Banking Regulators Float Broad Cyber Risk Approach

October 31, 2016

Contents

Introduction

In October 2016, the U.S. federal banking agencies[1] jointly issued an advance notice of proposed rulemaking regarding **enhanced cyber risk management standards** (the "**Enhanced Standards**").[2] The Agencies proposed the Enhanced Standards in an era of increased cybersecurity attacks and dangers, where heightened cybersecurity standards and compliance are inevitable.[3] Other regulators and groups – such as the New York State Department of Financial Services,[4] FinCEN,[5] and the financial ministers of the G-7[6] – have also recently proposed new rules and frameworks as a result of recent high-profile cyberattacks on banks and other institutions. The U.S. Department of the Treasury and U.S. Department of Homeland Security jointly held a meeting on October 20, 2016, with top executives within the financial services industry, top officials from various financial regulators, and other Administration officials to discuss cybersecurity and the possible systemic effects of a major cyberattack.[7] These actions are all part of a perhaps loosely coordinated effort to require the financial sector to "up its game" given the potentially serious consequences of failure.

In this era of increased cyberattacks, the art will be to develop a regulatory framework that is flexible enough, and sophisticated enough, to encourage enhanced standards and compliance without imposing costs too high for the risks. The balance is a delicate one. The advance notice of proposed rulemaking ("**ANPR**") therefore should receive careful thought and scrutiny. The Enhanced Standards intend to strengthen the ability of Covered Entities to prevent a cyberattack (operational resilience) and also

[1] The Board of Governors of the Federal Reserve System (the "**Federal Reserve**"), the Office of the Comptroller of the Currency (the "**OCC**") and the Federal Deposit Insurance Corporation (the "**FDIC**") (collectively, the "**Agencies**").

[2] The Enhanced Standards would apply on an enterprise-wide basis to U.S. bank holding companies and U.S. savings and loan holding companies with $50 billion or more in total consolidated assets, the U.S. operations of foreign banking organizations ("**FBOs**") with $50 billion or more in total U.S. assets, nonbank financial companies designated by the Financial Stability Oversight Council for supervision by the Federal Reserve ("**Designated Nonbank SIFIs**"), certain financial market infrastructures supervised by the Federal Reserve ("**Federal Reserve-Supervised FMIs**") and (directly or indirectly) certain service providers to these institutions (collectively, "**Covered Entities**").

[3] Including the attack on the **Bangladesh Central Bank** earlier in 2016.

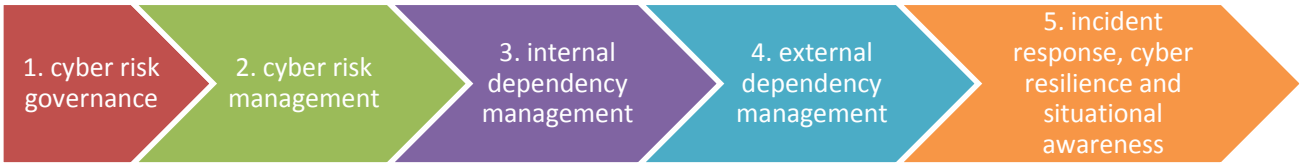
[4] *See* Davis Polk Memorandum, NYDFS Proposes New Cybersecurity Regulations (Oct. 13, 2016), available **here**.

[5] Davis Polk Beyond Sandbox Blog Post, FinCEN issues Advisory and FAQs on Cyber-Events and Cyber-Enabled Crime (Oct. 27, 2016), available **here**.

[6] G7 Fundamental Elements of Cybersecurity for the Financial Sector (Oct. 11, 2016), available **here**.

[7] Readout from a Treasury Spokesperson of the Administration's Meeting with Financial Regulators and CEOs on Cybersecurity in the Financial Services Sector (Oct. 20, 2016), available **here**.

reduce the potential impact on the financial system in the event of a cyberattack:[8]



Based on our review, if the final rules are anything like the form proposed, the ANPR would represent a major expansion of the existing and proposed patchwork of cybersecurity regulations and guidance. While it is not clear whether the end result will be in the form of specific regulations or regulatory policy statements, the Agencies will likely promulgate broad principles designed to create an environment that would prevent successful attacks in the first instance, and recover rapidly from any successful attack were it to occur. The ANPR contemplates a marriage of cybersecurity standards with a compliance regime that is inspired by the concepts of post-financial crisis banking regulation including governance by boards of directors (i.e., credible challenge) and senior management and review by independent risk management and audit functions as part of the three lines of defense model. The Enhanced Standards would increase testing to ensure compliance and require further participation by a Covered Entity's board of directors, which echoes the OCC's enhanced risk governance guidelines[9] and the Federal Reserve's expectations for governance and risk management for SIFIs.[10]

In the process, the Agencies would create enforceable standards for a broader range of covered entities in the financial sector, although some important players would be left out because of limitations in regulatory jurisdiction. The most dramatic expansion is the direct and indirect application of many of the Enhanced Standards to third-party service providers. This expansion would push compliance and other costs onto those service providers (who would presumably raise their prices on financial institutions) and, effectively, indirectly impose the standards on smaller financial institutions. In addition, for sector-critical functions, there would be a system-by-system regime at a higher tier of standards and compliance, including a recovery time objective of two hours. While the major service

The ANPR includes 39 questions that the Agencies seek feedback on, with comments due by January 17, 2017. These questions focus on the scope of application, sector-critical systems, the five categories of the Enhanced Standards, quantifying cyber risk, and implementation of the Enhanced Standards. Some key questions include:

- 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?
- 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?
- What policies do Covered Entities currently follow in reporting material cyber risks and vulnerabilities to the CEO and board of directors?
- 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?
- What would be the incremental costs to Covered Entities of moving toward a two-hour RTO objective for all sector-critical systems?

[8] Approaching cybersecurity through the lens of these categories is not unique to the ANPR. While some existing guidance uses more general categorization (*e.g.*, "Identify"), others use the format of a broad umbrella under which to promulgate a series of suggestions (*e.g.*, "Involve the Board of Directors").

[9] *See, e.g.*, Davis Polk Memorandum, Risk Governance: Visual Memorandum on Guidelines Adopted by the OCC (Nov. 7, 2014), available here.

[10] *See* SR Letter 12-17, "Consolidated Supervision Framework for Large Financial Institutions" (Dec. 17, 2012), available here.

providers that would likely be covered by any rulemaking are both well aware of cybersecurity risks and engaged in intensive efforts to mitigate them, and are already subject to the Agencies' supervision under the Bank Service Company Act, the direct application of the Enhanced Standards to such entities would be a significant regulatory step. There is also an open question as to whether foreign banks could realistically apply the standards only to their U.S. operations.

Since the 2010 Dodd-Frank Act, the Agencies have been working to increase the resiliency of SIFIs to make them less likely to fail in the first place (for example, by increasing expectations regarding strong governance and enterprise risk management[11] and by increasing capital and liquidity requirements[12]), and also to make them more resolvable and reduce the potential for systemic risk after failure.[13] The Enhanced Standards represent an extension of these efforts after the recognition of the significant and no-longer-hypothetical risk of major cyberattacks.

In addition to the five-category approach, the ANPR proposes a two-tiered framework, with more stringent standards for "entities that are critical to the functioning of the financial sector." Covered Entities with sector-critical systems[14] must adhere to sector-critical standards by implementing "the most effective, commercially available controls" to protect against a cybersecurity attack.

In this memorandum, we discuss:

- the scope of application of the enhanced cyber risk management standards;
- existing cybersecurity requirements and guidelines;
- the five categories of the Enhanced Standards; and
- sector-critical systems and the Enhanced Standards for them.

Who Is Covered by the Enhanced Standards?

Covered Entities

The Agencies are considering applying the Enhanced Standards to a wide swath of large and interconnected financial institutions and their third-party service providers, including:

- Bank holding companies ("**BHCs**") and savings and loan holding companies ("**SLHCs**") with ≥ $50 billion in total consolidated assets;
- Banks and savings associations, regardless of size, that are subsidiaries of a BHC or SLHC with ≥ $50 billion in total consolidated assets;
- Banks and savings associations with ≥ $50 billion in total consolidated assets;

---

[11] *See, e.g.,* Davis Polk Memorandum, Risk Governance: Visual Memorandum on Guidelines Adopted by the OCC (Nov. 7, 2014), available here.

