The Clearing House
At the Center of Banking Since 1853®

February 17, 2017

Via Electronic Submission

Mr. Robert V. Frierson, Esq., Secretary
Board of Governors of the Federal Reserve System
20th Street & Constitution Avenue, N.W.
Washington, D.C. 20551

Robert E. Feldman, Executive Secretary
Attn: Comments
Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, D.C. 20429

Legislative & Regulatory Activities Division
Office of the Comptroller of the Currency
40 7th Street, S.W.
Suite 3E-218, Mail Stop 9W-11
Washington, D.C. 20219

Re: Enhanced Cyber Risk Management Standards (Federal Reserve Docket No. R-1550 and RIN 7100-AE 61; OCC Docket ID OCC-2016-0016; FDIC RIN 3064-AE45)

Sirs and Madams:

The Clearing House Association L.L.C. and The Clearing House Payments Company L.L.C.[1] appreciate the opportunity to comment on the joint advance notice of proposed rulemaking ("ANPR") on "Enhanced Cyber Risk Management Standards" published by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation (collectively, "the agencies") on October 26, 2016.[2]

The agencies are considering proposing enhanced standards in order to "increase the

[1] The Clearing House is a banking association and payments company that is owned by the largest commercial banks and dates back to 1853. The Clearing House Association L.L.C is a nonpartisan organization that engages in research, analysis, advocacy and litigation focused on financial regulation that supports a safe, sound and competitive banking system. Its affiliate, The Clearing House Payments Company L.L.C., owns and operates core payments system infrastructure in the United States and is currently working to modernize that infrastructure by building a new, ubiquitous, real-time payment system. The Payments Company is the only private-sector ACH and wire operator in the United States, clearing and settling nearly $2 trillion in U.S. dollar payments each day, representing half of all commercial ACH and wire volume.

[2] 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").

operational resilience of . . . [large and interconnected financial institutions subject to the agencies' jurisdiction and those entities' service providers] and reduce the impact on the financial system in case of a cyber event experienced by one of these entities."[3] The Clearing House and its member banks share these important goals, and have every incentive to work actively to achieve them. In fact, financial institutions and financial market infrastructures ("FMIs") own the risk of loss that would accompany a poorly defended cyber attack, and we are acutely aware that the cybersecurity failure of one institution may lead to broader industry vulnerabilities and reputational harm. The sector's ability to withstand a major cyber attack is, therefore, clearly of utmost concern to the industry, and industry incentives are properly aligned with market forces.

At the same time, we recognize the benefits of revisiting and strengthening the existing cyber security regulatory framework. Our cybersecurity defenses are one of the core foundations for trust in the financial system, and they are constantly challenged by an ever-changing cybersecurity risk landscape. We urge the agencies to recognize that financial institutions' cybersecurity systems must remain both extremely resilient and responsive to the ever-changing threat environment – "agile," in the words of the Commission on Enhancing National Cybersecurity. In other words, we must allow individual institutions and the financial system at large to obtain the best cyber risk management outcomes possible, which may require different tactics by different members of the sector at different times.

Because we share the agencies' goals, the financial sector has been working diligently to address cybersecurity risk management and resiliency through industry-driven and -focused efforts to identify, develop and implement best practices, share threat information, and conduct training exercises. The White House and Congress have both stated a preference for cybersecurity approaches that are driven by, and coordinated with, industry.[4]

Government can play a vital role in defending our financial system. Indeed, it does: financial institutions, including The Clearing House and its member banks, regularly consult and share real-time cyber threat information with U.S. intelligence, law enforcement, and other agencies that have direct responsibility for cyber defense, and that are best positioned to ensure that cybersecurity issues are appropriately and robustly addressed. The Commission on Enhancing National Cybersecurity has strongly recommended enhancing information-sharing of this type, and we look forward to doing so.

Despite setting forth these shared goals—which we agree are important and worthy of

---

3 *Id.*

4 *See, e.g.*, Press Release, White House, *Engaging the International Community on Cybersecurity Standards* (Dec. 23, 2015), https://www.whitehouse.gov/blog/2015/12/23/engaging-international-community-cybersecurity-standards ("Simply put, . . . a consensus-based, private sector-driven [] standards development process, with input from all interested stakeholders, is superior to a top-down, national government-controlled approach to standards."); The Cybersecurity Enhancement Act of 2014 § 502, Pub. L. 113-274 (113th Cong.) ("The Director [of NIST], in coordination with appropriate Federal authorities, shall . . . as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security . . . In carrying out the[se] activities. . . , the Director shall ensure consultation with appropriate private sector stakeholders.").

sector-wide attention—the ANPR does not provide any analysis of whether or how the current regulatory framework addresses these goals. Likewise, the ANPR does not describe the agencies' views on what gaps exist in the current regulatory framework that would be addressed through the agencies' proposal. Rather, the ANPR moves hastily from the stated goals to proposing quite detailed, prescriptive regulations or standards. While the agencies note that their consideration of enhanced standards follows from their determination that cyber risks are expanding,[5] the agencies do not explain how (i) these risks are expanding, (ii) the current regulatory framework is deficient in addressing those expanding risks, or (iii) the proposed framework mitigates those deficiencies. A lack of clarity on these items makes it difficult to judge the proposals and weigh the benefits and costs of alternative approaches to meeting the agencies' goals.

The Clearing House accordingly recommends that, prior to proceeding with new requirements, the agencies should focus on consolidating existing standards, and work with industry stakeholders to assess the gaps that exist in the current regulatory framework and identify principles that will guide the agencies and the industry in closing those gaps. As the Commission on Enhancing National Cybersecurity recently observed, "[r]egulatory agencies should harmonize existing and future regulations with the Cybersecurity Framework to focus on risk management—reducing industry's cost of complying with prescriptive or conflicting regulations that may not aid cybersecurity and may unintentionally discourage rather than incentivize innovation. . . . [D]isparate regulations risk redundancy and confusion among regulated parts of our economy."[6]

Once a consolidated set of standards is developed, the agencies could then work with industry stakeholders to define a set of principles based on the stated goals, which could serve as a foundation for identifying what, if any, gaps exist within the current body of standards and developing any subsequent standards.

Until these principles are established, and in light of industry's extensive ongoing efforts, substantial incentives, and productive work with government partners to enhance cyber defenses, the agencies' proposed issuance of detailed prescriptive standards of the kind described in the ANPR would be unproductive. In particular, prescriptive standards by their nature address the mechanism (the "how") instead of the purpose (the "what"). Addressing the mechanism through prescriptive standards embeds inflexibility and a lack of responsiveness to new risks, which weakens institution-specific and sectoral risk management capabilities, and works at counter-purpose to our shared goals. Because financial institutions own the risk of loss, there is effectively no "moral hazard" that must be addressed with prescriptive regulatory standards. As the Commission recently concluded, "[t]he right mix of incentives must be provided, with a heavy reliance on market forces and supportive government actions, to enhance cybersecurity."[7]

---

5 "In response to expanding cyber risks, the agencies are considering establishing enhanced standards for the largest and most interconnected entities under their supervision, as well as for services that these entities receive from third parties." ANPR at 74316.

6 Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy* 20-21 (Dec. 1, 2016) (hereinafter "Commission Report").

7 *Id.* at 5.

The Clearing House submits that the actions proposed in the ANPR are not the kind of "supportive government actions" that have been endorsed by the Commission and other government bodies.[8]

Before taking further steps in the rulemaking process, The Clearing House urges the agencies to work collectively with all stakeholders to ensure that goals are well-defined and can be met in a way that does not mandate particular, and therefore likely inflexible, risk management mechanisms. As the agencies recognize in the ANPR, these issues are complex and dynamic, with many questions that can only be resolved in a collaborative dialogue with the financial industry. The Clearing House strongly encourages the agencies to engage with financial institutions to better assess and understand sector-wide risks, potential mitigations, and the role that standards could play in advancing cybersecurity. One venue for such a discussion could be a sector-wide group such as the Critical Infrastructure Partnership Advisory Council ("CIPAC") Financial Services Sector Cybersecurity Profile Development Working Group ("Working Group"),[9] to develop baseline principles based on the stated goals in the ANPR. The Clearing House believes that this collaborative process could enable better coordination with the Department of Homeland Security's ("DHS") and other federal agencies to harden key service providers.

The Clearing House strongly believes that these procedural recommendations are fundamental to our shared critical task of ensuring institutional and sectoral cybersecurity resilience. If, however, despite these recommendations, the agencies are nonetheless determined to move forward with the proposals outlined in the ANPR, The Clearing House recommends that the agencies issue flexible, risk-based objectives with clear definitions and procedural protections, in the form of guidance or policy statements rather than binding standards.

---

8 *See, e.g.*, Press Release, White House, *Engaging the International Community on Cybersecurity Standards* ("This non-governmental approach yields standards of better technical rigor and industry uptake, helps support innovation, and enables the rapid adaptation and evolution of standards.").

9 CIPAC was established by DHS to "facilitate interaction between governmental entities and representatives from the community of critical infrastructure owners and operators," on "a broad spectrum of activities to support and coordinate critical infrastructure security and resilience." Critical Infrastructure Partnership Advisory Council, DHS, https://www.dhs.gov/critical-infrastructure-partnership-advisory-council. Each critical infrastructure sector has developed councils to focus on sector specific issues, such as the Financial Services Sector Coordinating Council ("FSSCC"), which "serves as the primary private sector policy coordination and planning entity to collaborate with the United States Department of Treasury, Financial Services Government Coordinating Council (GCC) and other government entities to address the entire range of critical infrastructure security and resilience activities and sector-specific issues." FSSCC Charter, https://www.dhs.gov/sites/default/files/publications/FSSCC-Charter-03-15-508.pdf. The Working Group was approved in October 2016, to work under the CIPAC framework to "develop a financial services sector sector-specific cybersecurity profile that organizes existing frameworks (e.g., NIST [Cybersecurity Framework], [Federal Financial Institutions Examination Council Cybersecurity Assessment Tool]), agency and [self-regulatory organization] guidance, etc., against a consistently described hierarchy of risk management elements . . . [from which] a common lexicon will emerge that will enable better and sustained protection of financial services critical infrastructure." Working Group Formation Profile, Financial Services Sector Cybersecurity Profile Working Group. *See also* Financial Services Working Groups, DHS, https://www.dhs.gov/financial-services-working-groups.

