



February 17, 2017

**By Electronic Mail** ([regs.comments@federalreserve.gov](mailto:regs.comments@federalreserve.gov), [regs.comments@occ.treas.gov](mailto:regs.comments@occ.treas.gov),  
[Comments@fdic.gov](mailto:Comments@fdic.gov))

Robert deV. Frierson  
Secretary  
Board of Governors of the Federal Reserve System  
20<sup>th</sup> Street and Constitution Avenue NW  
Washington, DC 20551

Legislative and Regulatory Activities Division  
Office of the Comptroller of the Currency  
400 7<sup>th</sup> Street, SW, suite 3E-218, mail stop 9W-11  
Washington, DC 20219

Robert E. Feldman  
Executive Secretary  
Attn: Comments, Federal Deposit Insurance Corporation  
550 17<sup>th</sup> Street, NW  
Washington, DC 20429

**Re: Response to Enhanced Cyber Risk Management Standards, (Fed) Docket No. R-1550 and RIN 7100-AE61, (OCC) Docket ID OCC-2016-0016, (FDIC) RIN 3064-AE45**

Dear Sirs and Madams:

On behalf of the Securities Industry and Financial Markets Association (“SIFMA”),<sup>1</sup> American Bankers Association (“ABA”), and Institute of International Bankers (“IIB”), we appreciate the opportunity to submit this comment letter to the Board of Governors of the Federal Reserve System (“Fed”), the Office of the Comptroller of the Currency (“OCC”), and the Federal Deposit Insurance Corporation (“FDIC”) (collectively, “the Agencies”) in connection with their joint advance notice of proposed rulemaking (“ANPR”) on Enhanced Cyber Risk

---

<sup>1</sup> SIFMA is the voice of the U.S. securities industry. We represent the broker-dealers, banks and asset managers whose nearly 1 million employees provide access to the capital markets, raising over \$2.5 trillion for businesses and municipalities in the U.S., serving clients with over \$20 trillion in assets and managing more than \$67 trillion in assets for individual and institutional clients including mutual funds and retirement plans. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (“GFMA”). For more information, visit <http://www.sifma.org>.

Management Standards on October 26, 2016.<sup>2</sup> We commend the Agencies in their efforts to strengthen and improve cybersecurity in the financial sector, and we look forward to working with the Agencies to improve cybersecurity protections. We particularly appreciate your efforts to coordinate so that regulated entities are not subject to potentially conflicting or redundant obligations that could diffuse resources and focus.

We respectfully request that any rule resulting from the ANPR should (a) determine the application of requirements based on risk in addition to entity size; (b) use a risk-based approach and avoid imposing prescriptive and one-size-fits-all requirements; and (c) be harmonized and reconciled with existing cybersecurity frameworks and regulations. We believe the approach we recommend in this comment letter will best enable the financial industry and the Agencies to continue their coordinated efforts to mitigate cybersecurity risks most effectively and efficiently.

\* \* \*

Cybersecurity is a top priority for the financial industry. Financial institutions dedicate significant resources every day toward defensive measures designed to protect against cyber crime, safeguard consumer data, and maintain the integrity and resiliency of their systems in the face of countless cyber threats. These defensive measures include developing information security plans, training employees, hiring experts to conduct risk assessments, and deploying defensive software and other technology solutions. Financial institutions also dedicate a significant amount of time and resources toward compliance with an expanding, and often overlapping, set of cybersecurity regulations. Firms report that approximately 40 percent of corporate cybersecurity activities—which can include investments as high as \$500 million per year for the largest firms—are compliance-oriented rather than security-oriented.<sup>3</sup> In other words, substantial resources are already being invested in complying with regulatory requirements rather than directly targeting security risks.

SIFMA, ABA, and IIB have taken a leading role in coordinating the industry’s response to the operational and regulatory demands of cybersecurity, encouraging the adoption of core principles and practices that are risk-based and harmonized across the regulatory environment. The NIST Cybersecurity Framework,<sup>4</sup> developed as a result of Executive Order No. 13636 with the participation of over 3,000 cybersecurity professionals, is the hallmark of these efforts and represents the cybersecurity field’s consensus on the most effective approach to improve cybersecurity.<sup>5</sup> Financial institutions have already designed cybersecurity programs to align with the NIST Cybersecurity Framework or other voluntary frameworks and comply with the Federal Financial Institutions Examination Council’s (“FFIEC”) Cybersecurity Assessment Tool

---

<sup>2</sup> Office of the Comptroller of the Currency, Federal Reserve System, and the Federal Deposit Insurance Corporation, *Enhanced Cyber Risk Management Standards*, 81 Fed. Reg. 74315 (Oct. 26, 2016) (hereinafter, the “ANPR”).

<sup>3</sup> See PwC, *Global State of Information Security Survey 2016* (Oct. 9, 2015), <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html>.

<sup>4</sup> Nat’l Inst. of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014) (“NIST Framework”), <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>.

<sup>5</sup> See Executive Order – Improving Critical Infrastructure Cybersecurity, E.O. 13636 (Feb. 12, 2013).

(“CAT”) and cybersecurity regulations promulgated under the Gramm-Leach-Bliley Act (“GLBA”), which also adopt risk-based approaches to cybersecurity.

The Agencies’ ANPR risks undermining the cybersecurity efforts of financial institutions by failing to fully recognize extensive efforts that firms have already made to implement risk-based approaches such as the NIST Cybersecurity Framework and existing federal requirements. The ANPR proposes several standards which are prescriptive rather than risk-based, including applying the ANPR to entities with \$50 billion in assets (regardless of risk); establishing a specific recovery time objective (“RTO”) of two hours for certain systems; prescribing specific allocations of responsibility for different lines of risk management; and requiring offline storage and restoration of critical records. We request that any final rule issued by the Agencies adopt a risk-based approach consistent with the approach adopted by voluntary frameworks such as the NIST Cybersecurity Framework and further elaborated in the FFIEC CAT, setting control objectives rather than prescriptive requirements. A risk-based approach consistent with these pre-existing frameworks will allow financial institutions to leverage existing programs and investments to comply with the cybersecurity requirements of the Agencies and other regulators.