[12] *See* Davis Polk Memorandum, U.S. Basel III Final Rule: Visual Memorandum (Jul. 8, 2013), available here; *see also* Davis Polk Memorandum, U.S. Basel III Liquidity Coverage Ratio Final Rule (Sept. 23, 2014), available here; Davis Polk Memorandum, Single Counterparty Credit Limits Proposed Rule (Mar. 22, 2016), available here; Davis Polk Memorandum, Foreign Banks: Overview of Dodd-Frank Enhanced Prudential Standards Final Rule (Feb. 24, 2014), available here.

[13] *See* Section 165(d) of the Dodd-Frank Wall Street Reform and Consumer Protection Act; *see also* 12 CFR § 360; Agencies Announce Determinations and Provide Feedback on Resolution Plans of Eight Systemically Important, Domestic Banking Institutions (2016).

[14] The Agencies have not yet settled on a final definition for sector-critical systems, but indicated that they will look to the volume of a firm's clearing and settlement activities as a key indicator of the impact that a firm would have on the financial markets in the event of a cyberattack.

- U.S. operations of FBOs with ≥ $50 billion in total U.S. assets;
- Designated Nonbank SIFIs;
- Federal Reserve-Supervised FMIs; and
- Service providers to all of the above.

The ANPR states that the Enhanced Standards would apply on an enterprise-wide basis because "cyber risks in one part of an organization could expose other parts of the organization to harm." In practice, this ought to mean that a top-tier Covered Entity would be required to have a program, including policies and procedures, in place that covers not just the direct activities of the top-tier Covered Entity, but also activities by its subsidiaries. Under this approach, subsidiaries that are Covered Entities could generally rely on the enterprise-wide compliance program, including policies and procedures, instead of having to create their own separate programs. This approach is consistent with institutions' existing enterprise-wide compliance programs. The ANPR is unclear, however, about whether the scope of the regulatory authority of each Agency might, as it has done in some other recent final and proposed regulations, lead to some separate requirements, such as governance, on a legal entity by legal entity basis.[15] Certain large bank subsidiaries – for example, national banks with more than $50 billion in total consolidated assets – may be required to meet certain elements of the Enhanced Standards on a stand-alone basis, for example, by having the board of directors of the national bank approve and review the cybersecurity program to match the cyber risk profile of the national bank.[16]

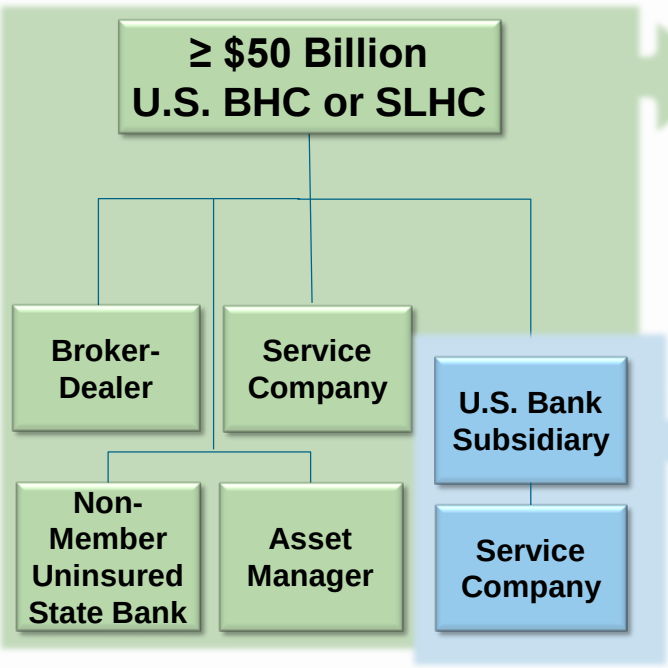
Each regulator would supervise, examine and enforce the Covered Entities that it regulates, as shown in the following diagrams. Subsidiaries of Covered Entities that are also Covered Entities may be subject to the regulations of and supervision by a different Agency than their direct or indirect parent.

[15] For example, although the Agencies promulgated a joint Volcker Rule, examinations are done by each Agency based upon whether it regulates the legal entity involved. Moreover, some Agencies have asked for separate certifications from CEOs at different levels. *See, e.g.*, Prohibitions and Restrictions on Proprietary Trading and Certain Interests in, and Relationships with, Hedge Funds and Private Equity Funds, 12 CFR part 44 (OCC); 12 CFR part 248 (FRB); 12 CFR part 351 (FDIC); 17 CFR part 255 (SEC); 17 CFR part 75 (CFTC); *see also* Davis Polk Visual Memorandum, Incentive Compensation for Financial Institutions: Reproposal (May 12, 2016), available **here**.

[16] OCC, Guidelines for Heightened Standards at 54,521, available **here** ("The covered bank's Framework should ensure that the covered bank's risk profile is easily distinguished and separate from its parent company for risk management and supervisory reporting purposes and that the safety and soundness of the covered bank is not jeopardized by decisions made by the parent company's board of directors and management . . . . Although the final Guidelines continue to provide that a covered bank should establish its own Framework when the parent company's and covered bank's risk profiles are not substantially the same, the Guidelines also clarify that even in these cases a covered bank may, in consultation with the OCC, incorporate or rely on components of its parent company's risk governance framework when developing its own Framework to the extent those components are consistent with the objectives of these Guidelines . . . . Indeed, the OCC encourages covered banks to leverage their parent company's risk governance framework to the extent appropriate, including using employees of the parent company . . . . We note that the extent to which a covered bank may use its parent company's framework will vary depending on the circumstances. For example, it may be appropriate for a covered bank to use the parent company's framework without modification where there is significant similarity between the covered bank's and parent company's risk profiles, or where the parent company's framework provides for focused governance and risk management of the covered bank. Conversely, a covered bank may incorporate fewer components of the parent company's framework where the risk profiles of the covered bank and parent are less similar, or the parent company's risk governance framework is less focused on the covered bank . . . . [M]odifications may be necessary when the parent company's risk management objectives are different than the covered bank's risk management objectives. For example, a parent company's board of directors and management will need to understand and manage aggregate risks that cross legal entities, while a covered bank's board and management will need to understand and manage only the covered bank's individual risk profile.").

Davis Polk

BHCs and SLHCs ≥ $50 Billion and Their Subsidiaries; Banks



- A U.S. BHC or SLHC with ≥ $50 billion in total consolidated assets and all of its subsidiaries (including broker-dealers and asset managers) would be Covered Entities and subject to Enhanced Standards
- The Federal Reserve would be the supervising agency

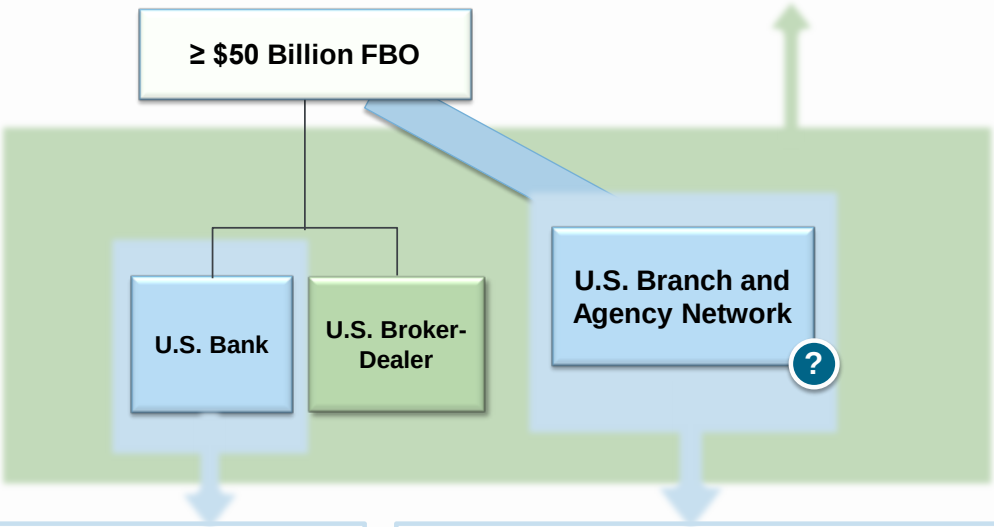
- A bank will be a Covered Entity if it is a subsidiary of a BHC or SHLC ≥ $50 billion in total consolidated assets*
- The supervising regulator of the bank and its subsidiaries for purposes of the Enhanced Standards would be the primary federal regulator of the bank:

• National Bank • National Savings Association	OCC
• State Member Bank	Federal Reserve
• State Non-Member Bank • State Savings Association	FDIC

* A bank that itself has ≥ $50 billion in total consolidated assets will also be a Covered Entity (as would its subsidiaries), but there are very few banks of this size in the United States that are not subsidiaries of a BHC or SLHC.