Finally, we understand that President Trump recently announced his plans to launch a cybersecurity review during his first 90 days in office. While the scope of this review is unclear, to the extent that it is intended to result in a broader cybersecurity strategy or framework across sectors of the economy, we urge the agencies to defer issuance of any additional proposed standards until this broader strategy has been adopted to ensure a consistent approach. In the interim, if the agencies identify any actual gaps, either at a technical or organizational level, in how financial institutions are currently protecting themselves, either individually or collectively, these can be addressed through targeted guidance, or these concerns can be raised during the examination process.

I. Executive Summary

Financial institutions are currently subject to numerous data security, safety and soundness, and general risk management regulatory requirements, guidance documents, informal standards, and frameworks, making the financial sector one of the most heavily-regulated sectors regarding cybersecurity. Collectively, these standards and other documents cover much of the ground that would be covered by the ANPR as to large national banks, financial market utilities, third-party vendors, and many other covered entities.

Recognizing the significance of cyber risks, industry-driven efforts have further sharpened our collective thinking and planning for potential cyber-attacks and demonstrated the private sector's commitment to mitigating these risks. Of course, it is worth noting that the private sector has every incentive to react promptly and robustly to mitigate cyber risk. Precisely because of these incentives, we share the agencies' goals, as stated in the ANPR, of increasing financial sector resiliency against cyber attack and minimizing the impact of a major incident on the sector.

The Clearing House believes that organic industry collaboration, established risk-management frameworks, and existing supervisory oversight have gone a long way, and may even be sufficient, in addressing cybersecurity in the financial sector. To the extent the agencies seek to provide further regulatory guidance, however, they should first synthesize existing standards and frameworks, and perform a gaps analysis to identify, in a rationalized manner, where any additional standards may be warranted. The agencies should also work with industry to develop baseline principles based on the stated goals in the ANPR. Prior to undertaking one or both of these efforts, issuing another layer of standards would be premature.

As such, The Clearing House recommends that, rather than issuing new standards at this stage, the agencies should work with industry, through the CIPAC Working Group, (i) to better understand what regulatory and industry requirements, standards, and guidance already exist, and develop a single consolidated framework from these existing materials, and (ii) to identify fundamental principles based on the ANPR's stated goals, which could form the basis for any future new standards. The Clearing House also requests that the agencies recognize that financial sector cybersecurity cannot be addressed in a siloed fashion, either within certain tiers of financial institutions or within the sector as a whole. Instead, a broader approach is warranted, by working with DHS and other federal agencies to harden key service providers. Financial institutions are simply not in the position to impose their regulators' requirements upon, or build redundancies to replace, other sectors of the economy, such as utility providers and internet

service providers. The Clearing House understands, however, the role that financial institutions play in managing cybersecurity risks and appreciates that financial regulators may not have direct jurisdiction to regulate these providers without coordinating with other sector-specific agencies and/or seeking additional legislative authority. The Clearing House supports such coordinated efforts.

To the extent the agencies do issue any new standards based on the ANPR, The Clearing House recommends that they be in the form of guidance rather than binding standards. Any final product should be in the form of flexible, risk-based, objectives rather than prescriptive, one-size-fits-all implementation requirements.

As to the specific standards proposed in the ANPR, The Clearing House's recommendations are as follows:

- The ***scope of covered entities*** should be determined using a multi-factor, risk-based standard, rather than using a bright-line, asset-based cutoff.

- Any additional ***service provider requirements*** should be implemented, to the extent possible, through direct agency oversight of service providers, in conjunction with other sectors' regulators, rather than by adding additional vendor oversight requirements for financial institutions.

- While boards of directors must provide effective supervision for appropriate ***cyber risk governance***, financial institutions should have discretion in determining how to structure this supervision, including the sources of information, level of involvement in approving day-to-day policies and procedures, and board reporting chains.

- Financial institutions should also have flexibility in developing their ***cyber risk management*** structure as part of their overall risk management strategy, including how they organize and allocate responsibilities among the "three lines of defense."

- The agencies should limit the scope of additional administrative requirements for ***internal and external dependency management*** to focus on business assets that are most likely to raise material risks to the financial institution's cybersecurity and on third-parties with access to key systems or information. The agencies should also provide financial institutions with the flexibility to streamline administrative processes relating to managing these dependencies.

- The ***incident response, cyber resilience, and situational awareness*** standards should be risk-, rather than outcome-focused, while recognizing that financial institutions cannot remove dependencies on other critical infrastructures and sectors.

- The scope of "***sector-critical systems***" should be narrow, predictable, and risk-focused. The agencies should adopt a multi-factor test, as well as a clear process, for determining which systems are sector critical. Specific control requirements for sector-critical systems should be achievable and risk-based.

- In light of the lack of well-developed metrics for ***quantifying cyber risks***, adopting a single cyber risk quantification methodology is premature.

II. Rather Than Issuing New Standards, the Agencies Should Consolidate Existing Guidance and/or Establish Baseline Principles.

The Clearing House shares the agencies' stated goals of improving cyber resiliency and limiting the effects of a major cyber event on the financial sector. While the ANPR lays out various proposed prescriptive standards purportedly intended to further this goal, The Clearing House respectfully submits that issuance of any new standards would be premature at this stage The Clearing House recommends that, rather than adopting new standards in the near term, the agencies work in collaboration with industry, such as through the CIPAC Working Group, to (i) map, harmonize, and consolidate existing standards into a single document, and (ii) establish baseline principles in line with the stated goals. These actions would provide a useful foundation for further discussions between the agencies and members of the financial sector, within the financial sector, and between financial sector regulators and both industry and regulators in other sectors.

A. The Agencies Should Consolidate Existing Standards Prior to Adopting a New Framework.

Financial institutions are currently subject to a considerable array of data security regulatory requirements and more informal standards. The demanding requirements in the *Interagency Guidelines Establishing Standards for Information Security* ("*Interagency Guidelines*"), as well as safety and soundness requirements and targeted guidance documents issued by the agencies and other financial regulators—on outsourcing and third-party relationships, data security, use of cloud services, and other issues—have made the financial sector one of the most highly-regulated sectors in the U.S. economy regarding cybersecurity.

Over the last several years, and as described in Part II of the ANPR, financial regulators and other agencies have issued numerous cybersecurity standards that have provided the framework for considering information security in financial institution examinations. These include (i) the Federal Financial Institutions Examination Council ("FFIEC") IT Examination Handbook and Cybersecurity Assessment Tool—both of which have just recently been revised; (ii) the National Institute of Standards and Technology ("NIST") Cybersecurity Framework; (iii) the Committee on Payments and Market Infrastructure ("CPMI") and the Board of International Organization of Security Commissions ("IOSCO") cyber resilience guidance; and (iv) the Board, OCC, and SEC *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* ("*Sound Practices Paper*").[10] Many of these documents were enacted as informal guidance, allowing their authoring agencies to issue them without the notice-and-

[10] As an appendix to its comment letter, the Financial Services Sector Coordinating Council ("FSSCC") has compiled a list of the dozens of financial services cybersecurity-related regulatory requirements, guidance, tools, and frameworks issued since the release of the NIST Cybersecurity Framework in early 2014.

comment process otherwise required under the Administrative Procedures Act ("APA").[11]

In addition to cyber-specific standards, many large financial institutions that would be covered by the proposed rules are also subject to general risk management frameworks, including the OCC *Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches* ("*Heightened Standards*") and the Federal Reserve's *Enhanced Prudential Standards for Bank Holding Companies and Foreign Banking Organizations* ("*Enhanced Prudential Standards*"). While applicable to various risks beyond cyber, regulators have noted that "operational risk," as covered by these standards, includes cybersecurity.[12]

The ANPR, in part, combines components of existing guidance.[13] At the same time, the proposal outlined in the ANPR would increase requirements for covered entities, as it would (i) transform certain guidance documents into mandatory standards, and (ii) add new requirements in addition to those drawn from prior guidance.[14] Such action by the agencies would increase

---

[11] Of these guidance documents, only the *Sound Practices Paper* was issued following a full APA process. The CPMI-IOSCO guidance was issued following a comment process. However, because the issuing bodies are not federal regulatory agencies, they are not subject to the same APA processes and standards. Similarly, while the NIST Cybersecurity Framework was issued in draft form and industry feedback was solicited, this was not required to be done through the formal APA notice-and-comment process, which, among other things, meant that NIST did not have to reply to the comments or explain why changes were not made in response to particular concerns expressed in comments.

[12] *See, e.g.*, Remarks by Thomas J. Curry, Comptroller of the Currency, Before the Exchequer Club (Sept. 18, 2013) ("[A]s important as it is to look back and deal with issues arising from the financial crisis, it is equally urgent that we look ahead and stay on top of emerging threats … The particular issue I have in mind . . . involves the operational risk posed by cyberattacks. . . .It's important to remember that cybersecurity is a safety and soundness issue, and more specifically, an example of operational risk."). *See also* Remarks by Thomas J. Curry, Comptroller of the Currency, For the Independent Community Bankers of America Annual Convention (Mar. 4, 2014) ("But while you need to attend to the traditional areas of risk, it's crucial that you keep your eyes focused on emerging areas of risk. And no area of emerging risk is more important today than the cyber threats that are increasingly common in our interconnected environment."); Remarks by Thomas J. Curry, Comptroller of the Currency, Before the Exchequer Club (May 16, 2012) (noting the importance of vigilance regarding IT security for processors during a speech on operational risk).

[13] For example:

- Many cyber risk governance requirements, as outlined in Category 1 of the ANPR, are drawn from the FFIEC IT Examination Handbook Management Booklet.
- As discussed in Section IV.B.2, below, the proposed "three lines of defense" risk management structure is drawn from the *Heightened Standards*, as is the requirement for an independent risk management function.
- The proposed two-hour recovery time objective for sector-critical systems, as discussed in Section VI.C.3, below, is drawn from the CPMI IOSCO cyber resilience guidance.

[14] As the ANPR notes, these standards are intended to be additive, not substitutes for the existing standards. *See, e.g.*, ANPR at 74317 ("The proposed enhanced standards would not replace the [Uniform Rating System for Information Technology ("URSIT")] but could be used, in part, to inform the cyber-related elements of the URSIT rating for covered entities . . . The [Interagency] Guidelines and safety and soundness standards would continue to apply to covered entities that are insured depository institutions.")

the time devoted by cybersecurity professionals on regulatory compliance. Experienced and knowledgeable cybersecurity resources are scarce in the marketplace – both in the financial sector and in the broader economy – such that financial institutions cannot meet this administrative burden by simply investing in an expanded workforce. Because of this, while The Clearing House agrees that having appropriate cybersecurity governance structures in place is important, it is critical that regulators and industry find an appropriate and realistic balance between tangible controls and administrative processes. If this balance is not struck appropriately, our mutual goals – increasing the financial sector's safety, soundness, and resiliency – will not be furthered, and may even be hindered.

