**DEPARTMENT OF THE TREASURY**

**Office of the Comptroller of the Currency**

12 CFR Part 30

Docket ID OCC-2016-0016

RIN 1557-AE06

**FEDERAL RESERVE SYSTEM**

12 CFR Chapter II

Docket No. R-1550

RIN 7100-AE 61

**FEDERAL DEPOSIT INSURANCE CORPORATION**

12 CFR Part 364

RIN 3064-AE45

**Enhanced Cyber Risk Management Standards**

**AGENCIES**: The Board of Governors of the Federal Reserve System; the Office of the Comptroller of the Currency; and the Federal Deposit Insurance Corporation.

**ACTION**: Joint advance notice of proposed rulemaking.

**SUMMARY**: 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) (collectively, the agencies) are inviting comment on an advance notice of proposed rulemaking (ANPR) regarding enhanced cyber risk management standards (enhanced standards) for large and interconnected entities under their supervision and those entities' service providers. The agencies are considering establishing enhanced standards to increase the operational resilience of these entities and reduce the impact on the financial system in case of a cyber event experienced

by one of these entities. The ANPR addresses five categories of cyber standards: cyber risk governance; cyber risk management; internal dependency management; external dependency management; and incident response, cyber resilience, and situational awareness. The agencies are considering implementing the enhanced standards in a tiered manner, imposing more stringent standards on the systems of those entities that are critical to the functioning of the financial sector.

**DATES**: Comments must be received by January 17, 2017.

**ADDRESSES**: Comments should be directed to:

Board: When submitting comments, please consider submitting your comments by e-mail or fax because paper mail in the Washington, DC area and at the Board may be subject to delay.

You may submit comments, identified by Docket No. R-1550 and RIN 7100-AE-61 by any of the following methods:

- **Agency Web Site:** http://www.federalreserve.gov. Follow the instructions for submitting comments at http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm.
- **Federal eRulemaking Portal:** http://www.regulations.gov. Follow the instructions for submitting comments.
- **E-mail:** regs.comments@federalreserve.gov. Include docket and RIN numbers in the subject line of the message.
- **FAX:** (202) 452-3819 or (202) 452-3102.

**Mail:** Robert deV. Frierson, Secretary, Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue NW., Washington, DC 20551.

All public comments will be made available on the Board's Web site at http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm as submitted, unless modified for technical reasons. Accordingly, your comments will not be edited to remove any identifying or contact information. Public comments may also be viewed electronically or in paper form in Room 3515, 1801 K Street, NW. (between 18th and 19th Streets NW.), Washington, DC 20006 between 9:00 a.m. and 5:00 p.m. on weekdays. For security reasons, the Board requires that visitors make an appointment to inspect comments. You may do so by calling (202) 452-3684. Upon arrival, visitors will be required to present valid government-issued photo identification and to submit to security screening in order to inspect and photocopy comments.

OCC: Because paper mail in the Washington, DC area and at the OCC is subject to delay, commenters are encouraged to submit comments through the Federal eRulemaking Portal or e-mail, if possible. Please use the title "Enhanced Cyber Risk Management Standards" to facilitate the organization and distribution of the comments. You may submit comments by any of the following methods:

- **Federal eRulemaking Portal—"Regulations.gov":** Go to *www.regulations.gov*. Enter "Docket ID OCC-2016-0016" in the Search Box and click "Search." Click on "Comment Now" to submit public comments.
- Click on the "Help" tab on the Regulations.gov home page to get information on using Regulations.gov, including instructions for submitting public comments.
- **E-mail:** *regs.comments@occ.treas.gov*.
- **Mail:** Legislative and Regulatory Activities Division, Office of the Comptroller of the Currency, 400 7th Street, SW., suite 3E-218, mail stop 9W-11, Washington, DC 20219.

- **Hand Delivery/Courier:** 400 7th Street, SW., suite 3E-218, mail stop 9W-11, Washington, DC 20219.

- **Fax:** (571) 465-4326.

*Instructions*: You must include "OCC" as the agency name and "Docket ID OCC-2016-0016" in your comment. In general, OCC will enter all comments received into the docket and publish them on the Regulations.gov website without change, including any business or personal information that you provide such as name and address information, e-mail addresses, or phone numbers. Comments received, including attachments and other supporting materials, are part of the public record and subject to public disclosure. Do not enclose any information in your comment or supporting materials that you consider confidential or inappropriate for public disclosure.

You may review comments and other related materials that pertain to this rulemaking action by any of the following methods:

- **Viewing Comments Electronically:** Go to *www.regulations.gov.* Enter "Docket ID OCC-2016-0016" in the Search box and click "Search." Click on "Open Docket Folder" on the right side of the screen and then "Comments." Comments can be filtered by clicking on "View All" and then using the filtering tools on the left side of the screen.
- Click on the "Help" tab on the Regulations.gov home page to get information on using Regulations.gov. Supporting materials may be viewed by clicking on "Open Docket Folder" and then clicking on "Supporting Documents." The docket may be viewed after the close of the comment period in the same manner as during the comment period.

- **Viewing Comments Personally:** You may personally inspect and photocopy comments at the OCC, 400 7th Street, SW., Washington, DC 20219. For security reasons, the OCC requires that visitors make an appointment to inspect comments. You may do so by calling (202) 649-6700 or, for persons who are deaf or hard of hearing, TTY, (202) 649-5597. Upon arrival, visitors will be required to present valid government-issued photo identification and to submit to security screening in order to inspect and photocopy comments.

FDIC: You may submit comments, identified by RIN 3064-AE45, by any of the following methods:

**Agency Website:** http://www.fdic.gov/regulations/laws/federal/propose.html.

Follow instructions for submitting comments on the Agency website.

- **E-mail:** Comments@fdic.gov. Include the RIN 3064-AE45 on the subject line of the message.
- **Mail:** Robert E. Feldman, Executive Secretary, Attention: Comments, Federal Deposit Insurance Corporation, 550 17th Street, NW, Washington, DC 20429.
- **Hand Delivery:** Comments may be hand delivered to the guard station at the rear of the 550 17th Street Building (located on F Street) on business days between 7:00 a.m. and 5:00 p.m.

**Public Inspection:** All comments received must include the agency name and RIN 3064-AE45 for this rulemaking. All comments received will be posted without change to http://www.fdic.gov/regulations/laws/federal/propose.html, including any personal information provided. Paper copies of public comments may be ordered from the FDIC Public Information

Center, 3501 North Fairfax Drive, Room E-1002, Arlington, VA 22226 by telephone at (877) 275-3342 or (703) 562-2200.