U.S. Operations of FBOs with Total U.S. Assets of ≥ $50 Billion

- For an **FBO with ≥ $50 billion in total U.S. assets**, its U.S. operations would be subject to the Enhanced Standards (whether or not the FBO has an IHC)
- The **Federal Reserve** would generally be the supervising agency



- A bank that is a subsidiary of an FBO with ≥ $50 billion in U.S. assets will be a Covered Entity
- The supervising regulator of the bank and its subsidiaries for purposes of the Enhanced Standards would be the primary federal regulator of the bank):

• State Member Bank	Federal Reserve
• National Bank • National Savings Association	OCC
• State Non-Member Bank • State Savings Association	FDIC

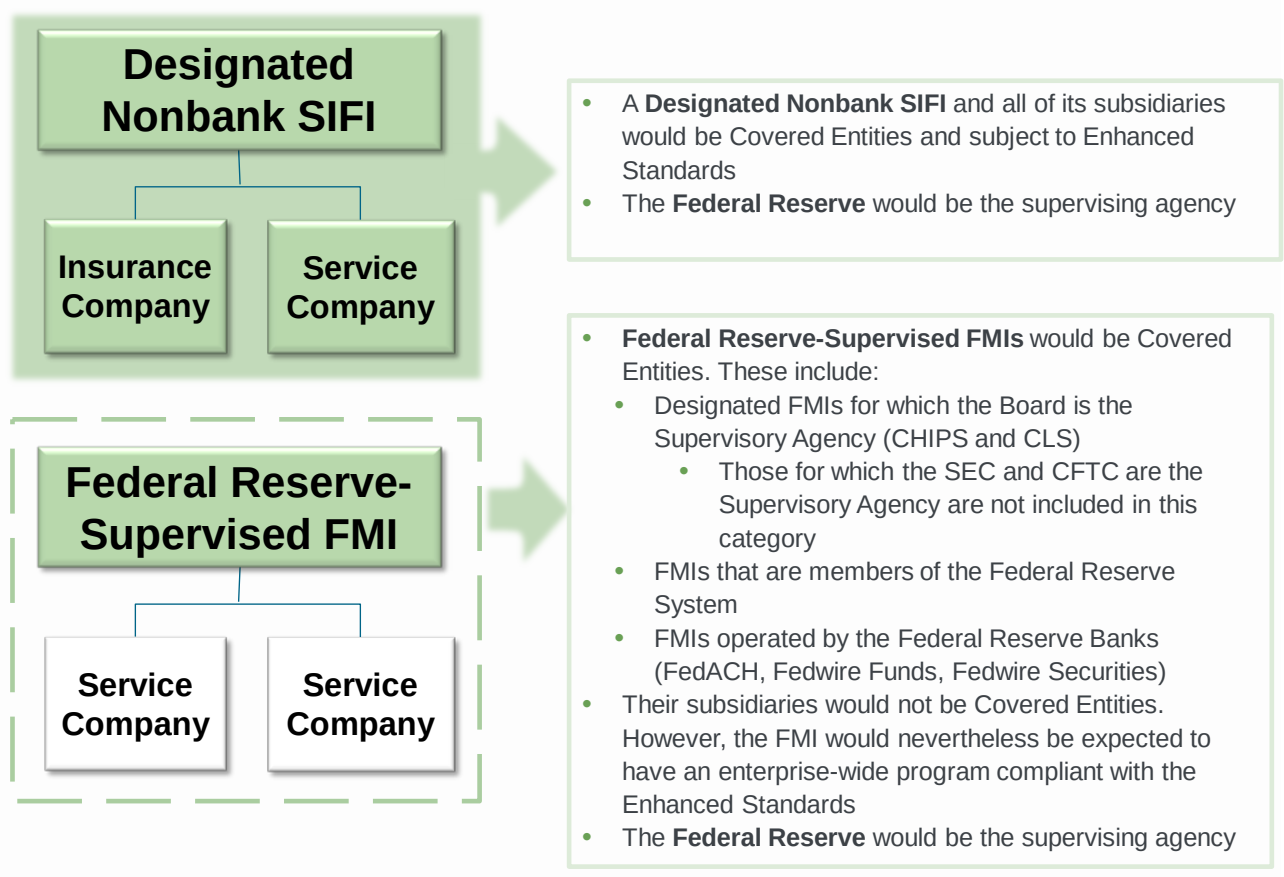
- An FBO's U.S. branches and agencies are part of its U.S. operations and may be subject to the Enhanced Standards
- The ANPR notes that certain U.S. branches and agencies of foreign banks that are subsidiaries of U.S. BHCs and SLHCs would be Covered Entities, but does not explicitly note that FBO's U.S. branches and agencies would be covered
- The supervising regulator of the branch or agency for purposes of the Enhanced Standards would be the primary federal regulator:

• State-licensed uninsured branches	Federal Reserve
• Federal branches or agencies of a foreign bank (insured and uninsured)	OCC
• State insured branch of a foreign bank	FDIC

The ANPR's thesis that cybersecurity programs should be on an enterprise-wide basis is in some tension with the Agencies' jurisdictional reach over FBOs. An FBO may or may not be able to apply the Enhanced Standards only with respect to its U.S. operations. For those foreign banks with a more limited U.S. footprint

– e.g., only an uninsured branch – some recognition of equivalent home country standards might be a solution.[17]

Designated Nonbank SIFIs and Federal Reserve Supervised FMIs



Service Providers to Covered Entities

The Agencies are also considering applying the Enhanced Standards to services ("**Covered Services**") provided by service providers to Covered Entities. The ANPR notes that doing so would "ensure consistent, direct application of the standards" no matter whether an operation is performed by a Covered Entity or its service provider. Under the ANPR, the Enhanced Standards would apply ***directly*** to certain critical service providers and ***indirectly*** to certain other service providers, by requiring Covered Entities to verify that their service providers are complying with the Enhanced Standards. As a result, the Agencies would have the power to enforce the Enhanced Standards not only against the Covered Entity, but also the service provider itself.

[17] An FBO with $50 billion in U.S. assets must generally have a U.S. risk committee and a U.S. chief risk officer for its U.S. operations, including its U.S. branch and agency network. Additionally, an FBO with $50 billion in non-branch U.S. assets is generally required to have an intermediate holding company. Davis Polk Memorandum, Foreign Banks: Overview of Dodd-Frank Enhanced Prudential Standards Final Rule (Feb. 24, 2014), available here.

While as a technical matter, the ANPR speaks of applying the Enhanced Standards to Covered Services, we believe that there is a possible extension of the Bank Service Company Act ("**BSCA**") implied in the ANPR in that it will cover entities that were traditionally thought to be outside the scope of the BSCA.[18] Under the BSCA, the Agencies have examination and oversight authority over service providers to banks and their subsidiaries and affiliates. The scope of the Enhanced Standards applicable to service providers potentially encompasses a somewhat larger group of entities, and if an entity providing a Covered Service did not meet the Enhanced Standards, direct action would, according to the ANPR, allow, among other things:

- facilitating supervisory action by the relevant agency (e.g., through exams, orders, etc.); and
- establishing an obligation on the service provider to meet the Enhanced Standards.

Further, the BSCA has traditionally been applied in situations where a service provider provides a core banking service or interfaces directly with a depository institution's customers.[19] For example, a utility that provides electricity to a Covered Entity would fit the colloquial definition of a service provider, but would generally not be considered to be a Bank Service Company subject to examination and oversight by a federal banking agency. It is thus conceivable that service providers that have traditionally thought of themselves as outside the scope of the bank regulatory agencies' supervision and enforcement could become subject to the Enhanced Standards.