Rather than adding requirements on top of, and beyond those in, the existing web of regulations, guidelines, and regulatory expectations, The Clearing House recommends that the agencies focus on mapping, harmonizing, and consolidating the existing standards applicable to financial institutions to determine whether there are any gaps warranting further regulatory action. Such consolidated guidance would not only be constructive in simplifying the administrative compliance burden for covered financial institutions – consistent with the recent recommendations from the Commission on Enhancing National Cybersecurity,[15] but it would also facilitate further discussions, both within the financial sector and with industry and regulators in other agencies, regarding how to strengthen the economy's cyber resiliency writ large.

As a nation, we are currently at a key time in our approach to managing cybersecurity risks. A plethora of standards and guidance exists, with some industry-by-industry variation. We now need to focus on identifying a standardized approach, with sector variances only as genuinely warranted. Financial regulators have a unique opportunity to work with industry to ensure that the financial sector continues to be a leader in this space. As such, it is important that any new efforts be done in a thoughtful way to ensure appropriate, meaningful progress is made while eliminating unnecessary and unintended adverse effects.

B. Before Adopting New Prescriptive Standards, the Agencies Should Establish Baseline Principles.

The agencies stated goals in proposing the enhanced standards, according to the ANPR, are to "increase the operational resilience of [large and interconnected entities subject to the agencies' jurisdiction] and those entities' service providers and reduce the impact on the financial system in case of a cyber event experienced by one of these entities." The Clearing House and its members share these goals, and have every incentive—even without regulation—

---

[15] Commission Report at 20-21 ("Regulatory agencies should harmonize existing and future regulations with the Cybersecurity Framework to focus on risk management—reducing industry's cost of complying with prescriptive or conflicting regulations that may not aid cybersecurity and may unintentionally discourage rather than incentivize innovation. . . Such disparate regulations risk redundancy and confusion among regulated parts of our economy. Federal regulators should harmonize their efforts relating to the Framework, an action called for in Executive Order 13636 but never executed. Regulatory agencies should make explicit how their requirements map to the Cybersecurity Framework . . . Because of the efficiencies and reduced compliance costs that covered entities would realize from a common framework, an agency that advances an approach which substantially departs from the baseline framework would be required to make the case that its added cost is outweighed by a public benefit.").

to actively work toward achieving them.

By way of illustrative example, the private sector has responded promptly to the recent SWIFT incidents. In addition to SWIFT implementing a broad, new Customer Security Programme,[16] banks and FMIs are actively engaging with each other on issues concerning cybersecurity. The topic has been discussed, for example, at meetings of The Clearing House's Managing Board, Enterprise Risk Committee, The Clearing House Interbank Payments Systems ("CHIPS") Business Committee, and a wire fraud work group of The Clearing House member banks. FMIs and banks have also participated in several cyber-attack exercises this year involving simulated compromises to wire systems. The financial sector, through its coordinating council and the Financial Services Information Sharing and Analysis Center ("FS-ISAC"), has sponsored discussions between SWIFT and its membership, focusing on cybersecurity events and contributing vulnerabilities, and has published a best practices paper highlighting the vulnerabilities exploited.[17] The Clearing House is also speaking directly with SWIFT to discuss synchronizing assurance programs, in an effort to avoid the proliferation of standards, guidelines, etc. that exist in the regulatory space.

Additionally, industry works closely with those federal agencies and law enforcement organizations that have direct responsibility for cyber defense, and are best positioned to ensure that cybersecurity issues are appropriately and robustly addressed, including DHS, the Federal Bureau of Investigation, the Department of the Treasury and other federal agencies with cybersecurity related expertise. The Clearing House looks forward to continuing to collaborate with these federal agencies, as well as the agencies that issued the ANPR, to continue to advance our shared goals of increasing cyber resiliency while decreasing and/or mitigating the industry's cybersecurity risk profile overall.

The Clearing House submits, however, that the ANPR moves too hastily from the goals stated—which are important and worthy of sector-wide attention—to detailed, prescriptive proposed regulations or standards. The agencies should first establish a set of principles based on the stated goals. Because the agencies skipped this critical step, many of the resulting proposed requirements are duplicative, ambiguous, impractical, divorced from the stated goals, or even counterproductive. The Clearing House recommends, therefore, that, prior to issuing any new standards based on the ANPR, the agencies should first work with industry, through the CIPAC Working Group, to develop a set of principles.

Once the agencies and industry agree on a fundamental set of principles, these principles

---

16 *See* Press Release, *Board Announcement: SWIFT AGM and Customer Security Programme* (June 10, 2016), https://www.swift.com/insights/press-releases/board-announcement_swift-agm-and-customer-security-programme.

17 We note that FS-ISAC has recently announced the establishment of the Financial Systemic Analysis & Resilience Center ("FSARC")—an organization formed by eight of the largest U.S. banks to coordinate research on systemic risk to the financial system and proactively identify ways to enhance the resilience of the critical infrastructure underpinning much of the U.S. financial system. *See* Press Release, *FS-ISAC Announces the Formation of The Financial Systemic Analysis & Resilience Center* (Oct. 24, 2016), http://www.prnewswire.com/news-releases/fs-isac-announces-the-formation-of-the-financial-systemic-analysis--resilience-center-fsarc-300349678.html.

(along with the consolidated guidance recommended in Section II.A) could serve as a foundation for further work in this space, including identifying any gaps in existing standards and practices, and then ensuring industry and agency alignment on any potential more detailed set of cybersecurity standards that flow from this principles-focused analysis.

In recent years, the government has focused on ensuring that its cybersecurity standards are principles-based and not prescriptive, precisely for this reason. Based on the ANPR, however, it remains unclear which principles the agencies are intending to advance. As a result, and as highlighted throughout Section IV.B, below, many of the prescriptive standards proposed in the ANPR would either not advance the ANPR's goals or would even hinder accomplishment of those goals.

III. To the Extent the Agencies Do Issue New Standards, They Should Be Issued as Guidance and Only After Fully Engaging with Stakeholders.

Part VIII of the ANPR notes that the agencies remain undecided as to their intended course regarding the proposed standards. The Clearing House welcomes this opportunity to participate in a notice-and-comment process prior to the agencies implementing any additional standards, and is eager to have the fullest possible stakeholder open comment process, whereby the agencies receive and respond to industry and other stakeholder input. Agency consideration of such perspectives will ultimately increase the likelihood that any resulting standards will be reasonable, enhance security, lower systemic risk, and not be overly prescriptive.

For numerous reasons, The Clearing House recommends that the result of this consultative process—whether it be a consolidated set, as recommended above, or additional standards—be policy statements or other flexible, less formal guidance documents rather than binding regulations or standards.

First, binding regulation is generally most warranted when moral hazard or other perverse incentives could lead banks to engage in activity that is contrary to safety and soundness and their chartered purpose. With cybersecurity, financial institutions own the risk – including both any direct costs and reputational concerns - and have every incentive to mitigate this risk without being forced to do so by heavy-handed regulation.[18] Where the industry efforts are as robust as they are with financial sector cybersecurity, prescriptive standards are unlikely to further mitigate risks sufficiently to justify the added compliance burden and can actually be counterproductive, as more fully discussed below, by requiring covered institutions to reallocate time and resources away from actual risk mitigation activities to regulatory compliance.

Second, guidance would provide covered entities with the flexibility needed to implement innovative programs designed to achieve the goal of reducing cyber risk. That adaptability is necessary to respond to the rapidly-evolving cybersecurity threat landscape and to take advantage of the consistently-developing cybersecurity best practices arsenal. As the recent CPMI IOSCO cyber resilience guidance notes, "[t]he guidance is principles-based, recogni[z]ing that the dynamic nature of cyber threats requires evolving methods to mitigate these threats.

---

[18] *See* Commission Report at 5.

Guidance requiring specific measures today may quickly become ineffective in the future."[19] By contrast, if the agencies issue prescriptive standards, covered entities may be bound to comply, without deviation, with the letter of inflexible and specific regulatory requirements.

Third, proceeding through guidance would provide agencies with flexibility if a covered entity is considered non-compliant or not fully meeting expectations, to take actions short of formal enforcement (e.g., through the examination process or by compelling a bank to develop a plan to remediate as a safety and soundness issue under the process outlined in 12 C.F.R. Part 30). Among other benefits of such flexibility, allowing regulators to address actual or perceived cyber vulnerabilities through non-disclosed proceedings rather than public enforcement could avoid unnecessarily publicizing vulnerabilities, when publicity could increase the risk to the covered institution, its customers, and the sector.

Fourth, additional standards would increase inefficiency and may even be counterproductive, by requiring financial institutions' information security professionals to spend their time and resources mapping against and complying with yet another different set of standards. A recent Financial Services Sector Coordinating Council ("FSSCC") survey found that cybersecurity personnel in some large multinational financial institutions were devoting up to 40% of their time mapping and translating different regulatory requirements for compliance purposes rather than responding to advancing threats or implementing next generation tools and processes.[20] Instead of focusing on further administrative work, these professionals should be focusing on the important work of ensuring that their networks, systems, and financial institutions are secure against cyber threats. As discussed above, at least some of the framework described in the ANPR appears to be drawn from existing standards and guidelines. It is unnecessary to duplicate the requirements in these other guidance documents if the resulting standards from the ANPR are intended to supplement and not replace them. To avoid creating duplicative requirements which would (i) create additional administrative work for information security professionals and (ii) fail to provide any additional security for the industry, The Clearing House recommends that the agencies synthesize existing standards, so that future conversations can focus on what, if any, standards should be added.

Fifth, guidance would provide financial institutions operating across borders (and therefore subject to cybersecurity standards from multiple jurisdictions) the necessary flexibility to navigate potential conflicts between various rules and international requirements. The U.S. Government should lead by example in allowing financial institutions to establish enterprise-wide standards that do not create international compliance risk.

Finally, issuing guidance rather than binding regulations would be consistent with past FFIEC and financial regulator practice regarding cybersecurity.

---

19 Board of the International Organization of Securities Commissions, *Guidance on Cyber Resilience for Financial Market Infrastructures* 7 (June 2016), http://www.bis.org/cpmi/publ/d138.pdf.