**FOR FURTHER INFORMATION CONTACT:**

Board: Anna Lee Hewko, Associate Director, (202) 530-6260; or Matthew Hayduk, Manager, (202) 973-6190; or Julia Philipp, Senior Supervisory Financial Analyst, (202) 452-3940; or Christopher Olson, Senior Supervisory Financial Analyst, (202) 912-4609, Division of Banking Supervision and Regulation; or Benjamin W. McDonough, Special Counsel, (202) 452-2036; or Claudia Von Pervieux, Counsel, (202) 452-2552; or Michelle Kidd, Counsel, (202) 736-5554, Legal Division; for persons who are deaf or hard of hearing, TTY (202) 263-4869.

OCC: Bethany Dugan, Deputy Comptroller for Operational Risk, (202) 649-6949; or Kevin Greenfield, Director, Bank Information Technology, (202) 649-6954; or Eric Gott, Risk Team Lead for Governance and Operational Risk, Large Bank Supervision, (202) 649-7181; or Patrick Kelly, Bank Examiner, Critical Infrastructure Protection, (202) 649-5519; or Carl Kaminski, Special Counsel, Beth Knickerbocker, Counsel, or Rima Kundnani, Attorney, Legislative and Regulatory Activities Division, (202) 649-5490, Office of the Comptroller of the Currency, 400 7th Street SW., Washington, DC 20219.

FDIC: Donald Saxinger, Senior Examination Specialist, IT Supervision Branch, Division of Risk Management Supervision, (703) 254-0214; or John Dorsey, Counsel, (202) 898-3807. Supervision & Legislation Branch, Legal Division.

***I. Background***

With advances in financial technology, financial institutions and consumers alike have become increasingly dependent on technology to facilitate financial transactions. In addition, the

largest, most complex financial institutions rely heavily on technology to engage in national and international banking activities and to provide critical services to the financial sector and the U.S. economy.

As technology dependence in the financial sector continues to grow, so do opportunities for high-impact technology failures and cyber-attacks. Due to the interconnectedness of the U.S. financial system, 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. For example, 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. Nonbank financial companies that the Financial Stability Oversight Council (FSOC) has determined should be supervised by the Board (referred to in the ANPR as nonbank financial companies) 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 United States. Third parties that provide payments processing, core banking, and other financial technology services to these participants in the financial sector also provide services that are vital to the financial sector.

The Board, the OCC, and the FDIC have incorporated information security into their supervisory review of information technology (IT) programs at supervised banking organizations for many years. The agencies also review the services of third-party service providers that support those entities, and the Board includes information security as part of the supervisory program for nonbank financial companies and FMIs.

In response to expanding cyber risks, the agencies are considering establishing enhanced standards for the largest and most interconnected entities under their supervision, as well as for services that these entities receive from third parties. The term "covered entities" is used throughout this document to refer to entities potentially covered by the standards described in this ANPR. The enhanced standards would be designed to increase covered entities' operational resilience and reduce the potential impact on the financial system in the event of a failure, cyber-attack, or the failure to implement appropriate cyber risk management.

The agencies are considering implementing the enhanced standards in a tiered manner, imposing more stringent standards on the systems of covered entities that are critical to the functioning of the financial sector, referred to in this ANPR as "sector-critical systems."

The agencies are seeking comment on all aspects of the enhanced standards described in this ANPR. The agencies plan to use information collected in this ANPR to develop a more detailed proposal for consideration. The agencies will again invite public comment on a detailed proposal before adopting any final rule.

## *II. Relationship to Existing Requirements and Guidance*

### *a. Existing Supervisory Programs*

As noted, the agencies have existing supervisory programs that contain general expectations for cybersecurity practices at financial institutions and third-party service providers. The enhanced standards would be integrated into the existing supervisory framework by establishing enhanced supervisory expectations for the entities and services that potentially pose heightened cyber risk to the safety and soundness of the financial sector.

Through the Federal Financial Institutions Examination Council (FFIEC), the agencies issued the Uniform Rating System for Information Technology (URSIT) in 1978 (revised

January 20, 1999).[1] The URSIT rating is used by federal and state regulators to uniformly assess IT risks at financial institutions, their affiliates, and service providers[2] for the purpose of identifying those institutions that require special supervisory attention. The URSIT framework includes elements to assess data security and other risk management factors necessary to determine the quality, integrity, and reliability of the financial institution's or third-party service provider's IT. The proposed enhanced standards would not replace the URSIT ratings but could be used, in part, to inform the cyber-related elements of the URSIT rating for covered entities. For example, supervisory work related to the proposed external dependency management standard discussed in this ANPR could be used, in part, to inform the development and acquisition component of the URSIT rating.

In 2003, the FFIEC published the first in a series of booklets on IT that make up the IT Handbook. The IT Handbook provides guidance to examiners in reviewing financial institutions and services provided by third parties. Certain booklets, such as the Business Continuity Planning booklet and the Information Security booklet, incorporate the agencies' expectations regarding cybersecurity risk management. The IT Handbook also includes work programs that an examiner may use to aid in assessing a company's URSIT rating. IT Handbook guidance would continue to be used for covered entities to assess IT risk management.

In 1999, Title V, Subtitle A of the Gramm-Leach-Bliley Act (GLBA)[3] required that each agency establish appropriate administrative, technical, and physical controls for the safeguarding of financial institutions' customer information. In 2000, the agencies published the *Interagency*

[1] 64 FR 3109, January 20, 1999.
[2] The agencies have statutory authority to supervise and examine services provided by third-party service providers to regulated financial institutions under the Bank Service Company Act (12 U.S.C. § 1867(c)).
[3] 15 U.S.C. §§ 6801-6809.

*Guidelines Establishing Information Security Standards* (Guidelines) implementing the GLBA safeguarding requirements.[4] The Guidelines require insured depository institutions to implement information security programs to ensure the security and confidentiality of customer information; protect against any anticipated threats or hazards to the security or integrity of such information; protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and ensure the proper disposal of customer and consumer information.

Additionally, the agencies have interagency guidelines that establish safety and soundness standards, including operational and managerial standards, for depository institutions.[5] These guidelines require an insured depository institution to have internal controls and information systems appropriate to the size of the institution and to the nature, scope, and risk of its activities and that provide for, among other requirements, effective risk assessment and adequate procedures to safeguard and manage assets. Insured depository institutions are also required to have internal audit systems based on the same criteria that provide for adequate testing and review of information systems. The Guidelines and safety and soundness standards would continue to apply to covered entities that are insured depository institutions.