We further request that the Agencies avoid imposing impractical and technically infeasible requirements. As explained below, the ANPR’s requirement of an RTO of two hours for sector-critical systems is not technically feasible and might have the unintended consequence of restoring a system to operation before the nature of the threat or the effects of the event have been fully understood and remediated. Firms already have financial and operational pressure to restore systems as quickly as possible to ensure that the effects of an attack cause the least amount of business impact and financial damage. This example, as well as others described below, demonstrates why an overly-prescriptive approach may not strengthen cybersecurity.

Additionally, the Agencies propose multiple requirements for covered entities to consider risk to the sector as a whole. Determining risk to the sector may be difficult for covered entities without visibility into different aspects of the sector or third parties. We believe that the Agencies can facilitate the creation of a stronger cybersecurity environment for the financial industry by coordinating with us on these important issues.

#### **A. The Scope Of The ANPR Should Focus On Risk In Addition To Size**

Application of the enhanced standards considered in the ANPR should be based on the potential for a cyber incident to impact the safety and soundness of the financial sector as a whole. Although the size of an institution is one factor in that analysis, we propose that the scope of the ANPR be revised to consider other risk factors, including the critical business functions that the entity is responsible for and the importance of these activities relative to the overall market. Any final rule relating to these in-scope requirements will be greatly enhanced by the adoption of a risk-based approach. Additionally, we request greater clarity from the Agencies on the mechanism they will use to apply the enhanced standards to third parties.

##### **1. Entity Size**

Generally, the Agencies are considering applying the enhanced standards of the ANPR to entities subject to their jurisdiction with total consolidated assets of \$50 billion or more on an

enterprise-wide basis. The Agencies explain that “[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.” We recognize that the \$50 billion designation aligns with regulations issued by the Fed to designate systemically important financial institutions under the Dodd-Frank Act.<sup>6</sup> But size should not be the only determinative factor.

We request that the Agencies consider a more flexible, risk-based standard that considers the potential for a cyber incident to impact the sector more broadly, taking into account the critical business functions performed by the entity or the size of the institution relative to the market. While many institutions meeting the \$50 billion threshold are likely to impact the safety and soundness of the financial sector as a whole, arbitrary measures of size are likely to impact smaller regional banks and credit unions which do not represent the same overall risk based on participation in key markets, delivery of important functions, and impact to the U.S. economy if they were unable to operate for a period of time. On the other hand, the financial sector is dependent upon other critical actors that may not reach the \$50 billion threshold, as the Agencies recognized by considering applying the standards to financial market utilities designated by the Financial Stability Oversight Council (“FSOC”) and covered by guidance on cyber resilience issued by the Committee on Payments and Market Infrastructures (“CPMI”) and the International Organization of Securities Commissions (“IOSCO”).<sup>7</sup>

As a potential alternative, a relative figure (such as five percent of a critical market) or a role-based determination (for example, applying to primary dealers or organizations providing sector-critical services) would provide a more useful standard that more accurately accounts for risk to the financial sector.

Moreover, the proposed standards should implement a risk-based standard that focuses on critical business functions and exempts enterprise systems<sup>8</sup> that do not affect a critical function of the covered entity. Such a risk-based approach would ensure that firms target resources consistent with the degree of risk. Without this revision, the proposed standards would require a substantial investment of time, resources, and personnel to apply the standards to all enterprise systems, regardless of the nature of the system, its particular risks, or its impact on the financial operations of the enterprise. For example, a large national bank’s derivatives trading operation might be critical, but applying the same standards to an enterprise system governing a non-critical facility would not be an efficient allocation of resources. Additionally, foreign banking entities should not be required to apply the standards to branches located outside of the United States that do not affect a critical function of the covered entity. We request that the Agencies tailor the scope of application to enterprise systems based on an assessment of their risk to a critical function.

---

<sup>6</sup> Federal Reserve System, *Enhanced Prudential Standards for Bank Holding Companies and Foreign Banking Organizations*, 12 C.F.R. pt. 252, <https://www.gpo.gov/fdsys/pkg/FR-2014-03-27/pdf/2014-05699.pdf>.

<sup>7</sup> CPMI and IOSCO, *Guidance on cyber resilience for financial market infrastructures* (June 2016), <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf>.

<sup>8</sup> We recommend that the Agencies define “systems” as the interconnected IT assets that perform a critical function, in recognition of the fact that individual IT assets within a system may fail without taking down the system or eliminating the system’s ability to perform its function.

In suggesting an alternative standard, we note the recent move by lawmakers in the House of Representatives to replace the \$50 billion benchmark of Dodd-Frank with a standard that considers size as one of a broader set of risk factors, authorizing the Financial Stability Oversight Council (“FSOC”) to make a final risk determination based on a consideration of several factors, including size, interconnectedness, the extent of readily available substitutes, global cross-jurisdictional activity of the entity, and the complexity of the entity.<sup>9</sup> We request that the Agencies join with the industry to identify risk factors that warrant consideration in the development of a more risk-based standard.

## 2. Third Parties

The Agencies are considering applying cybersecurity standards for third-party service providers. Financial institutions are keenly aware of the need to manage the risks, including cybersecurity risks, of using third-party service providers. These relationships are diverse and complex, driven by business needs and market forces. The financial sector is not the exclusive market for many of these service providers, and any application of requirements must consider other sectors and stakeholders. Without a risk-based approach to these relationships, regulations regarding the use of third-party service providers may be infeasible or lead to worse cybersecurity outcomes.