Regardless of whether the Agencies intended to bring a new group of service providers to banks within the scope of the Enhanced Supervision, it is clear that the Agencies are expanding their supervisory reach in other areas. The Agencies are also considering applying the Enhanced Standards indirectly to service providers that might not otherwise be covered by the BSCA – i.e., to service providers to Federal Reserve-Supervised FMIs and Designated Nonbank SIFIs. These Covered Entities would be required to verify that any third-party services are subject to the Enhanced Standards, which as a practical matter would require them to write the Enhanced Standards into their agreements with service providers and would thus impose obligations, and potential regulatory exposure, on such service providers.

While the ANPR contemplates application of the Enhanced Standards only to entities providing Covered Services to Covered Entities, given the nature of the financial sector and its service providers, it is likely that the Enhanced Standards will be applied more broadly throughout the financial system.

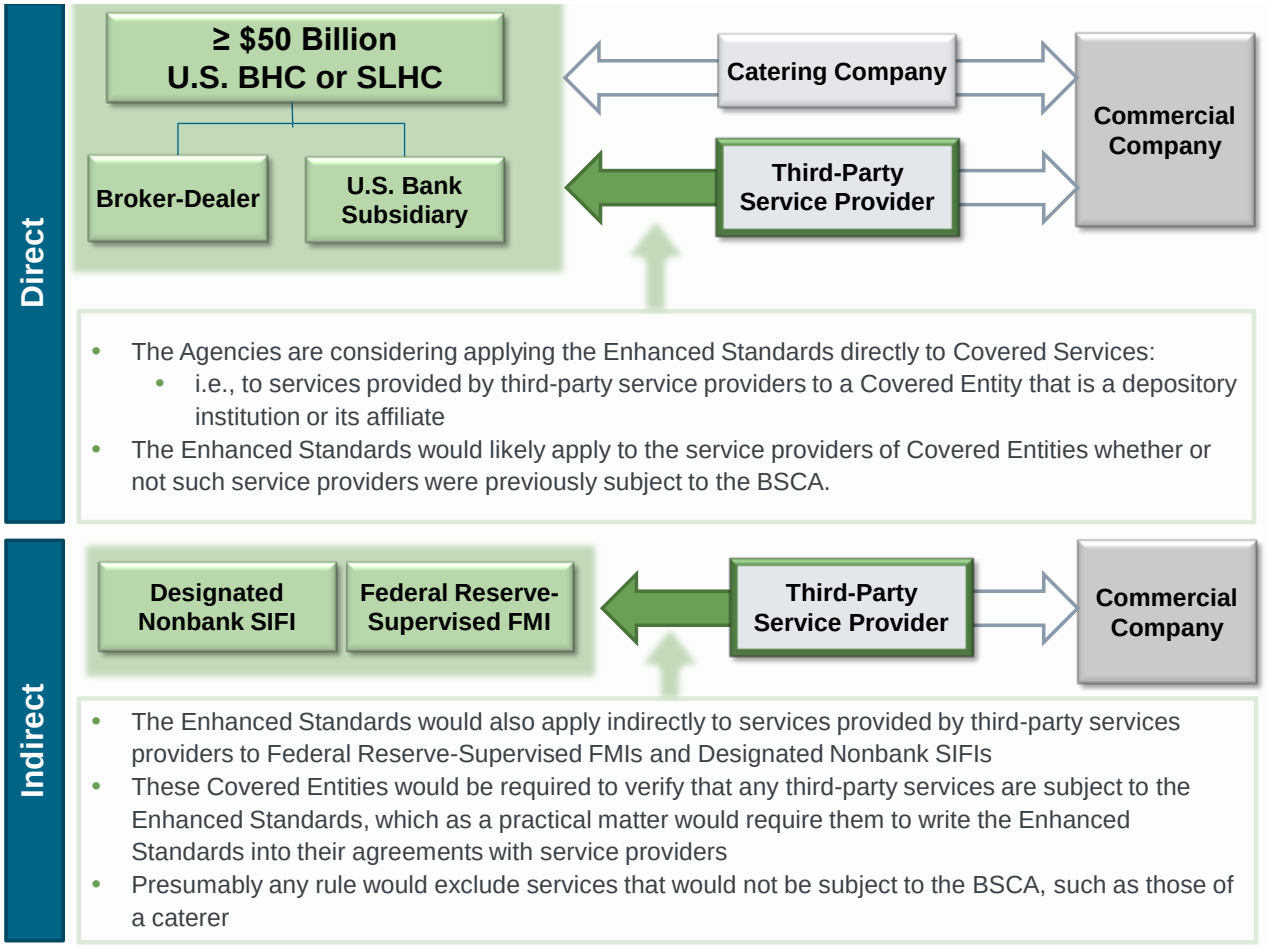
The ANPR does not indicate whether the Agencies are considering applying the Enhanced Standards to services provided by service providers to the U.S. operations of FBOs.

---

[18] 12 USC § 1867(c). The purpose of the Bank Service Company Act is to enable the U.S. banking agencies to regulate bank service companies that might otherwise have avoided prudential regulation. To accomplish this, the BSCA provides that companies meeting the definition of a "bank service company" are subject to regulation and examination by the U.S. banking agencies. While the BSCA relates primarily to the regulation and examination of service companies that are owned by insured depository institutions, Section 1867(c) serves to extend that regulation and examination authority to situations where an insured depository institution has outsourced BSCA services to a third party.

[19] *See, e.g.,* Third-Party Relationships: Risk Management Guidance, OCC Bulletin 2013-29 (Oct. 30, 2013), available **here** ("In contracts with service providers, stipulate that the performance of activities by external parties for the bank is subject to OCC examination oversight, including access to all work papers, drafts, and other materials. The OCC treats as subject to 12 USC § 1867(c) and 12 USC § 1464(d)(7), situations in which a bank arranges, by contract or otherwise, for the performance of any applicable functions of its operations. Therefore, the OCC generally has the authority to examine and to regulate the functions or operations performed or provided by third parties to the same extent as if they were performed by the bank itself on its own premises.").

Service Provider to Covered Entities



Existing Standards

If ultimately adopted, the Enhanced Standards would supplement an already expansive web of regulator-issued cybersecurity rules and guidance that many financial institutions currently adhere to, by choice or by requirement. For example:

- Insured depository institutions ("**IDIs**") of all sizes must currently comply with federal Interagency Guidelines Establishing Information Security Standards on safeguarding the confidentiality and security of customer information (the "**Security Guidelines**"), issued pursuant to the Gramm-Leach-Bliley Act of 1999.[20] The Security Guidelines require IDIs to implement an information security program covering administrative, technical, and physical safeguards intended specifically to protect individual consumers' personal information. The board of directors must approve the program and oversee its development, implementation, and maintenance.

[20] *See* 12 CFR part 30, appendix B (OCC); 12 CFR part 208, appendix D-2 and part 225, appendix F (FRB); 12 CFR part 364, appendix B (FDIC); and 12 CFR part 748, appendix A (NCUA).

- IDIs must also take into account the Federal Financial Institutions Examination Council's ("**FFIEC**") Information Security Booklet ("**FFIEC Guidance**"),[21] which was updated in September 2016, and may use the FFIEC's Cybersecurity Assessment tool in doing so. [22] According to the FFIEC, the tool "provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time." While the IT Handbook is not mandatory, the booklets promulgated in connection with the handbook lay out the FFIEC's expectations for an FFIEC-compliant institution's cybersecurity program.

- Several federal agencies have expressed support for the National Institute of Standards and Technology ("**NIST**") Framework for Improving Critical Infrastructure Cybersecurity [23] (the "**NIST Framework**") as a resource to assist companies in developing and implementing an appropriate cybersecurity program, although it is not specific to financial institutions.[24] The NIST Framework is voluntary by design, and is intended to be customizable for entities of different sizes and sophistication levels and across different industries, and thus is not proscriptive in a traditional one-size-fits-all model.