***b. FFIEC Cybersecurity Assessment Tool***

In June 2015, the FFIEC issued the Cybersecurity Assessment Tool (Assessment) as a voluntary self-assessment tool that financial institutions, including covered entities, may use to help assess their cyber risks and determine their cybersecurity preparedness.

[4] *See* 12 CFR part 208, App. D-2 and 12 CFR part 225, App. F (Board); 12 CFR 30, App. B (OCC); and 12 CFR part 364, App. B and 12 CFR part 391, subpart B, App. B (FDIC).
[5] *See* 12 CFR part 30, App. A and D, 12 CFR part 208, App. D-1, 12 CFR part 225, App. F.

The Assessment provides institutions with a repeatable and measurable process to determine whether the institutions have appropriate controls and risk management in place relative to the inherent risk profile of the institution. The Assessment incorporates baseline cybersecurity-related categories from the FFIEC IT Handbook, as well as key concepts from the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and other industry best practices. However, the Assessment does not establish binding minimum standards.

***c. NIST Cybersecurity Framework***

The NIST CSF is a voluntary framework for organizations to better understand, manage, and reduce their cybersecurity risk. The CSF is intended to be customized by different business sectors and individual organizations to best suit their risks, situation, and needs. It was also designed to improve communications, awareness, and understanding among IT, planning and operating units, and senior executives, to better address cyber risks. The NIST CSF Core consists of five concurrent and continuous functions: *Identify, Protect, Detect, Respond, and Recover*. Taken together, these functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk.

Similar to the NIST CSF, the enhanced standards would provide a clear set of objectives for sound cyber risk management. However, the binding requirements set forth in the enhanced standards would be designed specifically to address the cyber risks of the largest, most interconnected U.S. financial entities.

***d. CPMI-IOSCO Guidance***

In June 2016, the Committee on Payments and Market Infrastructures (CPMI) and the Board of the International Organization of Securities Commissions (IOSCO) released "Guidance

on cyber resilience for financial market infrastructures."[6] According to CPMI and IOSCO, the guidance "aims to add momentum to and instill international consistency in the industry's ongoing efforts to enhance FMIs' ability to preempt cyber-attacks, respond rapidly and effectively to them, and achieve faster and safer target recovery objectives if they succeed."[7] The guidance is intended to supplement the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) and is "not intended to impose additional standards on FMIs beyond those set out in the PFMI, but provides detail related to the preparations and measures that FMIs should undertake to enhance their cyber resilience capabilities with the objective of limiting the escalating risks that cyber threats pose to financial stability."[8] The agencies reviewed the CPMI-IOSCO guidance and took it into consideration as they developed the proposed enhanced standards described in this ANPR.

***e. Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System***

In April 2003, the Board, the OCC, and the Securities and Exchange Commission issued the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* (Sound Practices Paper).[9] The Sound Practices Paper focuses on minimizing the immediate systemic effects of a wide-scale disruption on critical financial markets and on establishing the appropriate back-up capacity for recovery and resumption of clearance and settlement activities in wholesale financial markets. As discussed in sections IV and VI, the

[6] *See* http://www.bis.org/cpmi/publ/d146.pdf.
[7] *See* http://www.bis.org/cpmi/publ/d146.htm.
[8] *See* http://www.bis.org/cpmi/publ/d146.pdf.
[9] Available at: http://www.sec.gov/news/studies/34-47638.htm.

agencies took the Sound Practices Paper into consideration as they developed the proposed enhanced standards described in this ANPR.

### *III. Scope of Application*

The agencies are considering applying the enhanced standards to certain entities with total consolidated assets of $50 billion or more on an enterprise-wide basis. A cyber-attack or disruption at one or more of these entities could have a significant impact on the safety and soundness of the entity, other financial entities, and the U.S. financial sector. The agencies are considering applying the enhanced standards to these entities on an enterprise-wide basis because cyber risks in one part of an organization could expose other parts of the organization to harm.

Each agency would apply these standards to large institutions subject to their jurisdiction.[10] Thus, the Board is considering applying the enhanced standards on an enterprise-wide basis to all U.S. bank holding companies with total consolidated assets of $50 billion or more, the U.S. operations of foreign banking organizations with total U.S. assets of $50 billion or more, and all U.S. savings and loan holding companies with total consolidated assets of $50 billion or more.[11] In this regard, the proposed standards would apply to subsidiaries of depository institution holding companies (other than depository institutions supervised by the OCC and FDIC) in view of the subsidiaries' potential to act as points of cyber vulnerability to the covered entities. The Board is also considering applying the standards to nonbank financial companies supervised by the Board pursuant to section 165 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), which directs the Board to establish enhanced prudential standards, including overall risk management standards, for these entities.[12]

---

[10] 12 U.S.C. §§ 321, 1818, 1831p-1 (Board); 12 U.S.C. §§ 1, 93a, 161, 481, 1463, 1464, 1818, 1831p-1, 3901, 3909 (OCC); 12 U.S.C. §§ 1818, 1819, 1831p-1 (FDIC).

[11] 12 U.S.C. §§ 1467a(g), 5365.

[12] 12 U.S.C. § 5365.

Similarly, the Board is considering applying the standards to financial market utilities designated by FSOC (designated FMUs) for which the Board is the Supervisory Agency pursuant to sections 805 and 810 of the Dodd-Frank Act; other FMIs over which the Board has primary (not backup) supervisory authority because the FMIs are members of the Federal Reserve System; and FMIs that are operated by the Federal Reserve Banks (collectively referred to as "Board-supervised FMIs").[13]

The OCC is considering applying the standards to any national bank, federal savings association (and any subsidiaries thereof), or federal branch of a foreign bank that is a subsidiary of a bank holding company or savings and loan holding company with total consolidated assets of $50 billion or more, or any national bank, federal savings association, or federal branch of a foreign bank that has total consolidated assets of $50 billion or more that does not have a parent holding company. The Board is considering applying the standards to any state member bank (and any subsidiaries thereof) that is a subsidiary of a bank holding company with total consolidated assets of $50 billion or more, and to any state member bank that has total consolidated assets of $50 billion or more that is not a subsidiary of a bank holding company. The FDIC is considering applying the standards to any state nonmember bank or state savings association (and any subsidiaries thereof) that is a subsidiary of a bank holding company or savings and loan holding company with total consolidated assets of $50 billion or more. Additionally, the FDIC is considering applying the standards to any state nonmember bank or state savings association that has total consolidated assets of $50 billion or more that does not have a parent holding company.

