expected.

**Incident response, cyber resilience, and situational awareness:** Under the enhanced standards being considered, covered entities would be required to be capable of operating critical business functions in the face of cyber-attacks and continuously enhance their cyber resilience. The Agencies are considering requiring covered entities to establish and implement plans to identify and mitigate the cyber risks posed through interconnectedness to sector partners and external stakeholders to prevent cyber contagion.

The Agencies are also considering requiring covered entities to establish and implement strategies to meet their 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.

In addition, the Agencies are considering requiring covered entities to establish protocols for secure, immutable, off-line storage of critical records, including financial records, loan data, asset management account information, and daily deposit records, including balances and ownership details, formatted using certain defined data standards to allow for restoration by another financial institution, service provider, or the FDIC as receiver.

The Agencies are considering requiring entities to establish plans and mechanisms to transfer business, where feasible, to another service provider or entity with minimal disruption and within prescribed timeframes if the covered entity or service provider is unable to perform.

The Agencies are considering requiring entities to conduct specific testing that addresses disruptive cyber events that could affect their ability to service clients.

Lastly, the Agencies are considering requiring entities to maintain on ongoing situational awareness of their operational status and cybersecurity posture to pre-empt cyber events and respond rapidly to them.

### **Sector Critical Systems**

The Agencies are considering application of the enhanced standards to the systems of all covered entities, with higher Sector Critical Standards applying to systems of covered entities that are deemed critical to the financial sector. In defining sector critical systems, the Agencies proceed from the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, published in 2003. The Agencies are considering that the following be regarded as sector critical systems:

- Systems that support the clearing or settlement of at least five percent of the value of transactions (on a consistent basis, to be defined) 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;

- Systems that support the clearing or settlement of at least five percent of the value of transactions (on a consistent basis, to be defined) in other markets (e.g., exchange-traded and over-the-counter derivatives) or support the maintenance of a significant share (e.g., five percent) of the total U.S. deposits or balances due from other depository institutions in the U.S.;
- Systems that provide key functionality (to be defined) to the financial sector for which alternatives are limited or nonexistent, or would take excessive time to implement (e.g., due to incompatibility) if significantly disrupted;
- Systems of non-covered entities supervised by an Agency that are otherwise determined by the Agencies to provide critical functionality to the financial sector, following notice to the entity and an opportunity to respond; and
- Services provided by third parties that support covered entities' sector-critical systems.

For sector critical systems, the Agencies are considering requiring covered entities to minimize the residual risk of such systems by implementing the most effective, commercially available controls.

The Agencies are also considering requiring covered entities to establish a recovery time objective of two hours for their sector critical systems, validated by testing, to recover from a disruptive, corruptive, or destructive cyber event.

### **Implementation of the Standards**

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

- A regulation requiring entities to maintain a risk management framework for cyber risks, in conjunction with supervisory guidance that describes minimum expectations for the framework;
- A regulation that imposes specific cyber risk management standards; or
- A regulation that would include details on the specific objectives and practices a covered entity would be required to achieve in each area of concern in order 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.

**Recommendation**

Staff recommends that the Board approve the attached Resolution to adopt and authorize for publication in the *Federal Register* the attached ANPR for public comment.

RMS Contacts:        Mark Moylan, Deputy Director (x40867)  
                             Don Saxinger, Senior Examination Specialist (x40214)

Legal Contact:        John Dorsey, Counsel (x83807)

Attachments