20 *See* Letter from FSSCC to Diane Honeycutt, National Institute of Standards and Technology, at 6 (Feb. 9, 2016), http://fsscc.morwebcms.com/files/galleries/NISTcommentletterSigned-0001.pdf.

To the extent the agencies do issue regulations rather than informal guidance, the agencies should issue flexible, risk-based standards focused on meeting particular objectives rather than prescriptive standards.[21] These standards could generally require financial institutions to have programs in place and/or set control objectives, while providing flexibility in terms of how organizations determine risk appetite and identify appropriate implementation and mitigation steps.[22]

---

[21] As described more thoroughly in Sections IV.B and C, below, a number of the standards proposed in the ANPR are overly prescriptive. These include, for example, specific requirements regarding board of director approvals, predictive incident response programs, and use of the most effective, commercially-available controls (for sector-critical systems).

[22] Reliance on a risk-based framework is a fundamental common feature of modern approaches to cybersecurity guidance—from federal agencies, from industry experts, and from foreign regulators alike. As the Department of Homeland Security has put it, for example, "[c]ybersecurity is about more than implementing a checklist of requirements—Cybersecurity is managing cyber risks to an ongoing and acceptable level." Department of Homeland Security, *Cyber Risk Management Primer for CEOs*, https://www.dhs.gov/sites/default/files/publications/C3%20Voluntary%20Program%20-%20Cyber%20Risk%20Management%20Primer%20for%20CEOs%20_5.pdf. As a recent study on federal cybersecurity efforts similarly concluded, "[t]he Department of Defense (DoD), Intelligence Community (IC), and Federal agencies via representation by the National Institute of Standards and Technology (NIST) have collectively taken action to move from a compliance-oriented approach to cyber security to one based on risk management." MITRE Corporation, "The Risk Management Framework and Cyber Resiliency" (2016), https://www.mitre.org/sites/default/files/publications/pr-16-0776-cyber-resiliency-and-the-risk-management-framework.pdf. For other examples reflecting the centrality of risk management as an organizing principle for cybersecurity, see FFIEC Cybersecurity Assessment Tool Frequently Asked Questions 1 (Oct. 17, 2016), https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT%20FAQs.pdf ("Management of financial institutions and management of third-party service providers are primarily responsible for assessing and mitigating their entities' cybersecurity risk. FFIEC member agencies developed the Assessment to help institutions' management identify their risks and determine their cybersecurity preparedness."); The Financial Industry Regulatory Authority ("FINRA"), *Report on Cybersecurity Practices* (February 2015), http://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf ("FINRA's objective is to focus firms on a risk management-based approach to cybersecurity. This enables firms to tailor their program to their particular circumstances; as every firm in our sweep emphasized, there is no one-size-fits-all approach to cybersecurity."); National Association of Insurance Commissioners, *Principles for Effective Cybersecurity: Insurance Regulatory Guidance*, http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf. ("Cybersecurity regulatory guidance for insurers and insurance producers must be flexible, scalable, practical and consistent with nationally recognized efforts such as those embodied in the National Institute of Standards and Technology (NIST) framework[; r]egulatory guidance must be risk-based and must consider the resources of the insurer or insurance producer, with the caveat that a minimum set of cybersecurity standards must be in place for all insurers and insurance producers that are physically connected to the Internet and/or other public data networks, regardless of size and scope of operations."); G7, *Fundamental Elements of Cybersecurity for the Financial Sector* (Oct. 2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/559186/G7_Fundamental_Elements_Oct_2016.pdf. ("Entities in the financial sector should establish cybersecurity strategies and frameworks tailored to their nature, size, complexity, risk profile, and culture.").

IV. If the Agencies Issue New Standards, The Clearing House Recommends That The Standards Be Principles- and Risk-Based, Flexible, and Clear.

If, in spite of The Clearing House's recommendations above, the agencies decide to proceed with new standards consistent with those proposed in the ANPR, The Clearing House makes the following recommendations, as explained in more detail below:

- The agencies should adopt standards that are principles- and risk-based, in line with the stated goals, rather than standards that are unnecessarily prescriptive or duplicative of already-existing requirements.

- Any new standards should recognize the dynamic cyber environment, clearly state the agencies' expectations, and include clear, well-defined, and precise terminology. For example, several categories of the proposed enhanced standards require entities to engage in "continual" assessment, which implies ongoing, real-time reassessments rather than periodic assessments.

- While the agencies are focused on lowering risk for the sector at large, individual financial entities are often not in the position to assess or manage the sector's risk overall, particularly in situations where the financial sector's risks are intertwined with other critical infrastructure sectors' risks. Any standards that are issued should recognize this limitation, and focus on managing financial institutions' own risks. More holistic measures should be pursued with other agencies, such as DHS, to manage risks that lie beyond the reasonable control of the sector itself.

A. The Scope and Manner of Application of the Enhanced Standards, With Respect to Both Covered Entities and Service Providers, Should be Revised to Use a Risk-Based Approach.

The ANPR states that the agencies are considering applying the new standards principally to firms under their jurisdictions based on asset value, leveraging the $50 billion standard from the Dodd-Frank Act. In addition, the agencies are considering applying these standards to covered entities' service providers. As described further below, The Clearing House urges the agencies to take a risk-based approach, both in determining the entities to which any new standards would apply and in the manner these standards would be imposed on service providers.

1. The Scope of Covered Entities Should be Determined Using a Risk-Based Standard, Rather than Using a Bright-Line Asset-Based Cutoff.

According to the ANPR, the agencies are considering applying the proposed enhanced standards to firms subject to the respective agencies' jurisdiction based on their asset holdings—namely, those "with total consolidated assets of $50 billion or more on an enterprise-wide basis," on the ground 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."[23]

---

[23] ANPR at 74318.

The rationale for using a fixed asset-based cutoff for applying enhanced standards does not accurately account for the nature of cyber risks to the financial services sector. The $50 billion asset value cutoff is derived from the Dodd-Frank Act's provisions addressing potential systemic risks associated with financial institutions' size and interconnectedness.[24] Such an asset-value-based cutoff may be appropriate when the issue is one of systemic importance and liquidity. That is because the largest financial institutions, despite being interconnected, may, due to their own resources, not be affected when smaller financial institutions with which they do business fail. Indeed, small bank failures are relatively common, and they do not threaten the economy more broadly, regardless of their interconnectedness or relationships with larger financial institutions.[25] The Dodd-Frank Act was enacted in the wake of the 2008 economic crisis, motivated by the concern that the threat of failure of the country's largest financial institutions, rather than all financial institutions, had the potential to cause systemic harm to the financial sector at large. Thus, the use of a size-based metric was, at the time of Dodd-Frank's passage, considered appropriate to measure systemic financial risk in certain contexts.

Even in those contexts, however, the Dodd-Frank Act itself recognizes the need to leave flexibility to look beyond size alone as a trigger.[26] Current and former lawmakers who played central roles in Dodd-Frank's enactment are also currently reassessing the $50 billion cutoff's appropriateness, suggesting that the cutoff should perhaps be higher or that regulation should be based on various risk factors – only one of which is asset value – rather than being solely based on this single factor.[27] In early December 2016, the House passed, in bipartisan form, the Systemic Risk Designation Improvement Act of 2016, which would replace the $50 billion asset cutoff with a multi-factor risk-based test to determine systemic importance based not only on size, but also interconnectedness, the extent of readily-available substitutes, global cross-jurisdictional activity, and complexity.[28]

Doubling down on the Dodd-Frank standard when lawmakers are questioning it would be unwise. Even if an asset-value-based threshold *were* appropriate for liquidity-based risk issues, however, a financial institution's size alone is generally not an adequate proxy for inter-connectedness or systemic consequence if a particular entity is a cyber breach victim, where the weakest link, regardless of size, can cause systemic risk. For example, in February 2015, hackers diverted $81 million in funds from the Bank of Bangladesh through the SWIFT system,

---

24 *See* 12 U.S.C. §§ 5365(a), 5325(a)(2).

25 This year alone, the FDIC has announced the closure of five banks across the country, in addition to eight bank closures in 2015 and 18 bank closures in 2014. *See* FDIC Failed Bank List, https://www.fdic.gov/bank/individual/failed/banklist.html.

26 *See* 12 U.S.C. 5325(a)(2)(A).

27 *See, e.g. Dodd-Frank Author: Current SIFI Threshold Is 'Mistake'*, ABA Banking Journal (Nov. 21, 2016), http://bankingjournal.aba.com/2016/11/dodd-frank-author-current-sifi-threshold-is-mistake/.

28 Systemic Risk Designation Improvement Act of 2016, H.R. 6392, 114th Cong. (2nd Sess. 2016). The bill passed with a vote of 254-161, including 20 Democrats.

reportedly by obtaining the bank's SWIFT credentials.[29] Reports suggest that the hackers may have obtained the credentials through insiders' cooperation at the bank,[30] or through the bank's other lax security practices, such as a lack of firewalls.[31] At least one other bank was also reportedly compromised in the scheme.[32]

As this incident illustrates, if common infrastructure or networks are compromised, the size of the institution that is breached is potentially irrelevant, as the Bank of Bangladesh is hardly considered a large entity in this sector.[33] It is perhaps because of this risk that, across the economy's different sectors, regulators have declined to issue cybersecurity standards with prescriptive requirements that vary based on size.[34] Applying an arbitrary size cutoff for covered entities without considering other risk factors would not be well-suited to increase the operational resilience and reduce the impact on the financial system in the event of a cyber incident. As such, The Clearing House recommends that the agencies adopt a flexible, risk-based approach, considering factors such as interconnectivity and market centrality, as opposed to a bright-line, single-factor cutoff such as the asset-based cutoff proposed in the ANPR.[35]

At the same time, as a practical matter, The Clearing House recognizes that smaller entities may not have the resources to implement cybersecurity programs that are as sophisticated and resource-intensive as larger entities. In light of these practical limitations, regulators (including the agencies and other financial regulators) have historically provided that

---

29 *See, e.g.*, Kim Zetter, *That Insane, $81M Bangladesh Bank Heist? Here's What We Know*, Wired (May 17, 2016), https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/.

30 Ruma Paul, *Exclusive: Some Bangladesh Bank officials involved in heist – investigator*, Reuters (Dec. 12, 2016), http://www.reuters.com/article/us-cyber-heist-bangladesh-exclusive-idUSKBN1411ST.