We request additional clarity on the mechanism that the Agencies would use to apply the enhanced standards directly to third parties and which third parties the Agencies intend to include in the scope of the proposed standards. It is important that the Agencies ensure that financial institutions are not responsible for addressing cybersecurity threats across all sectors, which would not appropriately account for cybersecurity risk elsewhere in the supply chain and lead to a disproportionate allocation of costs. We encourage the Agencies to work with other governmental actors to identify third and fourth parties that provide services that may have a critical impact on critical sector functions and develop appropriate strategies to mitigate those risks. Direct application of heightened standards to such critical service providers may assist financial institutions in prioritizing their resources based upon cyber risk to the entity. But the potential benefits should be considered in light of competing considerations, including the impact of such regulation on innovation, cost, technical flexibility, and the efficiency of decentralized risk management. In our view, there are equally effective alternative methods, outlined below, to seek assurances that resiliency activities are being addressed by critical third- and fourth-party service providers across the sector.

An effective approach could include coordination between the Agencies and other regulatory bodies to promote global use of a recognized framework, such as the NIST Cybersecurity Framework, in order to improve minimum standards of cybersecurity risk management across the economy. There has also been significant international coordination around a set of global regulatory standards for regulating cybersecurity.<sup>10</sup> This coordinated

---

<sup>9</sup> *Systemic Risk Designation Improvement Act of 2016*, H.R. 6392 – 114<sup>th</sup> Congress (passed the House on Dec. 12, 2016).

<sup>10</sup> For example, G-7 nations developed and released a set of voluntary guidelines for the financial sector. See *G7 Fundamental Elements of Cybersecurity for the Financial Sector*, available at [https://www.ecb.europa.eu/paym/pol/shared/pdf/G7\\_Fundamental\\_Elements\\_Oct\\_2016.pdf?69e99441d6f2f131719a9cada3ca56a5](https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf?69e99441d6f2f131719a9cada3ca56a5).

approach might also create greater synergy between sectors by taking advantage of the unique defensive positions of different economic actors. For example, supporting and facilitating telecommunications companies to proactively shut down malicious traffic before it reaches individual company networks would allow financial institutions to focus greater resources on cyber risks specific to the financial sector.

To the extent that the Agencies seek to apply new standards through required contractual language between covered entities and third parties, we remind the agencies that existing vendor oversight requirements have already been addressed by Appendix J of the FFIEC IT Examination Handbook, as discussed below. Existing requirements, including vendor due diligence and requirements to manage vendor cyber risk based on access to critical systems, are robust and appropriately focus on both business and cyber risks. Any requirements for the application of standards through contractual relationships should be carefully scoped and recognize best practices for risk management. This includes ensuring that the standards take into account pre-existing frameworks, that they apply only to third- or fourth-party service providers that are directly interconnected with risk to sector-critical systems, and that they be limited to requiring the covered entity to have procedures in place to receive pre-contract and post-engagement assurance from the third parties of their compliance.

### **3. Sector-Critical Designation**

The Agencies are considering applying a higher set of standards referred to as “sector-critical standards” to systems of covered entities that are critical to the financial sector. As discussed below in Section C (*infra* p. 12), there are several existing frameworks that already identify and apply a higher set of standards to sector-critical systems, and we request that the Agencies work to harmonize their proposal with these frameworks.

Beyond the potential for overlap or conflict with pre-existing sector-critical designations, the ANPR introduces significant uncertainties with its proposal of a two-tiered system. Without a clearer understanding of the scope of systems to be included in the designation of “sector-critical,” it is difficult to evaluate the effects of imposing the higher set of standards. Consequently, we request further clarification from the Agencies on definitions of key terms that will impact the scope of the “sector-critical” designation, including such terms as “financial sector,” “sector partners,” “widespread,” “critical business functions,” “key functionality,” and “core business functions.” Additionally, we request that the Agencies further collaborate and consult with sector-wide organizations to determine how third- and fourth-party sector-critical systems should be designated.

#### **B. The ANPR Should Use A Risk-Based Approach And Avoid Prescriptive Requirements**

The financial institutions covered by the ANPR have well-developed cybersecurity programs that have been designed to conform to the risk-based requirements established by federal law. We urge the Agencies to adopt a risk-based approach that builds on the NIST Cybersecurity Framework, the International Organization for Standardization’s (“ISO”) risk-based standards, and current federal requirements, all of which provide appropriate flexibility to

focus on better cybersecurity outcomes rather than compliance activities.<sup>11</sup> Financial institutions should have the flexibility to achieve risk reduction objectives through the implementation of controls that are best suited to minimize firms' specific risk exposures.

In contrast to existing federal requirements and prevailing industry standards, the ANPR contains prescriptive standards requiring specific actions. We request that the Agencies revise the ANPR to incorporate a risk-based approach in the following ways: by replacing the potentially counterproductive RTO time limit with a standard that requires resumption of service to meet contractual and regulatory obligations within a prompt, reasonable, and safe time period; by preserving the ability of boards of directors to use outside cyber expertise; by allowing flexibility in firms' allocation of cyber risk management responsibilities within the organization; by setting dependency management objectives focused on prioritization of critical systems and assets; by harmonizing the ANPR with existing industry initiatives regarding the offline storage and restoration of critical records; and by avoiding any impractical quantification of cyber risk or requirement of "most effective" commercially available controls.