- The Federal Reserve, the OCC and the Securities and Exchange Commission in 2003 released an Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (the "**Sound Practices Paper**"), identifying broad industry consensus on business continuity objectives, including in the context of cybersecurity disruptions.[25] While it does not include binding regulatory requirements, it aims to describe best practices for the U.S. financial system in the cybersecurity arena. The Sound Practices Paper's focus is to minimize the systemic effects of a wide-scale disruption on critical financial markets, and it emphasizes the need to establish backup capacity and quick resumption of clearance and settlement activities in wholesale financial markets.

- Perhaps most robust among existing cybersecurity guidance is the Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions Guidance on cyber resilience for financial market infrastructures (the "**CPMI-IOSCO Guidance**"), which institutions may implement on a voluntary basis.[26] Issued in late 2015, this guidance is intended to promote the safe and efficient operation of the financial market infrastructures to avoid the kind of financial shocks that can be transmitted across both domestic and international financial markets.

- More recent guidance includes the G7 Fundamental Elements of Cybersecurity for the Financial Sector (the "**Fundamental Elements**").[27] While the Fundamental Elements are not binding on U.S.

---

[21] The FFIEC is composed of the principals of the following: the Federal Reserve, the FDIC, the National Credit Union Administration ("**NCUA**"), the OCC, the State Liaison Committee ("**SLC**"), and the Consumer Financial Protection Bureau ("**CFPB**"). Although the FFIEC Guidance is not a formal regulation, it is used by bank examiners in assessing the level of security risks to a financial institution's information systems and, as such, sets forth regulatory expectations with respect to financial institutions' cybersecurity programs.

[22] FFIEC, Cybersecurity Assessment Tool, available **here**.

[23] Nat'l Inst. Standards & Tech., Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), available **here**.

[24] The SEC has suggested that it regards the NIST standard as a baseline for companies within its regulatory purview, as noted **here**. The FTC has also noted that the NIST Framework is "consisted with the process-based approach that the FTC has followed since the late 1990s . . . and the agency's educational messages to companies," as noted **here**. Further, the FCC has included instructions for complying with the suggestions of the NIST Framework in its Cybersecurity Risk Management and Best Practice Final Report, available **here**. Even the FFIEC provides information on mapping its own assessment tool to the NIST Framework, as noted **here**.

[25] Fed. Reserve, OCC & SEC, Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (Apr. 8, 2003), available **here**.

[26] Comm. on Payments & Market Infra., Board Int'l Org. Sec. Comm., Guidance on Cyber Resilience for Financial Market Infrastructures (Nov. 2015), available **here**.

[27] G7 Cyber Expert Group, G7 Fundamental Elements of Cyber Security for the Financial Sector (Oct. 11, 2016), available **here**.

financial institutions, they can be helpful for institutions to recognize the baseline standards for information security that are of sufficiently broad applicability and importance to warrant inclusion in an international summary of fundamental cybersecurity requirements.

- Even more recently, the New York Department of Financial Services has proposed a series of new cybersecurity rules for financial institutions that, if promulgated, would take effect January 1, 2017.[28] The rules would apply to banks, insurance companies and other financial institutions chartered or licensed by the New York Department of Financial Services, and would implement a series of mandatory requirements for those entities including prescriptive cybersecurity measures and vulnerability tests.

Many of these standards are inspired by existing safety and soundness standards, and the principles underlying their requirements should be deeply familiar to all Covered Entities. Most financial institutions to which the Enhanced Standards would apply already have a cybersecurity program that aligns with existing cybersecurity rules and guidance. As a result, these institutions may already have policies and procedures in place that broadly correspond to many of the potential new requirements. It is important to note, however, that while many of the proposed standards in the ANPR are present in existing guidance, the ANPR contemplates standards that would be required – and enforceable – rather than simply suggested.[29] One approach that the Agencies are considering, as set forth in the ANPR, is similar to the existing frameworks, combining a requirement for "a risk management framework for cyber risk" with "policy statements or guidance that describes minimum expectations" for that framework. The Agencies are, however, also contemplating a more prescriptive approach with "regulations that impose specific cyber risk management standards" that would also include "details on the specific objectives and practices a firm would be required to achieve in each area of concern." If the Agencies ultimately choose the latter approach, compliance obligations and related record-keeping requirements to document compliance could increase considerably.

Proposed Enhanced Standards – Five-Category Approach

Category One: Cyber Risk Governance

The ANPR identifies several key components of cyber risk governance:

Cyber Risk Management Strategy. The centerpiece of cyber risk governance as described in the ANPR is a formal, enterprise-wide cyber risk management strategy. A Covered Entity would be required to develop and maintain such a strategy and integrate it into the entity's overall business strategy and risk management.

- The cyber risk management strategy would articulate:

[28] N.Y. Dep't Fin. Serv., Cybersecurity Requirements for Financial Services Companies Proposed Rule (Sept. 13, 2016), available here. Most states have some form of financial breach rule, whether in the form of notification requirements or prescriptive mandates, and while many except financial institutions from their purview due to overlap with federal regulation, some such as Massachusetts, do not. *See, e.g.,* Mass. 201 CMR 17.00 Standards for the Protection of Personal Information of Residents of the Commonwealth, available here; Oregon ORS 646A.604 Notice of Breach of Security, available here.

[29] Most extant guidance is voluntary or sets general expectations rather than strict requirements. In general, these frameworks eschew check-the-box regulatory mandates in favor of a more fluid and flexible approach. Moreover, they may also afford substantial discretion to the individual entity to implement safeguards as it deems appropriate. Other guidance is more limited in scope than the Enhanced Standards, as their objective is to ensure protection of personal information of individuals, not to ensure that institutions develop a comprehensive cybersecurity program.

  - how the Covered Entity intends to address its inherent cyber risk – i.e., its cyber risk before mitigating controls or other factors are taken into consideration; and
  - how the Covered Entity would maintain an acceptable level of residual cyber risk – i.e., its remaining cyber risk after mitigating controls and other factors have been taken into consideration – and maintain resilience on an ongoing basis.
- The board of directors of the Covered Entity, or an appropriate board committee, would be responsible for approving the cyber risk management strategy.

Cyber Risk Tolerances. A Covered Entity would be required to establish cyber risk tolerances consistent with the firm's risk appetite and strategy. The Agencies are considering requiring the entity's board of directors, or an appropriate board committee, to review and approve the enterprise-wide cyber risk appetite and tolerances. In addition, a Covered Entity would be required to manage cyber risk appropriate to the nature of the firm's operations and reduce its residual cyber risk to the appropriate level approved by the board.

Cyber Risk Identification and Assessment. A Covered Entity would need to be able to identify and assess its activities and exposures that present cyber risk and determine ways to aggregate them to assess the Covered Entity's overall residual cyber risk.

Enterprise-Wide Cyber Risk Management Framework. A Covered Entity would be required to establish an enterprise-wide cyber risk management framework that includes policies and reporting structures to support and implement the Covered Entity's cyber risk management strategy. The framework must include the following:

- Delineated cyber risk management and oversight responsibilities, including reporting structures and expectations for independent risk management, internal controls, and internal audit personnel;
- Established mechanisms for evaluating whether the firm has sufficient resources to address the cyber risks it faces;
- Established policies to address resource shortfalls or knowledge gaps;
- Mechanisms for identifying and responding to cyber incidents and threats; and
- Procedures for testing the effectiveness of the firm's cybersecurity protocols and updating them as the threat landscape evolves.

Board Oversight. In addition to approving the cyber risk management strategy, the Covered Entity's board of directors would be responsible for overseeing and holding senior management accountable for implementing the firm's cyber risk management framework. Other requirements related to board oversight include the following:

- **Expertise**. 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.
- **Credible Challenge**. Consistent with existing supervisory expectations, the board of directors must be able to provide credible challenge to management regarding cybersecurity matters and the evaluation of cyber risks and resilience.
- **Independence**. The Agencies are considering requiring senior leaders with responsibility for cyber risk oversight to be independent of business line management. The 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.

Links to Existing Risk Governance Requirements. The ANPR indicates how the contemplated cyber risk governance standards would relate to existing risk governance requirements and standards for certain financial institutions:

- A Federal Reserve-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 Covered Entity's board of directors, consistent with the Federal Reserve's consolidated supervision framework for large financial institutions set out in SR Letter 12-17. In addition, the cyber risk management strategy would be part of the larger global risk management framework required by the enhanced prudential standards set out in 12 CFR part 252.
- 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 out at 12 CFR part 30 Appendix D.