31 Zetter, *That Insane, $81M Bangladesh Bank Heist? Here's What We Know*, Wired.

32 *Id.*

33 *See generally* Commission Report at 13 ("Our interconnections and interdependencies are becoming more complex and now extend well beyond critical infrastructure (CI). These interconnections reduce the importance of the CI label, because, by association, all dependencies may be critical. As these linkages grow, so does the need to consider their associated risks.")

34 *See, e.g.*, *Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services*, 81 Fed. Reg. 72986, 72987 (Oct. 21, 2016) (in issuing final version of cybersecurity requirements for Department of Defense (DoD) contractors, DoD responded to comments requesting that "due to the high cost of compliance, DoD provide for an alternative approach for small business," by stating that "[t]he value of the [covered] information (and impact of its loss) does not diminish when it moves to contractors (prime or sub, *large or small*)." (emphasis added)).

35 The Clearing House also recommends that, even for larger financial institutions that would clearly fall within the scope of the proposed standards under any likely definition of covered entities, financial institutions should have the flexibility in determining where to apply the enhanced standard within the entity, using a risk-based approach. For example, while the standards suggested in the ANPR would apply to covered entities on "an enterprise-wide basis because cyber risks in one part of an organization could expose other parts of the organization to harm," ANPR at 74318, financial institutions should have the flexibility to determine whether risk to the entity subject to U.S. jurisdiction is, in fact, at risk from, for example, foreign branch offices which may be technically segregated from the U.S. covered entity.

size should be only one factor taken into account in implementing a cybersecurity program, with standards focusing on risk-based, flexible requirements rather than specific, prescriptive, requirements, which can be tailored to an individual financial institution's size, business, and complexity.[36] The Clearing House's recommendation that the agencies apply any new standards beyond the largest financial entities, therefore, further supports the recommendation, described in Section II.A, above, to adopt risk-based standards, especially through informal guidance, so financial institutions can make risk-informed, cost-benefit analyses regarding their cyber risk management programs, regardless of size.

2. Any Further Service Provider Requirements Should Be Implemented Through Direct Service Provider Oversight, in Conjunction with Other Sectors' Regulators, Rather Than by Adding Requirements for Financial Institutions.

According to the ANPR, "the agencies are considering whether to apply the standards to third-party service providers with respect to services provided to . . . covered entities."[37] The ANPR suggests that the agencies could apply enhanced standards to service providers, either by directly regulating and overseeing third-party service providers or by imposing requirements on covered financial institutions to ensure, and to attest to, their service providers' compliance.[38]

Existing vendor oversight requirements—including requirements to perform vendor due diligence and manage vendor cyber risk based on access to critical systems and database—are sufficiently robust.[39] To the extent the agencies seek to apply enhanced standards to service providers, The Clearing House recommends that the agencies do so through direct agency oversight of these service providers, and not by placing additional onus on financial institutions to negotiate enhanced contractual requirements. Current regulations and standards require financial institutions to negotiate numerous controls in contracts with third parties. This can make innovation challenging, as many service providers offer unique services in fields with

---

[36] For example, the *Interagency Guidelines* require covered financial institutions to "implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities." 12 C.F.R. Part 30, App. B (as incorporated into the OCC regulations for national banks) (emphasis added).

[37] ANPR at 74318.

[38] *See id.* ("Direct application of the standards to these service providers could have potential benefits, including facilitating supervisory action in the event that a covered service was not meeting a proposed standard and establishing an obligation for meeting the standard on the depository institution or its affiliate, as well as on the third-party provider of the covered service. . . The Board also is considering requiring nonbank financial companies and Board-supervised FMIs to verify that any services the nonbank financial company or Board-supervised FMI receives from third parties are subject to the same standards that would apply if the services were being conducted by the nonbank financial company or Board-supervised FMI itself.").

[39] *See* FFIEC, IT Examination Handbook, Booklets on Information Security, Outsourcing Technology Services, and Supervision of Technology Service Providers; OCC, Bulletin 2013-29, Third-Party Relationships: Risk Management Guidance (Oct. 30, 2013).

limited competition, such that financial institutions lack the negotiating power to demand strict contractual terms in the face of vendor refusal. If the agencies' intent is to require financial institutions to include additional provisions in service provider contracts, this will not only make financial institutions' compliance, innovation, and vendor management increasingly more challenging, but in many cases, even the largest financial institutions will simply be unable to comply.

The Clearing House recognizes that the agencies' authority with respect to direct regulation or examination of, and enforcement against, service providers may be limited to certain contexts.[40] We submit, however, that the appropriate response to any such limitation is not to force regulated financial institutions to attempt to compensate for any jurisdictional gaps. Instead, The Clearing House, encourages the agencies (i) to take a holistic approach to managing sector risk from service providers, and (ii) to seek any additional statutory authority they deem necessary in order to apply the desired regulatory standards directly to service providers. The former approach could include, for example, agency coordination with DHS and other government agencies (such as the Federal Communications Commission regarding internet service providers) to assist in efforts to strengthen critical service providers. If, as The Clearing House recommends in Section II, above, the agencies work to consolidate existing requirements and/or establish basic principles rather than issuing new standards, the resulting work product would likely serve as a useful basis for further discussions not only between the agencies and the financial industry, but with Congress, as well as service providers and regulators from other industries as well.

While the financial sector certainly appreciates the serious risks associated with third-party service provider cybersecurity, there is only so much that can be done by the sector in isolation. Rather than focusing on financial institutions' vendor oversight requirements, the agencies can strengthen the financial sector's resiliency by strengthening the resiliency of the underlying service providers and infrastructure backbone. Such an endeavor will be far more successful, particularly if both the agencies and industry work with our partners in other industries to strengthen collectively.

---

40 *See* 12 U.S.C. § 1867(c) ("[W]henever a depository institution that is regularly examined by an appropriate Federal banking agency … causes to be performed for itself, by contract or otherwise, *any services authorized under this chapter*, whether on or off its premises … *such performance* shall be subject to regulation and examination by such agency to the same extent as if such services were being performed by the depository institution itself on its own premises." (emphasis added)). *See also Outsourcing Accountability? Examining the Role of Independent Consultants: Hearing Before the S. Comm. On Banking, Hous., & Urban Affairs Subcomm. on Fin. Insts. & Consumer Prot.*, 112th Cong. (2013) (statement of Daniel P. Stipano, Deputy Chief Counsel, Office of the Comptroller of the Currency) ("While the OCC believes its authority and use of independent consultants is generally appropriate, there is one area where we believe legislative action could be helpful. Under the current statutory scheme, the OCC faces significant jurisdictional obstacles if it seeks to take an enforcement action directly against an independent contractor. A recent court decision has further elevated the standard for taking such enforcement actions. The OCC would welcome a legislative change in this area that would facilitate our ability to take enforcement actions directly against independent contractors that engage in wrongdoing. Such a legislative change would be useful not only with respect to the use of independent contractors in an enforcement context but also, and perhaps more importantly, in cases where a bank has chosen to outsource significant activities to an independent contractor.")

B. If the Agencies Issue New Standards, They Should Be Principles-Based and Outcome-Focused.

The fifth section of the ANPR includes five categories of proposed enhanced standards for covered entities: (i) cyber risk governance; (ii) cyber risk management; (iii) internal dependency management; (iv) external dependency management; and (v) incident response, cyber resilience, and situational awareness. The Clearing House recommends that these standards be focused on objectives and end-goals, rather than prescriptive mandates for particular methods of achieving desired outcomes. As defined, the scope of covered entities includes sophisticated businesses with complex organizational structures and operations. They also, however, often have complex compliance and information security structures and controls already in place. Particularly where best practices are not clearly established, the agencies should allow financial institutions to leverage their internal expertise to develop the appropriate controls for their own businesses, rather than establishing a prescriptive approach that regulators have expressly avoided to date.

1. Cyber Risk Governance

As discussed in the recent industry report issued by The Clearing House (the "TCH Report"),[41] board oversight of risk management and internal control frameworks, including cyber risk, is one of the core functions of a board of a large U.S. banking organization. Foundationally, this involves the board of directors and/or a board committee overseeing that the organization has established appropriate risk management and control programs and oversight of management's implementation of those programs.[42] While the approaches taken by individual boards will appropriately vary, as the TCH Report notes:

- What is referred to in the ANPR as the board's "credible challenge" of management may be exhibited through several different types of actions, such as asking informed, probing questions of management (e.g., informed and active boards may engage senior management in discussions regarding the institution's use of internal and/or third party assessments of cybersecurity risk management programs as well as examination findings and resources being dedicated to cybersecurity risk management).[43]

---

41 The Clearing House, "The Role of the Board of Directors in Promoting Effective Governance and Safety and Soundness for Large U.S. Banking Organizations," May 2016, available at https://www.theclearinghouse.org/~/media/action%20line/documents/volume%20vii/tch_report_the-role-of-the-board-of-directors-in-promoting-governance.ashx.

42 We recognize and appreciate that footnote 16 of the ANPR provides that a reference "to the board of directors is intended to include the board of directors or an appropriate board committee." *See id.* at Recommendation 2.

43 *See generally*, *id.* at 14-15. *See also*, The Clearing House's Guiding Principles for Enhancing U.S. Banking Organization Corporate Governance (2015 Edition), https://www.theclearinghouse.org/~/media/files/association%20related%20documents/20150624%20tch%20guiding%20principles%20for%20enhancing%20u%20s%20bank%20organization%20corporate%20governance.pdf (the "TCH Guiding Principles") at 12 and 43 for additional information relating to the nature of a board's "challenge" (noting that the effectiveness of this challenge cannot appropriately be evaluated based

- Reporting to the board of directors by senior leaders with responsibility for cyber risk oversight should generally relate to cybersecurity risks, developments, policies, and/or other issues that are material in nature to the organization consistent with the board's role in guiding the strategic direction of the organization and providing effective and objective oversight of management's performance in carrying out its responsibilities.[44]

- The performance of core board functions (such as oversight of risk management and control frameworks) at the various levels of the banking organization may be coordinated at the top-tier parent holding company level (taking into account the independent legal and governance responsibilities of subsidiary boards). Each board function should not need to be performed by the board or a board committee of each covered entity within the organization.[45]

Under the ANPR, the agencies are considering a requirement for covered entities to develop a written, board-approved, enterprise-wide cyber risk management strategy that is incorporated into each firm's overall business strategy and risk management. This would require (i) an articulation of how the covered firm intends to address inherent cyber risk, and (ii) board approval of the strategy and oversight of management's implementation of the strategy, as well as board review and approval of the enterprise-wide cyber risk appetite.[46] The ANPR also notes that the agencies are considering additional board-related requirements such as requiring boards to have sufficient cyber expertise or access to independent cyber expertise to help oversee cyber risk, and mandating that senior leaders within the company are (i) responsible for overseeing cyber risk, (ii) independent of business line management, and (iii) report directly to the board.[47]

There are instances where we believe the requirements being considered are overly prescriptive and unnecessary, especially as they would apply to OCC-regulated banks subject to the *Heightened Standards* and Federal Reserve-regulated Bank Holdings Companies with assets over $50 billion, which are already required to maintain enhanced supervisory processes with regard to cybersecurity.[48] While the agencies recognize in the ANPR that these standards are very similar to those already implemented by OCC and the Federal Reserve with regard to general risk management frameworks,[49] The Clearing House asks that any new standards clearly

---

on the number of challenges recorded in the minutes or elsewhere and that "a regulator could obtain a broader understanding of board challenge that occurs during or outside of board meetings by addressing the topic during the director interactions with regulators [as described in the TCH Guiding Principles]").