### **1. RTO and Other Recovery Protocols**

The Agencies consider imposing a sector-critical standard requiring covered entities to establish an RTO of two hours for their sector-critical systems. We fully recognize the importance of resumption of service to an institution's resiliency program, but we respectfully submit that requiring sector-critical systems to return to operations within two hours for all possible scenarios is both technically infeasible and impractical as a security matter. In the cybersecurity context, the technical capability of a firm to restore a system to operations, and the time frame for doing so, varies greatly depending on the nature of the attack and the size and complexity of the system. Moreover, unlike kinetic disruptions (such as a loss of power, loss of location, etc.), which as a technical matter are immediately apparent and are limited to a defined sphere, cybersecurity attacks are often difficult to detect or diagnose and frequently pose a risk of contagion to other systems or the market at large. Additional time is required for investigating the actual cause of the operational impact and then testing and validating systems after the attack to ensure that the systems are ready for safe operation. There will inevitably be circumstances where a safe and secure recovery from a cyber attack will not be technically feasible within a two hour period, or even desirable, depending on the nature of the threat.

---

<sup>11</sup> As a general matter, we support the goals represented in the enhanced cyber risk management standards. We believe, however, that further collaboration and consultation with sector-wide organizations is necessary in order to obtain perspectives on sector risks that are not available to individual financial institutions. The Agencies, for example, should coordinate closely with sector-wide organizations focused on systemic risk and resiliency to provide analysis and recommendations on what systems should be considered "system critical" prior to expanding the definition of sector-critical systems. Additionally, to the extent that any final rule resulting from the ANPR includes requirements to conduct exercises with third-party suppliers, we encourage the Agencies to consider the creation of a central authority, or the exercise of such authority by the Agencies themselves, to coordinate exercises between financial institutions and financial market infrastructures. The Bank of Canada Joint Operational Resilience Management (JORM) program provides a useful model for coordinating tabletop exercises to test the capabilities of both the private and public sectors in the event of a crisis affecting the financial sector. See Harold Gallagher, Wade McMahon, and Ron Morrow, *Cyber Security: Protecting the Resilience of Canada's Financial System* (December 2014), <http://www.bankofcanada.ca/wp-content/uploads/2014/12/fsr-december14-morrow.pdf>.

A two-hour RTO requirement also creates immense practical difficulties. Cyber attacks come in almost infinite variety, and the precise nature of all threats facing a firm cannot be anticipated. Cyber events are often accompanied by many unknowns (e.g., have transactions been authorized?; has data been manipulated?; can utilities and other infrastructure be trusted?; has malware been contained?). As a consequence, establishing protocols in advance to ensure a two-hour recovery raises insurmountable practical difficulties. It would be challenging as a practical matter to define the starting point for measuring the two-hour RTO when the precise beginning point of a cyber event is obscure or recurring, or when the objective of the attack is unclear. As acknowledged in the recently issued NIST Guide for Cybersecurity Event Recovery, “full recovery or restoration may not be the immediate goal,” and the timing of the decision to initiate recovery processes should account for the need to “achieve[] key understandings of the adversary’s footprint and objectives” in order to avoid triggering a change in the attacker’s tactics or reducing the firm’s ability to discover impacted resources.<sup>12</sup>

In recognition of the fact that firms already have financial and operational pressure to restore systems as quickly as possible to ensure that the effects of an attack cause the least amount of business impact and financial damage, we request that the Agencies remove the RTO requirement altogether from the proposed standards. Rather than establishing arbitrary RTO time limits for specific systems, we recommend a more practical and feasible approach which focuses more broadly on resumption of service, measured by the entity’s best efforts to ensure the ability to safely meet contractual and regulatory service obligations. This approach would allow the entity to use appropriate means to restore access to critical services in a prudent manner, taking necessary steps to address risks to particular systems that accompany a cyber attack.<sup>13</sup> Any final rule resulting from the ANPR should emphasize safe recovery and limiting contagion rather than speed of recovery, and the rule should avoid imposing a requirement that is both impractical and technically infeasible.

## **2. Cyber Risk Governance – Board Cybersecurity Expertise**

The Agencies consider requiring the board of directors to have adequate expertise in cybersecurity or to maintain access to resources or staff with such expertise. We agree that financial institutions should establish processes to ensure that the board of directors is actively engaged in establishing and reviewing the firm’s risk profile. It is also important that boards have access to internal, external, and independent experts to ensure that the board adequately understands cybersecurity risks. But the composition of a board should be driven not by a specific skill set but by the overall experience of each member and the combination of experience across the board. Additionally, prescriptive requirements that a board approve specific policies and procedures may lead to unnecessary rigidity or interference with the board’s evaluation of the best method to supervise the firm’s management of cybersecurity risk.

---

<sup>12</sup> Nat’l Inst. of Standards and Technology, *Guide for Cybersecurity Event Recovery* (December 2016), Section 2.3.3, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf>.

<sup>13</sup> We encourage the Agencies to work with the sector to create alternative solutions to ensure that the most critical functions are enabled in the time of a crisis and that firms are able to maintain at least a minimal level of operations.



We therefore request that the Agencies avoid a rule that would interfere with the board's independence, composition, or ability to determine what is in the best interest of the firm.<sup>14</sup> We recommend that any final rule issued by the Agencies be consistent with the rule in the OCC's "Heightened Standards" that the board of directors should provide "credible challenges" to management's recommendations and decisions.<sup>15</sup> Consistent with that end, any final rule should also preserve the ability of the board to seek out and rely on outside expertise, as recommended and permitted in the FFIEC Audit IT Examination Handbook.<sup>16</sup>

### 3. Three Independent Functions of Cyber Risk Management

The Agencies consider requiring covered entities—"to the greatest extent possible and consistent with [firms'] organizational structure"—to integrate cyber risk management into the responsibilities of at least three independent functions. Firms are already required to assess risks under the Interagency Guidelines,<sup>17</sup> and many covered firms have already developed a risk management model using three independent lines of defense in accordance with the OCC Heightened Standards.<sup>18</sup> It is important to provide flexibility, as the OCC Heightened Standards do, in developing these three lines of defense and defining their roles and responsibilities, especially in the area of cyber risk.