Category Two: Cyber Risk Management

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 separate functions, such as the three lines of defense risk-management model, with appropriate checks and balances.[30] According to the Agencies, using the three lines of defense approach would allow Covered Entities to more accurately and effectively identify, monitor, measure, manage, and report on cyber risk.

Business Units. The Agencies are considering the following requirements for the units responsible for a Covered Entity's day-to-day business functions:

- Assess, on an ongoing basis, the cyber risks associated with the activities of the business unit;
- Assess the cyber risks and potential vulnerabilities associated with every business asset (i.e., workforce, data, technology, and facilities), service, and IT connection point for the business unit, and update these assessments as threats, technology, and processes evolve;
- Ensure that information regarding cyber risks is shared with senior management, including the CEO, as appropriate, in a timely manner so senior management can address and respond to emerging cyber risks and cyber incidents as they develop; and
- Adhere to procedures and processes necessary to comply with the Covered Entity's cyber risk management framework, with such procedures and processes designed to ensure that the business unit's cyber risk is effectively identified, measured, monitored, and controlled, consistent with the Covered Entity's risk appetite and tolerances.

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 units' 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. According to the Agencies, it is essential that the independent risk management function have sufficient

[30] Davis Polk Memorandum, Risk Governance Visual Memorandum on Guidelines Adopted by the OCC (Nov. 7, 2014), available here.

independence, stature, authority, resources, and access to the board of directors to ensure that the firm's operations are consistent with the cyber risk management framework. The reporting lines must be clear and separate from those for other operations and business units.

The Agencies are considering the following requirements for the independent risk management function:

- 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;
- On a continuous basis, identify, measure, and monitor cyber risk across the enterprise and continually assess the firm's overall exposure to cyber risk;
- Promptly notify the CEO and board of directors, as appropriate, when the assessment of a particular cyber risk by the independent risk management function differs from that of a business unit, as well as of any instances when a business unit has exceeded the Covered Entity's established cyber risk tolerances;
- Determine whether cyber risk controls are appropriately in place across the enterprise consistent with the Covered Entity's established risk appetite and tolerances;
- On an ongoing basis, 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; and
- 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.

Internal Audit. The Agencies noted the importance of cyber risk and cyber risk management for the internal audit function at Covered Entities, pointing to the critical role of internal audit with respect to a firm's risk management, internal controls, and corporate governance. The Agencies are considering the following requirements for the internal audit function:

- Assess whether the Covered Entity's cyber risk management framework complies with applicable laws and regulations and is appropriate for the entity's size, complexity, interconnectedness, and risk profile; and
- Incorporate an assessment of cyber risk management into the overall audit plan of the Covered Entity, including:
    - Evaluating 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. This evaluation must 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; and
    - Assessing the capabilities of the business units and independent risk management function 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.

Categories Three and Four: Internal and External Dependency Management

The Enhanced Standards would require the Covered Entities to identify and manage cyber risks associated with both "internal dependencies" and "external dependencies" as well as continually assess and improve, as necessary, their effectiveness in reducing those cyber risks on an enterprise-wide basis.

- **Internal Dependency:** refers to a Covered Entity's business assets (i.e., workforce, data, technology, and facilities) upon which the entity depends to deliver services, as well as the information flows and interconnections among those assets.
- **External Dependency:** refers to a Covered 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. External dependency also includes interconnection risks associated with non-critical external parties that maintain trusted connections to important systems.

The following table summarizes the proposed requirements for internal and external dependency management.

Topic	Internal Dependency Management Requirements	External Dependency Management Requirements
Dependency Management Strategy	▪ Integrate internal dependency management strategy into Covered Entity's overall strategic risk management. ▪ Internal dependency management strategy must include: ▪ Well-defined roles and responsibilities; ▪ Policies, standards, and procedures to identify and manage cyber risks associated with internal assets, including those connected to or supporting sector-critical systems, with regular updates throughout those assets' lifespans; ▪ Appropriate oversight to monitor effectiveness in reducing internal dependency-related cyber risks; and ▪ Appropriate compliance mechanisms.	▪ Integrate external dependency management strategy into Covered Entity's overall strategic risk management. ▪ External dependency management strategy must include: ▪ Well-defined roles and responsibilities; ▪ Policies, standards, and procedures for external dependency management throughout the lifespan of the relationship (e.g., due diligence, contracting and sub-contracting, onboarding, ongoing monitoring, change management, off-boarding), with regular updates; ▪ Appropriate metrics to measure effectiveness in reducing external dependency-related cyber risks; and ▪ Appropriate compliance mechanisms.
Prioritized Inventory	▪ Maintain a current and complete inventory of all internal assets on an enterprise-wide basis, prioritized according to their criticality to the business functions they support, the entity's mission and the financial sector, as well as business functions.	▪ Maintain current, accurate, and complete listing of all external dependencies and trusted connections enterprise-wide, prioritized based on their criticality to the business functions they support, the entity's mission, and the financial sector, as well as business functions.
Mapping	▪ Map internal assets and business functions to other assets and other business functions, information flows, and interconnections.	▪ Map external dependences and business functions to supported assets and business functions.
Tracking/	▪ Track connections among assets and	▪ Monitor in real time all external

Topic	Internal Dependency Management Requirements	External Dependency Management Requirements
Monitoring	cyber risk levels throughout the assets' life cycles to support relevant data collection and analysis across the organization. ▪ Ensure the tracking capability permits timely notification of internal cyber risk management issues to designated internal stakeholders.	dependencies and trusted connections that support the cyber risk management strategy. ▪ Track connections among external dependencies, organizational assets, and cyber risk levels throughout their lifespans. ▪ Ensure the tracking capability permits timely notification of cyber risk management issues to designated stakeholders.
Controls	▪ Assess cyber risk of assets and their operating environments prior to deployment. ▪ Continually apply controls and monitoring assets and their operating environments over the lifecycle of assets. ▪ Assess relevant cyber risks of assets (including insider threats to systems and data) and mitigate identified deviations, granted exceptions and known violations to internal dependency cyber risk management policies, standards, and procedures.	▪ Prioritize monitoring, incident response, and recovery of systems critical to the Covered Entity and the financial sector. ▪ Support continued reduction of cyber risk exposure of external dependencies to the Covered Entity and sector until board-approved cyber risk appetite and tolerances achieved. ▪ Support timely responses to cyber risks to Covered Entity and sector. ▪ Monitor universe of external dependencies. ▪ Support relevant data collection and analysis. ▪ Track connections among external dependencies, organizational assets, and cyber risk levels throughout their lifespans.
Backup Testing	Periodically test backups to business assets.	Periodically test alternative solutions in case an external partner fails to perform as expected.

The Enhanced Standards would require that the Covered Entities continually review their internal business assets in order to better identify and manage cyber risks associated with those business assets. Existing guidance already focuses on the importance of surveilling internal business assets for this reason. The FFIEC Cybersecurity Assessment Tool sets as a baseline the requirement to catalogue all organizational assets and prioritize the assets by importance to the business. The Enhanced Standards would require a continual process to manage these internal business assets through several key aspects, as referenced in the above chart.

One of the key aspects is the keeping of a comprehensive inventory of all business assets across the Covered Entity, prioritized in order of importance to the business functions that those assets support, the Covered Entity's mission and the financial sector as a whole. The inventory must show the interconnection between the business assets and how a cyberattack on one of those assets would impact the other internal

business assets. Similarly, CPMI-IOSCO Guidance requires that the financial market infrastructures[31] identify and maintain a catalogue of information assets.

Another key aspect is the implementation of controls to address inherent cyber risks associated with the Covered Entity's assets. The Covered Entity's board of directors must review and approve such controls. The NIST Framework requires a robust understanding of internal assets in order to identify potential threats to those assets. It also requires an infrastructure to monitor those assets on an ongoing basis. Even though existing guidance requires that a Covered Entity have controls in place to monitor internal assets, the Enhanced Standards would require the review and approval of the board of directors, a significant enhancement over existing guidance.