44 *See, generally, id.* at 11-12, 14-15, and 19-22.

45 *See generally, id.* at 8.

46 ANPR at 74320-21.

47 *Id.*

48 *See id.* at 73420. ("The agencies are considering standards under the cyber risk governance category that would be similar to the governance standards generally expected for large, complex financial organizations."). *See also id.* at note 15 (citing the *Heightened Standards* and Federal Reserve guidance, SR Letter 12-17, *Consolidated Supervision Framework for Large Financial Institutions*).

49 *Id.*

identify where the agencies expect OCC- and Federal Reserve-regulated entities to comply with additional requirements beyond those already applicable. Indeed, as noted above, regulators have already specifically identified cyber risk as one of the types of operational risks that is addressed by the *Heightened Standards*. The Clearing House further asks that the agencies ensure that any new standards are not unnecessarily duplicative—particularly if implemented as mandatory and inflexible.

According to the ANPR, one standard being considered is for boards "to have adequate expertise or to maintain access to resources or staff with such expertise."[50] It is critical that any final standard maintain flexibility in terms of how boards ensure an appropriately knowledgeable perspective on cybersecurity-related matters for purposes of carrying out their oversight responsibilities. Any final standard should allow each covered financial institution's board to make its own determinations regarding whether and/or under which circumstances it would be most appropriate for (i) one or more board member(s) to have particular cybersecurity expertise, (ii) the board to retain external cybersecurity experts for briefings or guidance, and/or (iii) the board to rely on their access to the financial institution's own resources or staff with such expertise, as well as assessments by third-parties engaged by management.[51] This is particularly important in light of the lack of general agreement as to whether it is a best practice for large entities to have at least one board member with cybersecurity expertise, or whether this could have unintended negative consequences, such as other board members deferring to the cyber expert entirely, and thereby forsaking their own obligations. Indeed, the *Heightened Standards* permit boards to rely on internal resources in maintaining its risk management standards.[52] The board of directors' role should be to provide informed oversight, and the board should have the flexibility to choose which source(s) to draw upon, in light of the facts and circumstances, to ensure it has an appropriately knowledgeable perspective.

The ANPR also proposes requiring that the board approve an enterprise-wide cyber risk management strategy that is incorporated into the overall business strategy and risk management of the firm. While we recognize that agencies may have intended the use of the term "enterprise-wide" to suggest that each covered entity within a banking group need not develop its own independent risk management strategy and cyber governance processes, we believe that this is a point that should be clarified. Flexibility should be maintained to ensure that each banking group

---

50 *Id.* at 74321.

51 Directors may choose to take advantage of different means to bring appropriately knowledgeable perspectives to cybersecurity-related matters. For example, these may include participation in relevant director education programs, whether provided in-house or externally. Moreover, as discussed in the TCH Guiding Principles, (i) it is a fundamental right of boards under applicable law to select and retain advisors where they determine that doing so is helpful to inform them in their exercise of their duties, and (ii) nomination and governance committees must balance many factors in filling board vacancies. *See generally* TCH Guiding Principles at Section 10 (Funding and Authority to Engage Advisors).

52 *See Heightened Standards* at 126 ("In providing active oversight, the board of directors may rely on risk assessments and reports *prepared by independent risk management and internal audit* to support the board's ability to question, challenge, and when necessary, oppose recommendations and decisions made by management that could cause the covered bank's risk profile to exceed its risk appetite or jeopardize the safety and soundness of the covered bank.").

can implement an appropriate and effective strategy and governance structure on a group-wide basis (i.e., to minimize possible risks of conflicting standards, unnecessary duplication of effort and actions by the boards of various "covered entities" throughout the organization, and unnecessary duplication of systems and resources).[53]

Finally, the ANPR proposes a requirement that boards ensure that covered entities maintain senior leadership who are responsible for cyber risk governance, independent of business lines, and with direct independent access to the board.[54] The Clearing House believes that such a requirement does not appropriately account for the ways in which financial institutions interact with their boards or how they organize their cyber roles and responsibilities:

Given the different nature of each covered entity's business and organizational structure, The Clearing House recommends that the agencies allow for the necessary oversight and organizational flexibility so that covered entities can appropriately manage cyber risk effectively, efficiently, and consistently with the agencies' goals and the financial institution's business structures. This includes (i) providing flexibility to permit senior cyber experts to report to the board via a more senior executive (such as the Chief Information Security Officer or Chief Risk Officer) to avoid confusion or lack of clarity that could result from too many staff members reporting to the board, and (ii) allowing senior leaders responsible for cyber risk governance to have both "business" and independent, cyber risk governance, functions where deemed appropriate by the board and management, taking into account considerations such as any inherent conflicts of interest that may arise.

2. Cyber Risk Management

Category 2 of the ANPR's Risk Management standards covers requirements for cyber risk management. Specifically, the ANPR calls for a "three lines of defense" model that would require at least three covered entity functions to include cyber risk management among their responsibilities. These functions would include (i) business units monitoring cyber risk and maintaining day-to-day management of that risk, (ii) an independent risk management function that would report to the board and Chief Risk Officer, and (iii) an audit function that would be responsible for determining whether the cyber risk management framework was compliant with applicable rules and regulations, and was sufficient to address the entity's cyber risk.[55]

As an initial matter, The Clearing House notes that the "three lines of defense" standard is drawn from the *Heightened Standards*, and, as such, many covered entities already have such a

---

[53] While the ANPR applies to "covered entities", cybersecurity risk management programs are often governed and designed at the holding company level and applied on a consolidated basis across the organization. Several of our member institutions have multiple affiliated entities (that would each independently be considered a "covered entity" under the proposal) that share IT resources and cybersecurity risk management frameworks. These covered entities may be subject to supervision by different agencies. The relationships in this regard among the holding company and other covered entities generally depend on the overall structure of the banking organization and will likely vary from organization to organization.

[54] ANPR at 74321.

[55] *Id.* at 74321-22.

model generally in place for risk management—including cyber risks. However, the *Heightened Standards* provide flexibility in developing these three lines,[56] and maintaining that flexibility is nowhere more important than it is for managing cyber risks.

a. First Line of Defense: Business Units

While other risks are most logically "owned" in the first instance by the business units, and while business lines certainly have an important role to play in the first line of defense to protect against cyber risk, there will not necessarily be an individual with cybersecurity expertise in each and every line of business. Taking a broader (e.g., enterprise-wide) approach to cybersecurity may also be far more effective than allowing individual business units to make their own decisions, by ensuring the businesses use consistent standards and eliminating gaps in cyber controls. As such, a more flexible approach would ultimately strengthen cybersecurity. Business units should be permitted to rely on information security professionals outside of the business unit as they manage that risk on a daily basis. The Clearing House therefore recommends that the agencies provide financial institutions with the flexibility to take a broader approach for the first line of defense.

b. Second Line of Defense: Independent Risk Management Function

The Clearing House similarly recommends that the agencies provide flexibility in the proposed requirement for the second line—the independent risk management function. Rather than mandating a specific reporting structure for this function, for example, The Clearing House recommends flexibility in allowing financial institutions to develop, or work within their existing, organizational structures and reporting chains, as long as the result effectively addresses cyber risks.

The ANPR also proposes requiring the independent risk management function to "continually" assess the firm's exposure to cyber risk.[57] Such a requirement suggests the need to assess on a constant, real-time basis, which is unrealistic. A more appropriate standard would be a requirement to assess on a "periodic" or "ongoing" basis.

Finally, the ANPR notes that "the agencies are considering requiring covered entities to assess the completeness, effectiveness, and timeliness with which they reduce the aggregate residual cyber risk of their systems to the appropriate, board-of-directors approved level." It also states that "[t]he Board is considering requiring covered entities, at the holding company level, to measure (*quantitatively*) the completeness, effectiveness, and timeliness with which they reduce the aggregate residual cyber risk of their systems to the appropriate, board-of-directors approved

---

[56] *See Heightened Standards* at 42 ("To allow covered banks some flexibility in designing their Framework, the final Guidelines provide that a front line unit may fulfill its responsibilities either alone or in conjunction with another organizational unit whose purpose is to assist a front line unit in fulfilling its responsibilities under the Framework.")

[57] ANPR at 74322.

level."[58] The ANPR does not clearly define what should be evaluated "quantitatively" from an IT risk perspective. The Clearing House recommends that the agencies either remove this proposed requirement entirely, or otherwise work with sector-wide industry groups to develop metrics that would be appropriate without being unnecessarily complex or burdensome.

c. Third Line of Defense: Audit Function

The Clearing House questions the appropriateness of the proposal to "explicitly requir[e] the audit function to assess whether the cyber risk management framework of a covered entity complies with applicable laws and regulations and is appropriate for its size, complexity, interconnectedness, and risk profile."[59] An entity's internal audit function would typically not be responsible for validating compliance with laws, regulations, or other standards, but would instead focus on evaluating, though sampling, whether the first and second lines have an effective process in place to ensure compliance. The proposed standards, as written, appear to require internal audit to go beyond this typical role. The ANPR similarly provides that the audit function's "evaluation would be required to include the entire security lifecycle, including penetration testing and other vulnerability assessment activities as appropriate based on the size, complexity, scope of operations, and interconnectedness of the covered entity."[60] It is not clear whether this statement would require the audit function to actually perform the penetration testing and other assessments, which is not typically part of the audit function's role, or to simply assess whether management's established program of testing is appropriate and effective.