The ANPR, however, includes language which indicates that the Agencies are considering prescriptive constraints on the functions of the three lines of defense. For example, the Agencies are considering requiring the audit plan "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." It is not clear by what metric a firm's internal audit function could evaluate the business unit's adaptability. Deciding when and how "to adapt" is a complex business judgment requiring evaluation of a broad range of business needs, impacts, and issues beyond the scope of an internal audit. We request that any final rule be revised to eliminate any requirement that a firm's internal audit function evaluate the business unit's or management's capabilities to adapt and remain in compliance with an approved risk management framework.

We recommend that the Agencies take a broad approach to cyber risk management that preserves necessary flexibility in defining the roles and responsibilities of the firm's three lines of defense. Due to the limited supply of qualified cybersecurity talent in the market, such an

---

<sup>14</sup> To allow firms to leverage global functions, we also recommend that the Agencies clarify in any final rule that wherever approval is required from the board or an appropriate committee thereof, the requirement may be satisfied by obtaining approval from the board or appropriate committee of any of the covered entity's parent companies.

<sup>15</sup> OCC, *OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations*, 12 C.F.R. pts. 30 and 170, at III.B., <https://www.occ.gov/news-issuances/news-releases/2014/nr-occ-2014-117a.pdf> (hereinafter "OCC Heightened Standards").

<sup>16</sup> FFIEC, *Audit IT Examination Handbook*, Objective 3, at A-2, <http://ithandbook.ffiec.gov/it-booklets/audit/appendix-a-examination-procedures.aspx>.

<sup>17</sup> Interagency Guidelines, 12 C.F.R. pt. 364, at III.B.

<sup>18</sup> OCC Heightened Standards, 12 C.F.R. pts. 30 and 170, at II.C., <https://www.occ.gov/news-issuances/news-releases/2014/nr-occ-2014-117a.pdf>.

approach should allow business units to rely on the cybersecurity expertise of professionals outside of the business unit where necessary. Moreover, when establishing a functioning three lines of defense model, financial institutions must take into account multiple types of risk, including cyber risk. These institutions have made significant strides in restructuring their unique organizations to address different types of risk under the three lines of defense model, and we request that the Agencies avoid causing unnecessary disruption by dictating a new and more restrictive organizational construct for addressing cyber risk alone. Firms should be allowed to adapt resources to the organization's risk profile.

#### **4. Internal Dependency Management**

The Agencies have proposed a requirement 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,” and that they “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.” Managing internal dependencies and maintaining an inventory of critical assets are important elements of cyber risk management. For global entities, identifying these dependencies and assets, understanding the extent of their impact, and developing a contingency plan to address potential loss of the supporting system is not a trivial undertaking. A requirement to identify and map all dependencies, connections, data flows, and business assets, not all of which are critical to the sector or material to the continuing operation of the firm, would be a resource-intensive project requiring substantial financial outlay and potentially pull valuable human resources away from their primary operational security duties. Such a broad and unfocused requirement would detract from a focus on the most serious and critical needs. Similarly, a requirement to assess the cyber risks and potential vulnerabilities associated with every business asset, service, and IT connection point for every business unit would draw important resources away from focusing on risks to critical systems.

Instead of such a broad standard, we request that the Agencies consider a risk-based approach that focuses on the interconnection of business assets and internal dependencies with risk to sector-critical systems and allows firms to determine the appropriate scope of risk assessments. While continuous monitoring of some systems and internal dependencies may be appropriate depending on their risk level and criticality to the entity’s continued operation, firms should be permitted to determine the appropriate level of monitoring required for other non-critical assets and internal dependencies. A prescriptive standard that requires detailed processes, mapping, and assessments for non-critical assets and dependencies, without regard for risk to the entity, will draw limited time and resources away from the goal of reducing systemic risk to the financial sector.

#### **5. External Dependency Management**

Similar to internal dependencies and business assets, covered entities should take a risk-based approach to managing external dependencies. Requiring covered entities to maintain a “current, accurate, and complete listing of all external dependencies and business functions, including mappings to supported assets and business functions” would not appreciably reduce risk and would redirect resources away from security operations toward compliance exercises.

The Agencies have also taken an overly prescriptive approach in requiring covered entities to identify and periodically test alternative solutions in case an external partner fails to perform as expected, without regard for the risk entailed in the function provided by the external dependency.<sup>19</sup>

We recognize the value of contingency planning for external dependencies, but we believe that alternative approaches should be more risk-based and more efficient. In place of a requirement that covered entities conduct alternative testing, we request that the Agencies consider the creation of a sector-specific approval or certification process for service providers, allowing third-party (and fourth-party) providers to demonstrate that they are incorporating sector-specific risk management processes and procedures into their own environments. Beyond such minimum certification standards, and with regard to individual third-party relationships, firms should be permitted to focus their efforts to reduce the risks associated with external dependencies based on individual risk assessments. For third parties that are interconnected with risk to sector-critical systems, the Agencies should consider a requirement that the third party and the covered entity define alternatives in case of their inability to meet service-level agreements due to a cyber incident. To the extent that alternative testing and mapping of external dependencies is necessary, we request that the requirement be limited to those external dependencies interconnected with risk to sector-critical systems.

We also note that monitoring all external dependencies in real time is not feasible as a practical matter. Some external dependencies, such as water, electricity, or telecommunications providers, are critical infrastructures subject to their own standards. For many external dependencies, it may not be possible to effectively monitor them at all, whether “in real time” or otherwise. To the extent that any final rule includes requirements to monitor external dependencies, we request that the Agencies revise the rule to require firms to apply measures to promptly receive alerts from external dependencies that are interconnected with risk to sector-critical systems.