As noted, the agencies are considering whether to apply the standards to third-party

[13] 12 U.S.C. §§ 5464(a), 5469; 12 U.S.C. §§ 330, 1818, 1831a; 12 U.S.C. § 248(j).

service providers with respect to services provided to depository institutions and their affiliates that are covered entities (covered services). This would ensure consistent, direct application of the standards regardless of whether a depository institution or its affiliate conducted the operation itself, or whether it engaged a third-party service provider to conduct the operation. Direct application of the standards to these service providers could have potential benefits, including facilitating supervisory action in the event that a covered service was not meeting a proposed standard and establishing an obligation for meeting the standard on the depository institution or its affiliate, as well as on the third-party provider of the covered service. The Board also is considering requiring nonbank financial companies and Board-supervised FMIs to verify that any services the nonbank financial company or Board-supervised FMI receives from third parties are subject to the same standards that would apply if the services were being conducted by the nonbank financial company or Board-supervised FMI itself.

Other financial entities, including community banks that are not covered entities, would continue to be subject to existing guidance, standards, and examinations related to the provision of banking services by third parties.

Questions on the Scope of Application

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?*

2. *What are the costs and benefits of applying the standards to covered entities on an enterprise-wide basis? If the agencies were to consider exempting certain subsidiaries within a covered entity from the standards, what criteria should be used to assess any such exemptions? What safeguards should the agencies require from a subsidiary seeking to be exempted from the standards to ensure that an exempted subsidiary does not expose the covered entity to material cyber risk?*
3. *What, if any, special considerations should be made regarding application of the standards to savings and loan holding companies that engage significantly in insurance or commercial activities?*
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?*
5. *What are the advantages and disadvantages of applying the standards directly to service providers to covered entities? What challenges would such an approach pose?*
6. *What factors are most important in determining an appropriate balance between protecting the safety and soundness of the financial sector through the possible*

*application of the standards and the implementation burden and costs associated with implementing the standards?*

## *IV. Sector-Critical Systems*

The financial sector operates through a network of interrelated markets and financial participants. As a result, a technology failure or cyber-attack at one covered entity could have wide-ranging effects on the safety and soundness of other financial entities, both within and outside the United States. While this interconnectedness warrants comprehensive cyber risk management by all financial market participants, it is especially important in the case of covered entities with sector-critical systems.

Thus, the agencies are considering establishing a two-tiered approach, with the enhanced standards applying to all systems of covered entities, and an additional, higher set of expectations, referred to in the ANPR as "sector-critical standards," applying to those systems of covered entities that are critical to the financial sector.

As discussed below in the ANPR, the agencies are proposing sector-critical standards in four of the five categories of standards that would require covered entities with sector-critical systems to substantially mitigate the risk of a disruption due to a cyber event to their sector-critical systems.

Previously in the Sound Practices Paper, the Board and the OCC, together with the Securities and Exchange Commission, introduced definitions of "critical financial markets" and "firms that play significant roles in critical financial markets," which emphasized the need to protect the most critical elements of the financial system from serious new risks posed in the post-September 11 environment. In the Sound Practices Paper, "critical financial markets" are defined as the markets for federal funds, foreign exchange, and commercial paper; U.S.

Government and agency securities; and corporate debt and equity securities. The Sound Practices Paper further provides: "firms that play significant roles in critical financial markets are those that participate (on behalf of themselves or their customers) with sufficient market share in one or more critical financial markets such that their failure to settle their own or their customers' material pending transactions by the end of the business day could present systemic risk. While there are different ways to gauge the 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."

While the scope of the Sound Practices Paper was limited to the resumption of clearance and settlement activities in wholesale financial markets, the definitions presented in the Sound Practices Paper provide a starting point for identifying systems (that is, sector-critical systems) that should be subject to the more stringent, sector-critical standards. Thus, consistent with the Sound Practices Paper, the agencies are considering whether 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, should be considered sector-critical systems for the purpose of the sector-critical standards. The agencies also are considering whether 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, should be considered sector-critical systems.

Because a cyber event may impact the safety and soundness of multiple financial participants and create systemic risk beyond these specific markets, the agencies are considering additional factors to identify sector-critical systems, such as substitutability and interconnectedness. Systems that provide key functionality to the financial sector for which alternatives are limited or nonexistent, or would take excessive time to implement (for example, due to incompatibility) also could have a material impact on financial stability if significantly disrupted. Systems that act as key nodes to the financial sector due to their extensive interconnectedness to other financial entities could have a material impact on financial stability if significantly disrupted.

Consistent with the approach to other services, any services provided by third parties that support a covered entity's sector-critical systems would be subject to the same sector-critical standards.

Questions on Sector-critical Systems

7. *Do covered entities currently have access to sufficient information to determine whether any of their systems would be considered sector-critical systems for the purpose of the standards? If not, what additional information would be necessary for an entity to identify whether it has one or more sector-critical systems for the purposes of the standards?*
8. *What are the advantages and disadvantages of requiring covered entities to identify and report to the agencies their systems that support operations and meet the applicable thresholds to be considered sector-critical systems? Alternatively, what are the advantages and disadvantages of having the agencies develop a process to identify the systems of covered entities that support operations and meet the applicable thresholds to*

*be considered sector-critical systems and to notify covered entities which of their systems would be subject to the sector-critical standards?*

9. *What thresholds for transaction value in one or more critical financial markets should the agencies consider for identifying sector-critical systems? Similarly, what, if any, additional thresholds should the agencies consider for identifying sector-critical systems that could have a material impact on financial stability if disrupted? For example, how should the agencies identify systems that provide functionality to the financial sector and for which alternatives are limited, nonexistent, or would take excessive time to implement? How should such factors be weighted? Commenters are encouraged to provide quantitative as well as qualitative support and analysis for proposed alternative methodologies, thresholds and/or factors.*
10. *What are the advantages and disadvantages of determining that a covered entity which holds a substantial amount of U.S. deposits and/or balances due from other depository institutions in the United States plays a significant role in a critical financial market? At what level of activity should a covered entity's systems related to holding U.S. deposits and/or balances due from other depository institutions in the United States be determined to be critical to the sector?*
11. *What factors should the agencies consider in a measure of interconnectedness resulting in a system being determined as critical to the financial sector, and how should such factors be weighted? Commenters are asked to provide quantitative as well as qualitative support and analysis for proposed alternative methodologies, thresholds and/or factors.*

*12. In some cases, entities, such as smaller banking organizations, may provide services considered sector-critical services either directly to the financial sector or through covered entities. What criteria should the agencies use to evaluate whether a financial entity that would not otherwise be subject to the enhanced standards should be subject to the sector-critical standards? How should the agencies weigh the costs of imposing the sector-critical standards to such smaller banking organizations against the potential benefits to the financial system?*

## *V. Enhanced Cyber Risk Management Standards*

As noted, the agencies are considering enhanced cyber risk management standards for covered entities to increase the entities' operational resilience and reduce the potential impact on the financial system as a result of, for example, a cyber-attack at a firm or the failure to implement appropriate cyber risk management.