The Clearing House recommends that the agencies revise the expected role of internal audit to better align with the audit function's typical and appropriate role. By ensuring that each business function continues to play its appropriate risk management role with respect to managing cyber risks, the agencies increase the efficacy of each function in managing that risk by allowing those functions to bring to bear their respective expertise.

3. Internal Dependency Management

The third category of standards proposed in the ANPR is focused on identifying and managing cyber risks from "internal dependencies" (i.e., business assets, including workforce, data, technology, and facilities). According to the ANPR, "[a] key aspect of the internal dependency management category is ensuring that covered entities ***continually*** assess and improve, as necessary, their effectiveness in reducing the cyber risks associated with internal dependencies on an enterprise-wide basis."[61] As discussed above in Section IV.B.2.b, a requirement to "*continually* assess and improve" the effectiveness of a program suggests a requirement to do so on a constant basis in real-time. The Clearing House recommends that this standard be revised to a more reasonable and realistic standard, such as to require periodic

---

58 *Id.* (emphasis added).

59 *Id.*

60 *Id.*

61 *Id.* (emphasis added).

assessment and improvement, or assessment and improvement when material risks have changed.

Another part of the internal dependency management requirement proposed in the ANPR states:

> The agencies are considering a requirement that covered entities maintain an inventory of all business assets on an enterprise-wide basis prioritized according to the assets' criticality to the business functions they support, the firm's mission and the financial sector. Thus, covered entities would be required to maintain a current and complete listing of all internal assets and business functions, including mappings to other assets and other business functions, information flows, and interconnections. Covered entities would track connections among assets and cyber risk levels throughout the life cycles of the assets and support relevant data collection and analysis across the organization.[62]

This proposed requirement, which would seem to apply to every single one of a financial institution's business assets, on an enterprise-wide basis, is exceedingly overbroad and would require significant administrative overhead, including tracking risk and connections of inventory assets throughout the asset's lifecycle. Even with respect to entities where a cyber incident could pose a systemic risk, these entities have hundreds—if not thousands—of business assets which pose little, or no, risk. Not only would the proposed standards require covered entities to have a complete inventory including those assets, but they also would be required to rank them in order of criticality to the business function they support—even if that business function is not a critical one – and expend extensive administrative effort to map these assets to "other assets and other business functions, information flows, and interconnections." This does not account for other controls that may be in place, such as internal firewalls or lack of connectivity with other, more significant, business units.

A financial institution could, for example, have its networks configured such that several of its "back office" functions (e.g., payroll, marketing, customer service, or procurement) are on a completely segregated network and in separate facilities from its core business functions. The standard proposed in the ANPR, however, would require each and every computer, printer, copy machine, scanner, and fax machine used by these functions to not only be inventoried, but also to be prioritized based on risk to *that* business function, and mapped. It is difficult to conceive of a scenario where doing so would strengthen the financial institution's cyber resiliency in any meaningful way. Instead, it would waste the financial institution's resources, diverting them from other efforts with the potential to actually improve cybersecurity.

To better align any standards with the ANPR's stated goals and our shared interest in continuing to strengthen and improve cybersecurity for the financial sector, The Clearing House recommends that any inventorying requirement be narrowed to apply only to those assets most likely to be material and pose a risk to the financial institution's cybersecurity.

---

62 *Id.* at 74323.

4. External Dependency Management

In the fourth category, the ANPR proposes standards regarding identifying and managing cyber risks from "external dependencies," such as vendors, suppliers, customers, utilities, and other third-parties. The Clearing House recommends a number of revisions and clarifications to these proposed standards in order to more adequately account for the varying nature of relationships, and thus the varying level of associated risks, between financial institutions and third-parties. As written, the proposed standards would require financial institutions to employ the same risk management standards for all third-parties, based on an inaccurate presumption that there is a singular relationship between financial institutions and their external dependencies.

First, similar to other aspects of the ANPR, the agencies should clarify the scope of third-parties that financial institutions would be required to consider under these standards. The ANPR would apply these standards to "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."[63] As written, this suggests that the requirements in this standard would apply to *all* third parties, including all vendors, with which a financial institution works, regardless of the level of connectivity (or lack thereof) to the institution's systems or information.

While financial institutions should generally assess the risk posed by third parties and appropriately manage identified risk, they should have the flexibility to implement risk management frameworks tailored to the relevant risk of particular third-party relationships. For example, financial institutions should be able to identify third parties posing little or no cyber risk to the financial institution either due to the particular relationships or available mitigations (for example, their lack of connectivity and access to data). This would allow financial institutions to focus their cyber-related external dependency management on those third-parties with the potential to pose actual, significant cyber risk. Without a risk-based, flexible approach, financial institutions would be required to expend extensive resources on administrative process, only a small percentage of which will actually serve to lower the overall risk, while the rest of this effort will simply divert scarce trained personnel to compliance efforts that do not bolster the institutions' or sector's risk profile. This could have a number of adverse consequences, including creating competitiveness problems for smaller banks and placing unnecessary barriers to financial institutions relying on a diverse array of innovative providers of on-demand services. As such, The Clearing House recommends that the scope of any substantive requirements be narrowed and risk-based, applying at most to third-parties with access to key systems or information.

Second, even if limited in scope to third-parties with access or connectivity, the proposed substantive requirements as outlined in the ANPR would create substantial overhead and documentation requirements (including keeping the documentation up-to-date) with questionable cybersecurity benefit. While The Clearing House appreciates the importance of managing cyber risk from vendors and other third-parties, standards should provide flexibility rather than a one-

---

63 *Id.* at 74320.

size-fits all requirement for every connection and every partner. The Clearing House, therefore, recommends that the standards instead permit each covered entity to identify the various technical scenarios under which third-parties are connected to or access their systems, have a defined set of connectivity/access standards to which it holds counterparties, and then apply the requirements of this section to that universe of connectivity options. Allowing financial institutions to assess their third-party oversight in such a systematic manner, rather than mandating individualized documentation, would dramatically streamline the administrative overhead as compared with the current proposal, while still ensuring that risks associated with each connectivity option are appropriately assessed and managed. This is particularly true for bank affiliates, which may be heavily interconnected, though perhaps with limited variation as to means of connection.

Third, as with the standards discussed in Sections IV.B.2.b and 3, above, the proposed standards for external dependency management provide that financial institutions should "continually assess and improve." First, the ANPR provides that "[a] key aspect of the external dependency management category is ensuring that covered entities continually assess and improve, as necessary, their effectiveness in reducing the cyber risks associated with external dependencies and interconnection risks enterprise-wide."[64] Later, the ANPR states that "the agencies are considering a requirement that covered entities continually apply and evaluate appropriate controls to reduce the cyber risk of external dependencies to the enterprise and the sector."[65] As discussed above, a requirement to continually assess suggests a constant, non-stop requirement to evaluate the programs, which is not a manageable standard. A requirement to "periodically" assess would be more appropriate.

Finally, as part of the ANPR's proposed requirement to monitor external dependencies, the ANPR provides that covered entities would be required to "prioritize monitoring, incident response, and recovery of systems critical to the enterprise *and the financial sector*. . ."[66] A requirement to prioritize monitoring of third-parties based on criticality to the sector at large would be incredibly broad and virtually impossible from a compliance perspective, since, read literally, this would require financial institutions to prioritize monitoring key utilities (e.g., power companies and internet service providers). The burden that would be imposed by such a requirement would far outweigh any benefits and is unworkable, where (i) it is highly unlikely that utilities will cede extensive vendor oversight to financial institutions, and (ii) the utilities are themselves in heavily regulated sectors with regulators who share the agencies' interest in cyber resiliency.

Different financial institutions may also have different views about which systems are critical to the financial sector because financial institutions sometimes lack visibility into the significance of a vendor's activities across the sector. For example, a vendor that is used by one bank but perhaps not in a critical way may be critical to a substantial number of other financial institutions, or may simply be used by a sufficiently large number of financial institutions to be

---

64 *Id.*

65 *Id.* at 74324.

66 *Id.* at 74323 (emphasis added).

sector-critical. The ANPR's approach risks inconsistent application of the new standard, or even requiring individual financial institutions to exercise significant oversight over a vendor that is not important to them solely because of the vendor's relationship with the institutions' peers. As such, The Clearing House recommends that any requirement or instruction to prioritize certain vendors be focused on those vendors that are significant to the individual financial institution at issue, and not the sector at large.

5. Incident Response, Cyber Resilience, and Situational Awareness

The final category of enhanced standards proposed in the ANPR covers incident response, cyber resilience and situational awareness, "designed to ensure that covered entities plan for, respond to, contain, and rapidly recover from disruptions caused by cyber incidents."[67] As with other portions of the ANPR, the standards proposed in this category are highly prescriptive, such that "[c]overed entities would be required to be capable of operating critical business functions in the face of cyber-attacks and continuously enhance their cyber resilience." In sum, the proposed standards in Category 5 of the ANPR are written in such a manner as to appear to require financial institutions to anticipate, and be prepared to respond to and recover from, any possible cyber risk, irrespective of probability. These requirements are another example of how the ANPR proposes issuing prescriptive requirements, departing from regulators' traditional risk-based approach to cybersecurity.

a. Incident Response

According to the ANPR, "[t]he agencies are considering a requirement that covered entities establish and maintain effective incident response and cyber resilience governance, strategies, and capacities," including requirements to "establish and implement plans to identify and mitigate the cyber risks they pose through interconnectedness to sector partners and external stakeholders to prevent cyber contagion." While entities that would be covered by the proposed standards have incident response programs, in line with current regulatory standards, these are typically reactive – i.e., *responsive* – programs, rather than proactive programs.

Under current standards, financial institutions are already required to have incident response programs. Supplement A to the *Interagency Guidelines*, the *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* ("*Guidance on Response Programs*"), requires financial institutions, as a "key part" of the institution's information security program, to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems."[68] The *Guidance on Response Programs* specifies the minimum components of a response program, including procedures for (i) assessing the nature and scope of an incident, (ii) notifying federal regulators and law enforcement, (iii) containing and controlling the incident, and (iv) notifying customers.[69]

---

67 *Id.* at 74324.

68 Supplement A to the *Interagency Guidelines*, Part II.

69 *Id.* at Part II(A)(1).