## **6. Offline Storage and Restoration of Critical Records**

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.

The industry is moving forward with a voluntary effort to create the capability to preserve critical records in case of a cyber event and to enhance resiliency for financial institutions’ customer accounts and data. The focus of this effort is to extend the industry’s capabilities to securely store and restore account data should the need arise, and it is an additional layer of

---

<sup>19</sup> The Agencies should also take into account industry-level continuity of operations plans that are already in place, such as the ability of banks to re-route transactions through FedWire in the event that the Clearing House Interbank Payments Systems (“CHIPS”) were unavailable.

protection on top of existing defenses that many financial firms utilize. Industry efforts have moved rapidly in the last year to develop voluntary standards for data formats, data encryption, and data vaults that would enable restoration of retail customer account data at another financial institution after a major incident.

Given the complexity of this undertaking, we request that the Agencies not impose specific requirements for the offline storage and restoration of critical records, other than acknowledging that covered entities should consider what recovery methods are appropriate for their operations in light of developing industry standards, until the industry has more fully developed a practical way to conform with such a requirement.

## **7. Quantifying Cyber Risk and Effective Controls**

Some language in the ANPR suggested that the Agencies are considering imposing requirements that rely on a quantification of cybersecurity risk. For example, the Agencies declared an intention to “develop a consistent, repeatable methodology to support the ongoing measurement of cyber risk within covered entities.” Although we agree with the Agencies in principle on the potential benefits of such a methodology, it is difficult in practice to develop a method for quantifying cyber risk, whether within an individual financial institution or (even more so) across the entire financial sector. We urge the Agencies to avoid “baking in” a rigid quantification of cyber risk as they develop the standards being considered in the ANPR. This includes avoiding specific threat identification and modeling requirements that do not account for the inherent unpredictability and varied nature of cyber threats.

For a similar reason, we request that the Agencies avoid any rule that requires the adoption of the “most effective commercially available controls,” which limits flexibility and could require unreasonable controls for limited risks or risks that are otherwise controlled or mitigated. Such a standard would also raise questions about how the effectiveness of such controls should be measured. A broader, more holistic approach that focuses on risk management and mitigation is more consistent with the reality of cyber risk and variety of consequences that may potentially result from a cyber event. Covered entities should be allowed to adapt their environments to the needs of their business, improving their risk management and mitigation processes according to an evolving threat landscape.

### **C. The ANPR Should Complement Existing Cybersecurity Frameworks And Regulations**

As the Agencies are aware, financial institutions are subject to numerous cybersecurity requirements from several regulatory bodies of overlapping jurisdiction. In addition to regulations from the Agencies issuing the ANPR,<sup>20</sup> other regulatory bodies with jurisdiction over

---

<sup>20</sup> For the FDIC: Enforcing Federal Deposit Insurance Act and Federal Deposit Insurance Corporation Improvement Act, codified at 12 U.S.C. §§ 1811–1835a; Bank Service Company Act, 12 U.S.C. § 1861 *et seq.*; Interagency Guidelines, 12 C.F.R. pt. 364, App. B; Cybersecurity Awareness Resources (including Cyber Challenge Announcement), FIL-55-2015; Technology Outsourcing: Informational Tools for Community Bankers, FIL-13-2014; Clarifying Supervisory Approach to Institutions Establishing Account Relationships with Third-Party Payment Processors, FIL-41-2014; Pre-Employment Background Screening Guidance on Developing an Effective Pre-Employment Background Screening Process, FIL-46-2005; Final Guidance on Response Programs Guidance on

financial institutions have issued cybersecurity regulations, including the Commodity Futures Trading Commission (“CFTC”),<sup>21</sup> the Securities and Exchange Commission (“SEC”),<sup>22</sup> the Federal Trade Commission (“FTC”),<sup>23</sup> the National Credit Union Administration (“NCUA”),<sup>24</sup> the Financial Industry Regulatory Authority (“FINRA”),<sup>25</sup> and the National Futures Association (“NFA”),<sup>26</sup> not to mention requirements and guidelines at the international and state levels.<sup>27</sup>

The Agencies acknowledge that extensive efforts have already been made to coordinate existing cybersecurity regulations and requirements. The Agencies issuing the ANPR are members of FFIEC, which has been empowered to develop uniform guidance and has promulgated CAT to guide both regulators and industry in establishing and maintaining comprehensive cybersecurity protections at financial institutions.<sup>28</sup> In addition to the CAT, FFIEC has developed and published comprehensive guidelines, such as the IT Examination Handbook, to provide detailed guidance on cybersecurity protections.<sup>29</sup> The Fed, the OCC, and the SEC jointly issued the Interagency White Paper to address the functions supporting critical financial markets.<sup>30</sup> Regulations have also been issued under the GLBA<sup>31</sup> to set uniform requirements for entities regulated by the SEC, FDIC, Fed, OCC, and other agencies with respect to the development and maintenance of a comprehensive information security program, including the “Safeguards Rules” promulgated by the FTC,<sup>32</sup> NCUA,<sup>33</sup> and the SEC.<sup>34</sup> At the international level, the Finance Ministers of G-7 nations recently developed and released a set of

---

Response Programs for Unauthorized Access to Customer Information and Customer, FIL-27-2005; Supervisory Policy on Identity Theft, FIL-32-2007.