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;[14] 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. The agencies are considering establishing a two-tiered approach, with the proposed enhanced standards applying to all systems of covered entities and an additional, higher

[14] With regard to providers of services, depending on the size and structure of the organization and the relative size of the unit providing services to a depository institution, its subsidiaries or affiliates, it may be appropriate for some functions to be performed by business line executive management instead of the board of directors or a board committee of the organization. For these firms, "enterprise-wide," for purposes of the ANPR, encompasses the governance processes, policies, procedures, and controls related to or impacting the performance of services by a third party for a depository institution, its subsidiaries, or affiliates.

set of expectations, or "sector-critical standards," applying to those systems of covered entities that are critical to the financial sector. The "sector-critical standards" would require covered entities to substantially mitigate the risk of a disruption due to a cyber event to their sector-critical systems.

As noted, the standards would be organized into five categories:

*Category 1: Cyber risk governance;*

*Category 2: Cyber risk management;*

*Category 3: Internal dependency management;*

*Category 4: External dependency management; and*

*Category 5: Incident response, cyber resilience, and situational awareness.*

The term "internal dependency" in this ANPR 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. The term "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.

The categories are organized in this order to emphasize the core *cyber risk governance* and *cyber risk management* standards the agencies would expect a covered entity to develop to establish a foundation for making informed risk-based decisions in support of its business objectives. Standards in the *internal dependency management*, *external dependency*

*management*, and *incident response, cyber resilience, and situational awareness* categories are designed to work together and to be mutually reinforcing.

In the discussion of the individual enhanced standards that follows, a reference to application of the enhanced standards to covered entities is intended to include application of the enhanced standards to services provided to the covered entities, unless otherwise specified. The proposed standards for covered entities are described first; additional proposed standards for sector-critical systems then are listed separately.

*Category 1 – Cyber Risk Governance*

A key aspect of *cyber risk governance* is developing and maintaining a formal cyber risk management strategy, as well as a supporting framework of policies and procedures to implement the strategy, that is integrated into the overall strategic plans and risk governance structures of covered entities. Therefore, the agencies are considering standards under the *cyber risk governance* category that would be similar to the governance standards generally expected for large, complex financial organizations.[15] For example, the standards would provide that the

[15] For OCC-regulated covered entities, see 12 CFR part 30 Appendix D. An OCC-regulated covered entity would be expected to incorporate its cyber risk management strategy and framework into its overall risk management framework required pursuant to the "OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches" set forth at 12 CFR part 30 Appendix D. These OCC guidelines establish minimum standards for the design and implementation of a risk governance framework for large insured national banks, insured federal savings associations, and insured federal branches of foreign banks. Among other items, the OCC guidelines state that the board of directors of a covered bank should require management to establish and implement an effective framework that complies with the guidelines and approve any significant changes to the framework; the board should actively oversee a covered bank's risk-taking activities and hold management accountable for adhering to the framework; and each covered bank should have a comprehensive written statement that articulates the bank's risk appetite and serves as a basis for the framework (i.e., a risk appetite statement). The OCC guidelines set forth roles and responsibilities for front line units, independent risk management, and internal audit. A Board-regulated covered entity would be expected to incorporate its cyber risk management strategy and framework into its overall corporate strategy and the institutional risk appetite maintained by the entity's board of directors. *See* SR letter 12-17, "Consolidated Supervision Framework for Large Financial Institutions," which outlines the general supervisory expectation that large bank holding companies and nonbank financial companies maintain a clearly articulated corporate strategy and institutional risk appetite; *see also* 12 CFR part 252, subparts D and O, which establishes risk management requirements for certain large bank holding companies and nonbank financial companies.

board of directors, or an appropriate board committee,[16] 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.

Specifically, the agencies are considering, as an enhanced standard in this category, a requirement that covered entities 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.[17] The strategy would articulate how the entity intends to address its inherent cyber risk (that is, its cyber risk before mitigating controls or other factors are taken into consideration) and how the entity would maintain an acceptable level of residual cyber risk (that is, its remaining cyber risk after mitigating controls and other factors have been taken into consideration) and maintain resilience on an ongoing basis.

A covered entity also would be required to 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. Thus, as part of the enhanced standard in this category, the agencies are considering requiring the entity's board of directors to review and approve the enterprise-wide cyber risk appetite and tolerances of the covered entity. The enhanced standard also would provide that a covered entity must reduce its residual cyber risk to the appropriate level approved by the board of directors.

Covered entities would need to be able to identify and assess those activities and exposures that present cyber risk, then determine ways to aggregate them to assess the entity's

[16] In the discussion of the enhanced standards that follows, a reference to the board of directors is intended to include the board of directors or an appropriate board committee.

[17] For Board-regulated covered entities, this would be part of the larger global risk management framework that is required by 12 CFR 252.33.

residual cyber risk. This is important because cyber risk has the potential to produce losses large enough to threaten an entity's financial health, its reputation, or its ability to maintain core operations if faced with a material cyber event.

The board of directors of a covered entity would oversee and hold senior management accountable for implementing the entity's cyber risk management framework. In this regard, the agencies are considering requiring the board of directors to have adequate expertise in cybersecurity or to maintain access to resources or staff with such expertise. Consistent with existing agency expectations, the enhanced standards would require the board of directors to have and maintain the ability to provide credible challenge to management in matters related to cybersecurity and the evaluation of cyber risks and resilience.

The agencies also are considering requiring senior leaders with responsibility for cyber risk oversight to be independent of business line management. In this regard, these senior leaders would need to have direct, independent access to the board of directors and would independently inform the board of directors on an ongoing basis of the firm's cyber risk exposure and risk management practices, including known and emerging issues and trends.

A covered entity would be required 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. The entity would be required to include in its framework delineated cyber risk management and oversight responsibilities for the organization, including reporting structures and expectations for independent risk management, internal control, and internal audit personnel; established mechanisms for evaluating whether the organization has sufficient resources to address the cyber risks facing the organization; and established policies for addressing any resource shortfalls or knowledge gaps. The entity also

would be required to include in its cyber risk management framework mechanisms for identifying and responding to cyber incidents and threats, as well as procedures for testing the effectiveness of the entity's cybersecurity protocols and updating them as the threat landscape evolves.