The Covered Entities must have a structure in place to "identify and manage cyber risks associated with their external dependences and interconnection risks"[32] and must continually review and improve upon the way they handle and prevent against any potential cyberattacks. Existing guidance already focuses on the importance of surveilling relationships and dependencies with external parties, thus financial institutions should already be monitoring these relationships. The Enhanced Standards would require a continual process to manage these external business relationships through several key aspects, as detailed in the chart above. Similarly, the FFIEC Cybersecurity Assessment Tool requires that financial institutions[33] have a formal monitoring program in place to oversee the ongoing relationship with external parties.

One key aspect of the external relationship dependencies category involves a process to catalog and monitor all external relationships and trusted connections in real time. The Enhanced Standards propose that the Covered Entities prioritize the external relationships and trusted connections in order of importance to the business functions that the external relationships support, the Covered Entity's mission and the financial sector as a whole. This proposal is similar to the approach described in the FFIEC Cybersecurity Assessment Tool where the financial institution must diagram connections with external parties and conduct due diligence on a third-party vendor before entering into contracts with those third parties. The FFIEC Cybersecurity Assessment Tool also states that the financial institutions must conduct an annual audit of high-risk vendors. Similarly, the NIST Framework requires the an organization[34] monitor external service provider activity to detect potential cybersecurity events. However, CPMI-IOSCO Guidance is not as clear as the Enhanced Standards regarding how financial market infrastructures should monitor external parties, merely stating that it should identify and classify external dependencies.

The Enhanced Standards reference the importance of maintaining an accurate record of internal business assets and external business relationships, including: (1) mappings to other assets and other business functions, information flows, and interconnections; and (2) mappings to supported assets and business functions, respectively. Similarly, U.S. G-SIBs and other financial institutions have been engaging in comparable, extensive and difficult mapping exercises as part of their U.S. resolution planning processes.[35] The mapping process allows the Covered Entities to certify that they will be able to maintain critical services in resolution.

---

[31] Financial market infrastructures include systemically important payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories.

[32] Notice of Proposed Rulemaking, *Enhanced Cyber Risk Management Standards* (Oct. 19, 2016).

[33] FFIEC is responsible for developing uniform reporting systems for federally supervised financial institutions, their holding companies, and the nonfinancial institution subsidiaries of those institutions and holding companies.

[34] Any organization may implement the NIST Framework, not specific to financial institutions.

[35] *See* the public sections of the U.S. G-SIBs' resolution plans submitted October 1, 2016, available **here**.

Category Five: Incident Response, Cyber Resilience and Situational Awareness

All existing regulatory frameworks applicable to the financial sector address incident response. Indeed, to a large extent the ANPR is a consolidation and expansion of existing requirements and recommendations. Under the ANPR, Covered Entities would be required to undertake several steps to achieve effective incident response, cyber resilience, and situational awareness.

- First, the ANPR would require Covered Entities to establish and maintain effective incident response and cyber resilience governance, strategies and capabilities based on their enterprise-wide cyber risk management strategies and supported by appropriate policies, procedures, governance, staffing, and independent review.
    - As contemplated, this requirement would involve effective escalation protocols linked to organizational decision levels, cyber contagion containment procedures, communication strategies, and processes to incorporate lessons learned back into the program. It would also require cyber resilience strategies and exercises which consider wide-scale recovery scenarios and are designed to achieve institutional and financial sector-wide resilience, and minimize risks to or from interconnected parties. Further, Covered Entities would need to address the risk of contagion through connected systems. Recovery strategies should be designed to achieve recovery point objectives based on the criticality of the data necessary to keep the institution operational.
    - Similar requirements are reflected in existing regimes, primarily through the Security Guidelines' board of directors reporting guidance for IDIs, the NIST Framework's mandate to incorporate lessons learned into existing protocols, and the testing requirements of NIST, the FFIEC Guidance, and CPMI-IOSCO Guidance. The risks of contagion are also already addressed primarily in the CPMI-IOSCO Guidance. While the proposed or final regulations which are developed from the ANPR may ultimately require an elevated standard for this area of cyber response, financial institutions should already be implementing similar procedures in accordance with existing guidance.
- Second, the ANPR would require Covered Entities to establish and implement strategies to meet the Covered Entity's obligations for performing core business functions in the event of a disruption.
    - As contemplated, this requirement may require new compliance efforts, such as the preservation of critical records through protocols for secure, immutable, offline storage of critical records, 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. While this requirement is similar to the CPMI-IOSCO Guidance's "golden copy," whereby the Guidance suggests that Covered Entities preserve an uncorrupted version of all critical data to be used in restoring impacted systems data, the explicit discussion of the role of third parties in restoring core business functions and the need for standardized data storage standards are new additions to financial institutions' cybersecurity compliance concerns.
    - The core business function aspect of the ANPR would also require Covered Entities to maintain plans and mechanisms to transfer business, where feasible, to another financial institution or service provider with minimal disruption and within prescribed time frames if the original Covered Entity or service provider is unable to perform. The idea that a breached institution may be required to transfer business to a competitor is a new concept in cybersecurity preparations and compliance. It is, however, a core component of both resolution planning and in what happens when a financial institution either fails or exits a business line.
    - The core business function requirements would also dictate specific testing that addresses cyber events that could affect ability to service clients, and significant downtime that would

threaten the business resilience of clients. Routine testing is already required for IDIs by the Security Guidelines, and recommended for other institutions by the NIST Framework and CPMI-IOSCO Guidance. While the proposed or final rules enacted as a result of the ANPR may ultimately require an elevated standard for this area of cyber response, financial institutions should already be implementing similar procedures in accordance with existing guidance. Covered Entities would also need to test external interdependencies, such as connectivity to payment systems, clearing entities and other critical service providers, which would be undertaken jointly with codependent entities. The testing would need to validate the effectiveness of internal and external communication protocols with shareholders. Routine testing is already required for financial institutions' cybersecurity measures. The requirement for cooperation between dependent entities, however, is a new addition to financial institutions' cybersecurity compliance concerns.

- Third, the ANPR would require Covered Entities to establish and maintain ongoing situational awareness of operational status and cybersecurity posture to preempt cyber events and respond rapidly.
  - As contemplated, this requirement would involve establishing and maintaining threat profiles, threat modeling capabilities, gathering actionable cyber threat intelligence and performing security analytics on an ongoing basis; and maintaining capabilities for ongoing vulnerability management.
  - These requirements are largely covered by existing regulation, such as the FFIEC Guidance, the NIST Framework, and CPMI-IOSCO Guidance. While the proposed or final rules enacted as a result of the ANPR may ultimately require an elevated standard for this area of cyber response, financial institutions should already be implementing similar procedures in accordance with existing guidance.

As with each of the other categories, the Enhanced Standards in this category are intended by the ANPR to apply to Covered Entities' service providers as well as the Entities themselves, a sweeping enlargement of the cybersecurity compliance requirements that substantially exceeds guidance. The following chart compares the Enhanced Standards to the existing guidance currently in place as it relates to incident response, cyber resilience and situational awareness.

Required by ANPR	Required or Suggested by Existing Guidance (for some types of Financial Institutions)
Establish and maintain effective incident response and cyber resilience governance, strategies and capabilities	
Requires effective escalation protocols linked to organizational decision levels, cyber contagion containment procedures, communication strategies, and processes to incorporate lessons learned back into the program.	Largely addressed by the Security Guidelines' board of directors reporting guidance for IDIs and the NIST Framework's mandate to incorporate lessons learned into existing protocols.
Requires cyber resilience strategies and exercises which consider wide-scale recovery scenarios and are designed to achieve institutional and financial sector-wide resilience, and minimize risks to or from interconnected parties.	Similar requirements are reflected in the NIST Framework, the FFIEC Guidance, and CPMI-IOSCO Guidance, all of which require the implementation of strategies that minimize risks of contagion and operational disruption. Exercises to test cyber resilience also already recommended by FFIEC Guidance, CPMI-IOSCO Guidance and the Fundamental Elements.