<sup>21</sup> Enforcing Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.*; Commodities Exchange Act, 7 U.S.C. § 7b-2; CFTC Safeguards Rule, 17 C.F.R. § 160.30; Risk Management Program Rule, 17 C.F.R. § 23.600; CFTC Staff Advisory No. 14-21, Best Practices Memo; DCO Cybersecurity Rule, 80 Fed. Reg. 80114-01; System Safeguards Rule, 80 Fed. Reg. 80140-01.

<sup>22</sup> Enforcing Securities Act of 1933, 15 U.S.C. § 77a *et seq.*; Securities Exchange Act of 1934, 15 U.S.C. § 78a *et seq.*; Sarbanes-Oxley Act, Pub. L. No. 107-2014, 116 Stat. 745; Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.*; Regulation S-P, 17 C.F.R. § 248.30; Regulation SCI, 17 C.F.R. §§ 242.1000–1007; OCIE’s 2015 Cybersecurity Examination Initiative (Sept. 15, 2015); OCIE’s Cybersecurity Examination Sweep Summary (Feb. 3, 2015); OCIE’s Cybersecurity Initiative (Apr. 15, 2014).

<sup>23</sup> Enforcing Federal Trade Commission Act, 15 U.S.C. § 45; Gramm-Leach-Bliley, 15 U.S.C. §§ 6801–6809; Safeguards Rule, 16 C.F.R. pt. 314; Identity Theft Rule, 16 C.F.R. pt. 681.

<sup>24</sup> Enforcing Federal Credit Union Act, 12 U.S.C. §§ 1751–1795k; Interagency Guidelines, 12 C.F.R. 748, App. A; Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice (Adoption of the Interagency Guidelines with slight modifications), 12 C.F.R. pt. 748, App. B.

<sup>25</sup> Enforcing FINRA Rule 2010; FINRA Rule 3110; FINRA Rule 3120.

<sup>26</sup> Enforcing NFA Compliance Rule 2-9; NFA Compliance Rule 2-36; NFA Compliance Rule 2-49.

<sup>27</sup> Forty-seven states have implemented data breach notification requirements and numerous states have implemented information security requirements.

<sup>28</sup> FFIEC, *Cybersecurity Assessment Tool*, <https://www.ffiec.gov/cyberassessmenttool.htm> (last modified Feb. 13, 2016).

<sup>29</sup> FFIEC, IT Examination Handbook, <http://ithandbook.ffiec.gov/>.

<sup>30</sup> Federal Reserve System, Office of the Comptroller of the Currency, and the Securities and Exchange Commission, *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, 68 Fed. Reg. 17809 (Apr. 11, 2003), <https://www.occ.gov/news-issuances/bulletins/2003/OCC2003-14a.pdf>.

<sup>31</sup> Pub. L. No. 106–102, 113 Stat. 1338 (codified, in relevant part, at 15 U.S.C. §§ 6801–6809).

<sup>32</sup> 16 C.F.R. pt. 314.

<sup>33</sup> 12 C.F.R. pt. 748.

<sup>34</sup> 17 C.F.R. § 248.30.

fundamental voluntary guidelines for the financial sector.<sup>35</sup> The Committee on Payments and Market Infrastructures (“CPMI”) and the International Organization of Securities Commissions (“IOSCO”) have also published guidance on cyber resilience for financial market infrastructures.<sup>36</sup>

Coordination of regulatory standards allows heavily regulated firms to efficiently strengthen their cybersecurity programs while reducing unnecessary compliance costs. U.S. Treasury Secretary Jack Lew has encouraged agencies “to collaborate with the private sector to establish cyber security best practices and improve information sharing.”<sup>37</sup> Comptroller of the Currency Thomas J. Curry has underscored that “[o]ne of the lessons we have learned in the bank regulatory community is that collaboration is vital, especially in dealing with highly complex, rapidly evolving challenges like cybersecurity.”<sup>38</sup> And Deputy Treasury Secretary Sarah Bloom Raskin stressed the need to “figure out ways [to] harmonize [cybersecurity standards]. We don’t want to see emerge the development of multiple sets of standards, multiple guidances.”<sup>39</sup>

We appreciate the opportunity to collaborate with the Agencies on the establishment of these standards. Although the Agencies note that they have taken into account several pre-existing standards and frameworks in developing the ANPR, we wish to draw attention to some areas where the standards proposed in the ANPR are already covered by existing regulatory requirements. To the extent that the Agencies decide to issue new rules that overlap with pre-existing standards, such as those discussed below, we request that the Agencies harmonize the ANPR with existing regulatory standards to avoid unnecessary inefficiencies or potentially conflicting standards.

- Third-Party Management and the FFIEC IT Examination Handbook, Appendix J: The Agencies are considering applying the standards in the ANPR to third-party service providers. We note that FFIEC has already provided extensive guidance on third-party service providers in Appendix J of the FFIEC IT Examination Handbook,<sup>40</sup> which has

---

<sup>35</sup> G7 Fundamental Elements of Cybersecurity for the Financial Sector (Oct. 11, 2016), <https://www.treasury.gov/resource-center/international/g7-g20/Documents/G7%20Fundamental%20Elements%20Oct%202016.pdf>.

<sup>36</sup> CPMI and IOSCO, *Guidance on cyber resilience for financial market infrastructures* (June 2016), <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf>.

<sup>37</sup> Remarks of Secretary Jacob J. Lew, Department of the Treasury, at the 2014 Delivering Alpha Conference (July 16, 2014), <http://www.treasury.gov/press-center/press-releases/Pages/jl2570.aspx>.

<sup>38</sup> Thomas J. Curry, Comptroller of the Currency, *Remarks at BITS Emerging Payments Forum* (June 3, 2015), <http://www.occ.treas.gov/news-issuances/speeches/2015/pub-speech-2015-78.pdf> (“One of my top priorities as Comptroller . . . has been to address the risks that cyber threats pose to individual banks and the banking system. This effort necessarily requires extensive and ongoing coordination among regulators and banks, large banks and small banks, regulators and the rest of the Government, and the financial sector and other critical infrastructure.”).