Questions on Cyber Risk Governance

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?*

*Category 2 – Cyber Risk Management*

In general, the enhanced standards would require covered entities, to the greatest extent possible and consistent with their organizational structure, to integrate cyber risk management into the responsibilities of at least three independent functions (such as the three lines of defense risk-management model) with appropriate checks and balances. This would allow covered entities to more accurately and effectively identify, monitor, measure, manage, and report on cyber risk.

Business Units

The agencies are considering requiring units responsible for the day-to-day business functions of a covered entity to assess, on an ongoing basis, the cyber risks associated with the activities of the business unit. Business units also would need to ensure that information regarding those risks is shared with senior management, including the chief executive officer (CEO), as appropriate, in a timely manner so that senior management can address and respond to emerging cyber risks and cyber incidents as they develop.

As part of this proposed enhanced standard, business units would be required to adhere to procedures and processes necessary to comply with the covered entity's cyber risk management framework. Such procedures and processes would be designed to ensure that the applicable business unit's cyber risk is effectively identified, measured, monitored, and controlled, consistent with the covered entity's risk appetite and tolerances. Business units would assess 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. To this end, the covered entity would be expected to ensure that business units maintain, or have access to, resources and staff with the skill sets needed to comply with the unit's cybersecurity responsibilities.

Independent Risk Management

The agencies are considering a requirement that covered entities incorporate enterprise-wide cyber risk management into the responsibilities of an independent risk management function. This function would report to the covered entity's chief risk officer and board of directors, as appropriate, regarding implementation of the firm's cyber risk management

framework throughout the organization. Independent risk management would be required to 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. Additionally, independent risk management would be continually required to 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 of any instances when a unit of the covered entity has exceeded the entity's established cyber risk tolerances.

On a continuous basis, independent risk management would be required to identify, measure, and monitor cyber risk across the enterprise, and to determine whether cyber risk controls are appropriately in place across the enterprise consistent with the entity's established risk appetite and tolerances. On an ongoing basis, the independent risk management function would be required to identify and assess the covered entity's material aggregate risks 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.

Additionally, the agencies are considering requiring covered entities to assess the completeness, effectiveness, and timeliness with which they reduce the aggregate residual cyber risk of their systems to the appropriate, board-of-directors approved level. The Board is considering requiring covered entities, at the holding company level, to measure (quantitatively) the completeness, effectiveness, and timeliness with which they reduce the aggregate residual cyber risk of their systems to the appropriate, board-of-directors approved level. As noted, this is important because cyber risk has the potential to produce losses large enough to threaten an

entity's financial health, its reputation, or its ability to maintain core operations if faced with a material cyber event.

Therefore, the independent risk management function would be required to establish and maintain an up-to-date understanding of the structure of a covered entity's cybersecurity programs and supporting processes and systems, as well as their relationships to the evolving cyber threat landscape.

To satisfy these requirements, it is essential that a covered entity's independent risk management function have and maintain sufficient independence, stature, authority, resources, and access to the board of directors to ensure that the operations of the entity are consistent with the cyber risk management framework. The reporting lines must be clear and separate from those for other operations and business units.

Audit Function

Audit evaluates the effectiveness of risk management, internal controls, and governance processes, among other things, and advises management and the board of directors on whether a covered entity's policies and procedures are adequate to keep up with emerging risks and industry regulations. As such, audit plays an important role in risk management, internal control, and corporate governance.

Consistent with a strong overall governance process, the agencies consider cyber risk and cyber risk management as important to the internal audit function at covered entities. Therefore, the agencies are considering explicitly requiring the audit function to 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.

Further, as part of this enhanced standard, audit would be required to incorporate an assessment of cyber risk management into the overall audit plan of the covered entity. The plan would be required to provide for 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. Such an evaluation would be required to include the entire security lifecycle, including penetration testing and other vulnerability assessment activities as appropriate based on the size, complexity, scope of operations, and interconnectedness of the covered entity. The audit plan would be required to provide for an assessment of the business unit and independent risk management functions' capabilities to adapt as appropriate and remain in compliance with the covered entity's cyber risk management framework and within its stated risk appetite and tolerances.

Questions on Cyber Risk Management

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?*
16. *The agencies seek comment on requiring covered entities to organize themselves in a manner that is consistent with the contemplated enhanced standards for cyber risk management. Besides the approach outlined in the ANPR, what other approaches could ensure that entities are effectively identifying, monitoring, measuring, managing, and reporting on cyber risk?*

*Category 3 – Internal Dependency Management*

Standards within the *internal dependency management* category are intended to ensure that covered entities have effective capabilities in place to identify and manage cyber risks associated with their business assets (that is, their workforce, data, technology, and facilities) throughout their lifespans. These risks may arise from a wide range of sources, including insider threats, data transmission errors, or the use of legacy systems acquired through a merger.

A key aspect of the *internal dependency management* category is ensuring that covered entities continually assess and improve, as necessary, their effectiveness in reducing the cyber risks associated with internal dependencies on an enterprise-wide basis. As part of the overall cyber risk management strategy, as discussed in the c*yber risk governance* section of this ANPR, the agencies are considering a requirement that a covered entity integrate an internal dependency management strategy into the entity's overall strategic risk management plan. The strategy would guide and inform measures taken to reduce cyber risks associated with a covered entity's internal dependencies. The internal dependency management strategy would be designed to ensure that: roles and responsibilities for internal dependency management are well defined; policies, standards, and procedures to identify and manage cyber risks associated with internal assets, including those connected to or supporting sector-critical systems, are established and regularly updated throughout those assets' lifespans; appropriate oversight is in place to monitor effectiveness in reducing cyber risks associated with internal dependencies; and appropriate compliance mechanisms are in place.

Another key aspect of the *internal dependency management* category is having current and complete awareness of all internal assets and business functions that support a firm's cyber risk management strategy. The agencies are considering a requirement that covered entities

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. Thus, covered entities would be required to maintain a current and complete listing of all internal assets and business functions, including mappings to other assets and other business functions, information flows, and interconnections. Covered entities would 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. This would contribute to establishing and implementing mechanisms to prioritize monitoring, incident response, and recovery of systems critical to the entity and to the financial sector. A covered entity's tracking capability would need to enable timely notification of internal cyber risk management issues to designated internal stakeholders. In addition, covered entities would support the reduction of the cyber risk exposure of business assets to the enterprise and the sector until the board-approved risk appetite and tolerances are achieved; and support timely responses to cyber threats to, and vulnerabilities of, the enterprise and the financial sector.