Required by ANPR	Required or Suggested by Existing Guidance (for some types of Financial Institutions)
Requires Covered Entities to address the risk of contagion through connected systems. Recovery strategies should be designed to achieve recovery point objectives based on the criticality of the data necessary to keep the institution operational.	The mandate to address contagion is addressed in the CPMI-IOSCO Guidance.
Establish and implement strategies to meet the Covered Entity's obligations for performing core business functions in the event of a disruption	
Requires the preservation of critical records through protocols for secure, immutable, offline storage of these records, 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.	While similar in some respects to the concept of a "golden copy" in the CPMI-IOSCO Guidance, which recommends that institutions preserve an uncorrupted version of all critical data to be used in restoring impacted systems data, the explicit discussion of the role of third parties in restoring core business functions and the need for standardized data storage standards are new additions to financial institutions' cybersecurity concerns.
Requires Covered Entities to maintain 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.	Not previously specifically required.
Requires specific testing that addresses (i) cyber events that could affect the ability to service clients, and (ii) significant downtime that would threaten the business resilience of clients.	In general, systems testing requirements or recommendations are reflected in the NIST Framework, the FFIEC Guidance, and CPMI-IOSCO Guidance.
Requires Covered Entities to test external interdependencies, such as connectivity to markets and other critical service providers, which would be undertaken jointly with codependent entities. The testing would need to validate the effectiveness of internal and external communication protocols with shareholders.	Not previously specifically required.
Establish and maintain ongoing situational awareness of operational status and cybersecurity posture to preempt cyber events and respond rapidly	
Requires establishing and maintaining threat profiles, threat modeling capabilities, gathering actionable cyber threat intelligence and performing security analytics on an ongoing basis; and maintaining capabilities for ongoing vulnerability management.	The requirement to maintain situational awareness and to update and maintain cyber intelligence is required or recommended by FFIEC Guidance, the NIST Framework, and CPMI-IOSCO Guidance.

What Are Sector-Critical Systems?

The Agencies are considering applying more stringent "sector-critical standards" to "sector-critical systems," defined as those systems of Covered Entities that are critical to the financial sector. Any services provided by third parties that support a Covered Entity's sector-critical systems would be subject to the same sector-critical standards.

In order to identify specific sector-critical systems, the Agencies are considering a framework based on the definitions set out in the Sound Practices Paper.[36] That paper focused on level of market share and the potential systemic risk from significant disruption with respect to "firms that play significant roles in critical financial markets" although applied to the narrower context of clearance and settlement activities in wholesale financial markets.

With market share as a key factor, sector-critical systems could include the following, according to the ANPR:

- 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;
- Systems that support the clearing or settlement of at least five percent of the value of transactions (on a consistent basis) in other markets, e.g., exchange-traded and over-the-counter derivatives; and
- Systems that support the maintenance of a significant share (e.g., five percent) of total U.S. deposits or balances due from other depository institutions in the U.S.[37]

Other key factors that could be used to identify sector-critical systems include:

- ***Substitutability***: Systems that provide key functionality to the financial sector for which alternatives are limited or nonexistent, or would take excessive time to implement, such as due to incompatibility); and
- ***Interconnectedness***: Systems that act as key nodes to the financial sector due to their extensive interconnectedness to other financial entities.

The issues regarding sector-critical systems about which the Agencies seek comments include:

- Whether to have Covered Entities or the Agencies identify sector-critical systems;
- Appropriate thresholds for transaction value in critical financial markets;

[36] Fed. Reserve, OCC & SEC, Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (Apr. 8, 2003), available here.

[37] A small number of vendors provide nearly all U.S. banks with core banking software which processes deposits among other transaction types. It is conceivable that one of their systems "support[s] the maintenance of a significant share (e.g., five percent) of total U.S. deposits or balances due from other depository institutions in the U.S."

- Specific factors to consider in assessing a system's level of substitutability and interconnectedness; and
- Criteria for evaluating whether a smaller banking organization that is not otherwise subject to the Enhanced Standards should be subject to the sector-critical standards if it provides sector-critical services directly or through Covered Entities.

Standards for Sector-Critical Systems of Covered Entities

The ANPR suggests two additional stringent requirements that would apply to sector-critical systems – i.e., to systems of Covered Entities that are critical to the functioning of the financial sector. These additional requirements are:

- **State of the Art.** Covered Entities would be required to minimize residual cyber risk of sector-critical systems – i.e., substantially mitigating the risk of a disruption or failure due to a failure event – by implementing the most effective, commercially available controls.
  - The state of the art is expensive, and is always changing. This requirement would enhance operational resilience of sector-critical systems, but likely at significant cost.
  - The Agencies are also considering requiring BHCs and other Covered Entities that they would supervise to quantitatively measure compliance with this requirement, i.e., by quantitatively measuring their ability to reduce aggregate residual cyber risk of their sector-critical systems, and their ability to reduce risk to a minimal level.
- **Validated Recovery Time Objective ("RTO") of Two Hours.** Covered Entities would be required to establish an RTO of two hours for sector-critical systems to recover from a disruptive, corruptive or destructive cyber event.
  - **Testing Program Required.** The RTO would be required to be validated by a testing program that includes a range of severe but plausible scenarios and would "challenge" areas such as communications protocols, governance arrangement and resumption and recovery practices.
  - This requirement is largely consistent with the Sound Practices Paper recommendation that core clearing and settlement organizations have an RTO of two hours, but under the ANPR would apply more broadly to all sector-critical systems. The Sound Practices Paper notes that firms that play significant roles in the critical financial markets should assume that core clearing and settlement organizations that they rely on will recover and resume operations within the business day of the disruption, and the firms themselves should recover as soon as possible but certainly within the business day on which as disruption occurs. The Sound Practices Paper goes on to note that in some markets, such as wholesale payments, long-established RTO benchmarks were two hours. Thus, the ANPR's approach represents a significant ratchet of how fast recovery should be expected, and who is covered. The ANPR indicates that a broad two hour RTO may be appropriate because of advances in technology.

The ANPR notes that, consistent with its approach to other services, any services provided by third parties supporting a Covered Entity's sector-critical systems would also be subject to the same standards as the sector-critical firm itself.

The sector-critical standards impose substantially greater obligations than the Enhanced Standards. Given the nature of the entities that could be deemed to provide sector-critical systems, the sector-critical standards could become the *de facto* standard for all financial institutions.

Consistent Repeatable Methodology

The ANPR states that the Agencies are "seeking to develop a consistent, repeatable methodology to support the ongoing measurement of cyber risk within Covered Entities." Although the ANPR points out several methodologies to measure cyber risk for the financial sector, such as the FAIR Institute's Factor Analysis of Information Risk standard and Carnegie Mellon's Goal-Question-Indicator-Metric process, it notes that "the [A]gencies are not aware of any consistent methodologies to measure cyber risk across the financial sector using specific cyber risk management objectives."

Conclusion

Financial institutions that would be Covered Entities, bank vendors and small financial institutions should consider whether the Enhanced Standards, including the sector-critical standards, would substantially raise compliance and operational costs. By increasing the costs to vendors to serve large financial institutions, costs will increase for small banks too. Many issues and details are left underspecified or open in the ANPR – the Agencies would benefit greatly from comments submitted by knowledgeable industry participants, who are in some cases better positioned than the Agencies to know which requirements would strike an appropriate balance between the important goal of protecting the resilience of our financial system, on the one hand, and allowing banks and other financial institutions to effectively serve their current clients while continuing to innovate and find ways to provide services to underserved individuals, businesses and markets.

Davis Polk

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

John L. Douglas	**202 962 7126**	**john.douglas@davispolk.com**
Avi Gesser	**212 450 4181**	**avi.gesser@davispolk.com**
Reuben Grinberg	**212 450 4967**	**reuben.grinberg@davispolk.com**
Joseph Kniaz	**202 962 7036**	**joseph.kniaz@davispolk.com**
Jon Leibowitz	**202 962 7050**	**jon.leibowitz@davispolk.com**
Jennifer E. Kerslake	**212 450 6259**	**jennifer.kerslake@davispolk.com**
Neil H. MacBride	**202 962 7030**	**neil.macbride@davispolk.com**
Gabriel D. Rosenberg	**212 450 4537**	**gabriel.rosenberg@davispolk.com**
Margaret E. Tahyar	**212 450 4379**	**margaret.tahyar@davispolk.com**