<sup>39</sup> Lalita Clozel, *Regulators Must Improve Cybersecurity Coordination: Top Treasury Official*, *American Banker* (Mar. 17, 2016) (quoting Deputy Treasury Secretary Sarah Bloom Raskin) (emphasis added), <http://www.americanbanker.com/news/law-regulation/regulators-must-improve-cybersecurity-coordination-top-treasury-official-1079975-1.html>.

<sup>40</sup> FFIEC, *IT Examination Handbook, Appendix J, Strengthening the Resilience of Outsourced Technology Services*, <http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-j-strengthening-the-resilience-of-outsourced-technology-services.aspx>.

become the industry standard for cybersecurity controls with respect to outsourced technology services. Appendix J follows a risk-based approach to third party management, stating that “[a] financial institution’s third-party management program should be risk-focused and provide oversight and controls commensurate with the level of risk presented by the outsourcing arrangement.”<sup>41</sup> Appendix J also provides strategic considerations and other risk-based guidance with respect to third party capacity, testing, and cyber resilience.<sup>42</sup> To the extent that any rule resulting from the ANPR applies to third-party service providers, we request that those standards be harmonized with Appendix J in order to avoid potentially duplicative or conflicting standards.

- Cyber Resilience and Incident Response Programs: The Agencies are considering a requirement that covered entities establish and maintain enterprise-wide cyber resilience and incident response programs. The FFIEC CAT identifies the incident response program and various elements of cyber resilience as key components of cybersecurity maturity for financial firms.<sup>43</sup> The Interagency Guidelines Establishing Information Security Standards also require financial institutions to develop and implement a risk-based response program to address incidents of unauthorized access to customer information.<sup>44</sup> To the extent that any rule resulting from the ANPR requires the establishment of cyber resilience and incident response programs, we request that the rule be harmonized with existing standards in order to avoid duplicative or conflicting standards. We also request that the Agencies clearly define any terms which may affect the scope of the rule, including any requirements to test, obtain intelligence, or perform analytics on an “ongoing basis.” In order to best align with existing standards, any requirement to establish cyber resilience and incident response programs should be based on periodic assessments of applicable risk as determined by the covered entity.
- Two-Tiered Approach: The Agencies are considering establishing a two-tiered approach to implementation of the enhanced standards, applying a higher set of expectations referred to as “sector-critical standards” to systems of covered entities that are critical to the financial sector. Of course, there are several existing frameworks that already identify and apply a higher set of standards to sector-critical systems, including the Interagency Paper on Sound Practices,<sup>45</sup> Section 9 of Executive Order 13636 designating the Treasury Department as the sector-specific agency for the financial sector,<sup>46</sup> the Fed’s designation of systemically important financial institutions (“SIFI”),<sup>47</sup> the Financial Stability Oversight Council’s (“FSOC”) designation of systemically important financial market

---

<sup>41</sup> *Id.*

<sup>42</sup> *Id.*

<sup>43</sup> FFIEC, *Cybersecurity Assessment Tool*, <https://www.ffiec.gov/cyberassessmenttool.htm> (last modified Feb. 13, 2016).

<sup>44</sup> Interagency Guidelines, 12 C.F.R. pt. 364, Supp. A to App. B, at II.

<sup>45</sup> Federal Reserve System, Office of the Comptroller of the Currency, and the Securities and Exchange Commission, *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, 68 Fed. Reg. 17809 (Apr. 11, 2003), <https://www.occ.gov/news-issuances/bulletins/2003/OCC2003-14a.pdf>.

<sup>46</sup> Exec. Order 13636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

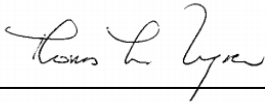
<sup>47</sup> Federal Reserve System, *Enhanced Prudential Standards for Bank Holding Companies and Foreign Banking Organizations*, 12 C.F.R. pt. 252, <https://www.gpo.gov/fdsys/pkg/FR-2014-03-27/pdf/2014-05699.pdf>.

utilities (“SIFMU”),<sup>48</sup> the SEC’s Regulation SCI,<sup>49</sup> and CFTC regulations pertaining to critical infrastructure.<sup>50</sup> The Agencies’ new two-tiered approach risks complicating the regulatory space and creating inefficient compliance costs. We suggest that the Agencies adopt a definition and approach consistent with the Interagency Paper on Sound Practices, which considers a firm significant in a particular critical market if it consistently clears or settles at least five percent of the value of the transactions in that critical market. Adopting this standard would reduce the risk of conflicting or confusing standards and harmonize existing practices and procedures implemented across the industry with any final rules resulting from the ANPR.

\* \* \*

We welcome further engagement and discussion with the Agencies about the comments in this letter. We look forward to working with the Agencies on the creation of cybersecurity protections that complement existing requirements and standards to facilitate effective management of cybersecurity risk. If you have any questions or require further information, please do not hesitate to contact Thomas Wagner at 212-313-1161 or [twagner@sifma.org](mailto:twagner@sifma.org).

Sincerely,



---

Thomas M. Wagner  
Managing Director  
SIFMA



---

Doug Johnson  
Senior Vice President  
ABA



---

Richard Coffman  
General Counsel  
IIB

cc: Alan Charles Raul, Sidley Austin LLP  
Clayton G. Northouse, Sidley Austin LLP  
Grady Nye, Sidley Austin LLP

---

<sup>48</sup> 12 C.F.R. pt. 1320.

<sup>49</sup> 17 C.F.R. § 240, 242, and 249.

<sup>50</sup> 17 C.F.R. pt. 39.