Another key aspect within the *internal dependency management* category is establishing and applying appropriate controls to address the inherent cyber risk of a covered entity's assets. The agencies are considering a requirement that covered entities 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) by:

- assessing the cyber risk of assets and their operating environments prior to deployment;
- continually applying controls and monitoring assets and their operating environments (including deviations from baseline cybersecurity configurations) over the lifecycle of the assets; and

- 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.

As part of this enhanced standard, the agencies are considering requiring covered entities to continually apply appropriate controls to reduce the cyber risk of business assets to the enterprise and the financial sector to the board-approved level. The agencies are also considering a requirement that covered entities periodically conduct tests of back-ups to business assets to achieve resilience.

*Category 4 – External Dependency Management*

As noted, the term "external dependencies" refers to an entity's relationships with outside vendors, suppliers, customers, utilities, and other external organizations and service providers that the entity depends on to deliver services, as well as the information flows and interconnections between the entity and those external parties. In addition, the external dependency management category includes the management of interconnection risks associated with non-critical external parties that maintain trusted connections to important systems. Standards within the *external dependency management* category are intended to ensure that covered entities have effective capabilities in place to identify and manage cyber risks associated with their external dependencies and interconnection risks throughout these relationships.

A key aspect of the *external dependency management* category is ensuring that covered entities continually assess and improve, as necessary, their effectiveness in reducing the cyber risks associated with external dependencies and interconnection risks enterprise-wide. As part of the overall cyber risk management strategy, as discussed in the *cyber risk governance* section of this ANPR, the agencies are considering a requirement that a covered entity 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. This external dependency management strategy would ensure that roles and responsibilities for external dependency management are well defined; policies, standards, and procedures for external dependency management throughout the lifespan of the relationship (for example, due diligence, contracting and sub-contracting, onboarding, ongoing monitoring, change management, off boarding) are established and regularly updated; appropriate metrics are in place to measure effectiveness in reducing cyber risks associated with external dependencies; and appropriate compliance mechanisms are in place.

As part of an external dependency management strategy, the agencies are considering a requirement that covered entities 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.

Another key aspect of the *external dependency management* category is having the ability to monitor in real time all external dependencies and trusted connections that support a covered entity's cyber risk management strategy. The agencies are considering a requirement that covered entities 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. Thus, covered entities would be able to generate and maintain a current, accurate, and complete listing of all external dependencies and business functions, including mappings to supported assets and business functions. Covered entities would be required to 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. A covered entity's tracking capability would enable timely notification of cyber risk management issues to designated stakeholders.

Another key aspect within the *external dependency management* category is establishing and applying appropriate controls to address the cyber risk presented by each external partner throughout the lifespan of the relationship. The agencies are considering a requirement that covered entities 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. As part of this requirement and in order to address the rapidly changing and complex threat landscape, the agencies are considering a requirement that covered entities continually apply and evaluate appropriate controls to reduce the cyber risk of external dependencies to the enterprise and the sector.

Questions on Internal and External Dependency Management

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.*

18. *What challenges and burdens would covered entities encounter in maintaining an internal and external dependency management strategy consistent with that described by the agencies?*
19. *How do the proposed internal and external dependency management standards compare with processes already in place at banking organizations?*
20. *What other approaches could the agencies use to evaluate a covered entity's internal and external dependency management strategies? Please be specific as to each approach.*
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? Please be specific.*

*Category 5 – Incident Response, Cyber Resilience, and Situational Awareness*

Standards within the *incident response, cyber resilience, and situational awareness* category would be designed to ensure that covered entities 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. 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. In addition, covered entities would be required to establish processes designed to maintain effective situational awareness capabilities to reliably predict, analyze, and respond to changes in the operating environment.

The agencies are considering a requirement that covered entities 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. The agencies are considering a requirement that covered entities 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. In addition, the agencies are considering a requirement that covered entities establish and maintain 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. These cyber resilience and incident response programs would be required to include effective escalation protocols linked to organizational decision levels, cyber contagion containment procedures, communication strategies, and processes to incorporate lessons learned back into the program. Cyber resilience strategies and exercises would be required to consider wide-scale recovery scenarios and be designed to achieve institutional resilience, support the achievement of financial sector-wide resilience, and minimize risks to or from interconnected parties.

The IT Handbook calls for examiners to determine whether covered entities have established plans to address recovery and resilience strategies for cyber-attacks that may disrupt access, corrupt data, or destroy data or systems.[18] In addition to establishing recovery time objectives (RTOs), recovery and resilience strategies should address the potential for malware or corrupted data to replicate or propagate through connected systems or high availability solutions. For cyber-attacks that may potentially corrupt or destroy critical data, recovery strategies should be designed to achieve recovery point objectives based on the criticality of the data necessary to keep the institution operational.

[18] FFIEC IT Examination Handbook, Business Continuity Planning, Appendix J.

In this category, the agencies also are considering a requirement that covered entities 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.

The preservation of critical records in the event of a large-scale or significant cyber event is essential to maintaining confidence in the banking system and to facilitating resolution or recovery processes after a catastrophic event. The agencies are therefore considering requiring covered entities to 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.

Transition plans are essential in the event a service is terminated or an entity cannot meet its obligations. Thus, the agencies are considering a requirement that covered entities establish 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 covered entity or service provider is unable to perform. As a result, if performance is not feasible and contractual termination/remediation provisions have been exercised, client data would be returned to the original covered entity or service provider in a method that is transferable to an alternate entity or service provider with minimal disruption to the operations of the covered entity.

Testing the cyber resilience of operations and services helps to identify potential threats to the ongoing performance of the operation or service. A prolonged disruption of a significant

operation could generate systemic risk. The agencies are considering a requirement that covered entities conduct specific testing that addresses disruptive, destructive, corruptive, or any other cyber event that could affect their ability to service clients; and significant downtime that would threaten the business resilience of clients. In addition, the agencies are considering a requirement that the testing address external interdependencies, such as connectivity to markets, payment systems, clearing entities, messaging services, and other critical service providers or partners; that the testing of cyber resilience be undertaken jointly where critical dependencies exist; and that the testing validate the effectiveness of internal and external communication protocols with stakeholders.

A key element of situational awareness is the timely identification, analysis, and tracking of data about the state of, and potential cyber risks to, the organization. The agencies are considering a requirement that covered entities maintain an ongoing situational awareness of their operational status and cybersecurity posture to pre-empt cyber events and respond rapidly to them. Covered entities also would be required to establish and maintain threat profiles[19] for identified threats to the firm; establish and maintain threat modeling[20] capabilities; gather actionable cyber threat intelligence and perform security analytics on an ongoing basis; and establish and maintain capabilities for ongoing vulnerability management.

Questions on Incident Response, Cyber Resilience, and Situational Awareness

*23. How well do the proposed standards for incident response, cyber resilience, and situational awareness address the safety and soundness of individual financial*

[19] Threat profiles include information about critical assets, threat actors, and details about how threat actors might attempt to compromise those critical assets.

[20] Threat modeling refers to using a structured process to identify how critical assets might be compromised by a threat actor and why, what level of protection is needed for those critical assets, and what the impact would be if that protection failed.

*institutions and potential systemic cyber risk to the financial sector, including with respect to the testing strategies and approaches? How could they be improved?*

24. *What is the extent to which it would be operationally and/or commercially feasible to comply with requirements to use certain defined data standards in order to increase the substitutability of third-party relationships to reduce recovery times for systems impacted by a significant cyber event?*
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?*
26. *How do covered entities currently evaluate their situational awareness capabilities? What factors should the agencies consider essential in considering a covered entity's situational awareness capabilities?*
27. *What other factors should be included within the incident response, cyber resilience, and situational awareness category?*
28. *What additional requirements should the agencies consider to improve the resilience or situational awareness of a covered entity or the ability of a covered entity to respond to a cyber-attack?*

### *VI. Standards for Sector-Critical Systems of Covered Entities*

As noted, the agencies are considering two tiers of standards, with more stringent standards to apply to systems of covered entities that are critical to the functioning of the financial sector.

In particular, the agencies are considering a requirement that covered entities minimize the residual cyber risk of sector-critical systems by implementing the most effective,

commercially available controls. Minimizing residual cyber risk means substantially mitigating the risk of a disruption or failure due to a cyber event.

As a second sector-critical standard, the agencies are considering requiring covered entities to establish an RTO of two hours for their sector-critical systems, validated by testing, to recover from a disruptive, corruptive, or destructive cyber event. Testing programs would include a range of scenarios, including severe but plausible scenarios, and would challenge matters such as communications protocols, governance arrangements, and resumption and recovery practices. As stated in the Sound Practices Paper, an RTO is the "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." The scope of application of this proposed sector-critical standard could go beyond the core clearing and settlement organizations discussed in the Sound Practices Paper to include other large, interconnected financial systems where a cyber-attack or disruption also could have a significant impact on the U.S. financial sector. With advances in technology and consistent with the two-hour RTO for core clearing and settlement activities in the Sound Practices Paper, the agencies are considering establishing a two-hour RTO for the sector-critical systems of covered entities.

Additionally, the Board is considering requiring Board-supervised covered entities, at the holding company level, 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. Such measurement would take into account the risks associated with internal dependencies, external dependencies, and trusted connections with access to sector-critical systems.

Questions on Standards for Sector-Critical Systems of Covered Entities

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 should 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?*

32. *Should different RTOs be set for different types of operations and, if so, how? Should RTOs be expected to become more stringent over time as technology advances?*

33. *The Board requests comment on the benefits of requiring Board-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?*

## *VII. Approach to Quantifying Cyber Risk*

The agencies are seeking to develop a consistent, repeatable methodology to support the ongoing measurement of cyber risk within covered entities. Such a methodology could be a valuable tool for covered entities and their regulators to assess how well an entity is managing its aggregate cyber risk and mitigating the residual cyber risk of its sector-critical systems. At this time the agencies are not aware of any consistent methodologies to measure cyber risk across the financial sector using specific cyber risk management objectives. 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 agencies are familiar with different methodologies to measure cyber risk for the financial sector. Among others, these include existing methodologies like the FAIR Institute's Factor Analysis of Information Risk standard and Carnegie Mellon's Goal-Question-Indicator-Metric process. Building upon these and other methodologies, the agencies are considering how best to measure cyber risk in a consistent, repeatable manner.

Questions on Approach to Quantifying Cyber Risk Section

*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?*

35. *What other models, frameworks, or reference materials should the agencies review in considering how best to measure and monitor cyber risk?*
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?*

## *VIII. Considerations for Implementation of the Enhanced Standards*

The agencies are considering various regulatory approaches to establishing enhanced standards for covered entities. The approaches range from establishing the standards through a policy statement or guidance to imposing the standards through a detailed regulation. Under one approach, 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. This approach would be similar to the approach that the agencies have taken in other areas of prudential supervision, such as the *Interagency Guidelines Establishing Standards for Safety and Soundness* and the *Interagency Guidelines Establishing Information Security Standards*.[21]

Under a second approach, the agencies could propose regulations that impose specific cyber risk management standards. For example, the standards could require covered entities to establish a cybersecurity framework commensurate with the covered entity's structure, risk

[21] *See* 12 CFR part 208, App. D-1, D-2; 12 CFR part 225, App. F (Board); 12 CFR part 364, App. A, B (FDIC); 12 CFR part 30, App. A, B, and D (OCC).

profile, complexity, activities, and size. Such standards would address the five categories of cyber risk management, discussed above, that the agencies consider key to a comprehensive cyber risk management program: (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. Within each category, a covered entity would be expected to establish and maintain policies, procedures, practices, controls, personnel and systems that address the applicable category, and to establish and maintain a corporate governance structure that implements the cyber risk management program on an enterprise-wide basis and along business line levels, monitors compliance with the program, and adjusts corporate practices to address the changes in risk presented by the firm's operations.

Under a third approach, the agencies could propose a regulatory framework that is more detailed than the second approach. As with the second approach, the regulation could contain standards for the five categories of cyber risk management. However, in contrast to the second approach, the regulation would include details on the specific objectives and practices a firm would be required to achieve in each area of concern in order to demonstrate that its cyber risk management program can adapt to changes in a firm's operations and to the evolving cyber environment.

In considering which option, or combination of options, to pursue to implement the standards, the agencies will consider whether the approach adopted ensures that the enhanced standards are clear, the additional effort required to implement the standards, whether the standards are sufficiently adaptable to address the changing cyber environment, and the potential costs and other burdens associated with implementing the standards.

Questions on Considerations for Implementation of the Enhanced Standards

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

38. *What are the trade-offs, in terms of the potential costs and other burdens, among the three options discussed above? The agencies invite commenters to submit data about the trade-offs among the three options discussed above.*

39. *Which approach has the potential to most effectively implement the agencies' expectations for enhanced cyber risk management?*

**[THIS SIGNATURE PAGE RELATES TO THE ADVANCE NOTICE OF PROPOSED RULEMAKING TITLED "ENHANCED CYBER RISK MANAGEMENT STANDARDS"]**

By order of the Board of Governors of the Federal Reserve System, October 19, 2016.

*Robert deV. Frierson (signed)*

Robert deV. Frierson,
Secretary of the Board

BILLING CODE: 6210-01-P