The FFIEC IT Examination Handbook Information Security Booklet also includes incident response program requirements. According to the Booklet, "[t]he goal of incident response is to minimize damage to the institution and its customers," and the program should include "defined protocols to declare and respond to an identified incident."[70] The Booklet further provides that "[m]anagement should prepare for potential incidents by developing an incident response plan that is comprehensive, coordinated, and integrated with existing institution policies, procedures, and training," and "periodically test" the plan.[71]

Both the *Guidance on Response Programs* and the FFIEC IT Examination Handbook generally require covered financial institutions to plan and prepare to respond to a breach. However, the focus is almost entirely on identifying, developing, implementing, and practicing procedures for post-incident. By contrast, the proposal described in the ANPR focuses on identifying possibilities that may trigger incident response. Identifying potential cyber risk scenarios can be an important exercise, but the dynamic nature of cyber threats and the complex nature of the financial sector and its systems makes it unreasonable to anticipate all possible threats. As such, The Clearing House recommends that any incident response program requirements, including requirements to identify cyber risks, be risk-, rather than outcome-focused, requiring financial institutions to be prepared for reasonably foreseeable risks rather than requiring them to be "effective."

b. Cyber Resiliency

The fifth category of the ANPR's proposed standards also includes requirements regarding resiliency following an incident. As with many of the standards discussed above, the proposed standards here warrant a holistic approach to cybersecurity, and should be clarified.

First, the ANPR notes that the agencies "also are considering a requirement that covered entities establish and implement strategies to meet the entity's obligations for performing core business functions in the event of a disruption, including the potential for multiple concurrent or widespread interruptions and cyberattacks on multiple elements of interconnected critical infrastructure, such as energy and telecommunications."[72] As written, this appears to suggest that financial institutions would be required to prepare for resumption of business operations even in the event of a widespread electrical and internet connectivity outage. While many, if not all, covered entities utilize backup data centers and other redundancies, this can only go so far, and financial institutions cannot be expected to replace core utilities in the event of a catastrophic, geographically dispersed, cyber attack. As discussed in Section IV.A.2, above, The Clearing House recommends that the government work with all critical infrastructure entities to prepare for such a scenario and ensure entities in other sectors are similarly hardened and resilient, rather than requiring entities in one critical infrastructure sector (the financial sector) to create plans to account for the disruption of another critical infrastructure sector. Such a holistic

---

70 FFIEC IT Examination Handbook Information Security Booklet at 50.

71 *Id.*at 51.

72 ANPR at 74324.

approach is the most effective way to ensure cyber resiliency by keeping cyber readiness and resiliency responsibilities with those best equipped to serve those functions in each sector.

Second, the ANPR provides that "[t]he agencies are [] 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."[73] The Clearing House requests that the agencies clarify whether this would only require an offline tertiary recovery system built on the same architecture/software as the financial institution's primary recovery platforms, or would require another system built on a completely different platform. Because the latter would be far more challenging to develop and keep updated on a real-time basis (and would therefore make recovery of updated data more challenging), The Clearing House recommends that this requirement apply only to tertiary systems built on the same platform as the primary recovery systems. Additionally, the proposed standard (and particularly the use of the word "immutable") appears to be adding a "write once, read many" (or "WORM") storage requirement, a standard that is often applied to data stored online to avoid data tampering. Applying such a requirement to off-line storage would be overly burdensome and costly without a countervailing benefit to cybersecurity or resiliency, because off-line storage is not subject to the same risk of modification as online data. The Clearing House recommends that the language of the proposed standard be revised to eliminate any potential requirement for WORM storage of offline data.

c. Situational Awareness

Finally, under the proposal outlined in Category 5, "covered entities would be required to establish processes designed to maintain effective situational awareness capabilities to reliably predict, analyze, and respond to changes in the operating environment."[74] This would include "a requirement that covered entities maintain an ongoing situational awareness of their operational status and cybersecurity posture," including "establishing[ing] and maintain[ing] threat profiles . . . [and] threat modeling capabilities; [and] gather[ing] actionable cyber threat intelligence."[75]

As written, this appears to suggest that, to comply with the standard, situational awareness would have to be sufficient to predict and preempt cyber events (in other words, be "effective"). It further suggests that financial institutions must know about every risk that could potentially affect them, such that if something goes wrong that an institution did not anticipate, the assumption would be that the institution is noncompliant with this requirement. This is a sharp departure from the traditional regulatory position: that the fact of a breach is not necessarily indicative of regulatory violations, and regulators' focus should be on the

---

73 *Id.*

74 *Id.*

75 *Id.* at 74325.

reasonableness of data security program and controls rather than the mere fact of a breach.[76]

While The Clearing House recognizes the importance of keeping apprised on the evolving threat landscape, mandating that situational awareness be "effective . . . to reliably predict" this evolution is to demand a level of perfection and clairvoyance that is impossible in an area like cyber where the risks and threats are constantly evolving. It is also unclear what actions financial institutions could take, beyond the robust information-sharing that the industry has already undertaken, to meet the agencies' expectations under this standard. The Clearing House suggests that any final standard clarify that financial institutions should use their best efforts to maintain situational awareness, while recognizing that any situational awareness may inevitably be imperfect, and provide financial institutions with suggestions regarding how agencies expect them to maintain situational awareness. Similarly, to the extent the requirement to maintain situational awareness includes modeling requirements, the agencies should provide further guidance as to how financial institutions can prove the models' validity to regulatory agencies, particularly in light of the rapid evolution of cyber-related threats.

C. The Agencies Should Clarify the Definitions and Standards for "Sector-Critical Systems" To Ensure that Requirements Are Clear, Practical, and Appropriate.

In Section IV of the ANPR, the agencies suggest defining "sector-critical systems," which would be subject to higher, "sector-critical standards," which are described in Section VI. The agencies should clarify and refine the definitions and standards outlined in these sections. As described more fully below, this is particularly true regarding the proposed (i) definition of "sector-critical systems," a term that is described differently in Sections IV and VI of the ANPR; (ii) requirement to implement the most effective commercially-available controls; and (iii) mandatory two-hour Recovery Time Objective ("RTO").

1. The Definition of "Sector-Critical Systems" Should Be Clear, Consistent, and Risk-Focused.

The Clearing House appreciates that the proposed tiered approach generally recognizes that there are varying risks even among covered entities. To the extent the agencies wish to pursue that approach, however, it is important that the definition of "sector-critical systems" be clear and appropriate. Section IV of the ANPR proposes defining these systems as those that

---

[76] *See, e.g.*, Stephen Joyce, *SEC Official Predicts More Cyber Enforcement Cases*, Bloomberg BNA (June 7, 2016), https://www.bna.com/sec-official-predicts-n57982073694/ (describing a speech by David Glockner, SEC Director of Chicago Regional Office, at a Practicing Law Institute Conference, where he said "The SEC has been quite clear that reasonableness and perfect are two different things. We expect firms to be diligent, we expect them to be thinking about this area, we expect that companies' procedures both from a policy perspective and a technology perspective are proportional to their risk."); Discussion Draft of H.R. ___, Data Security and Breach Notification Act of 2015: Hearing Before the Subcomm. of H. Comm. on Energy and Commerce, 114th Cong. 3 (2015) (statement of the Fed. Trade Com.) ("[T]hrough [the FTC's enforcement] actions and [consent] orders, the Commission has made clear that it does not require perfect security; that reasonableness and appropriate security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; and that the mere fact that a breach occurred does not mean that a company has violated the law.").

"support the clearing or settlement of at least five percent of the value of transactions 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"[77] and "other large, interconnected financial systems where a cyber-attack or disruption also could have a significant impact on the U.S. financial sector."[78]

The proposed definition introduces numerous uncertainties:

- *What scope of systems is intended to be included?* The current definition provides that these systems are those that "support" clearing or settlement. It is unclear, however, the scope that this is intended to cover. For example, would these further heightened standards apply only to clearing systems? Or would they apply to the entities involved in clearing and settlement, and all support infrastructure for clearing systems? As written, this definition is ambiguous.

- *How will the value of overall market be determined?* The definition in the ANPR relies on certain five percent market thresholds for systems in various financial sectors. To determine any individual entity's market share, however, the value of the market itself must be determined. Individual financial institutions do not necessarily have the market visibility to measure these markets' size or to determine the overall value of transactions settling or clearing them. The agencies should clarify (i) how they would calculate the value of different financial markets for the purpose of identifying sector-critical entities; (ii) what agency or other organization will be responsible for collecting the information necessary to determine the markets' size and calculating the corresponding five-percent figures; and (iii) whether the agencies will implement a process whereby the agencies ensure that analyses are consistently applied and communicated across the sector, since financial institutions will likely only know their own size, but not necessarily their relative size. In light of these challenges, and the importance of ensuring a risk-based approach, The Clearing House recommends removing this bright-line percentage-based standard entirely.

- *How would "key functionality" be determined?* Beyond the five percent threshold determination, the ANPR also proposes alternative methods of identifying sector-critical systems, including identifying systems that provide "key functionality to the financial sector for which alternatives are limited or nonexistent, or would take excessive time to implement."[79] This alternative definition should also be clarified. It is unclear, for example,

---

[77] ANPR at 74319.

[78] *Id.* at 74325. Notably, as drafted, the current definition limits sector-critical systems to those belonging to covered entities – meaning that a system could be systemically important and heavily interconnected, but because it is not maintained by an entity meeting the $50 billion asset-based cutoff in the proposed definition of covered entity, it might not be considered sector critical under the proposed standards. While, on the one hand, this is logical in that the standards for sector-critical systems are intended to be implemented in addition to the broader enhanced standards included in the ANPR, this underscores the need to apply a different, risk-based standard to the definitions of both "covered entities" and "sector-critical systems," since there may be systems that are systemically important that are maintained by entities that would not meet the definition of "covered entities."

[79] *Id.* at 74319.

who would determine whether a system provides "key functionality" and what the process would be for making that determination. The agencies should also clarify how long the agencies consider to be "excessive time" to implement an alternative, including (i) whether this relates to the two-hour RTO described in Section VI of the ANPR and Section VI.C.3, below; (ii) whether the meaning of this term could vary based on system criticality; or (iii) whether this determination should be made on a case-by-case basis.

- *How does the description of the term in Section VI relate to the proposed definition in Section IV?* Under Section VI of the ANPR, which designates standards for sector-critical systems, the term "sector-critical systems" is described differently than in the Section IV; the Section VI definition appears broader than the definition in Section IV because it includes any "large, interconnected financial system."[80] To ensure clarity regarding this important term, the definition of "sector-critical systems" should be consistent throughout any final standards.

In light of these ambiguities, the current proposal is simply not well-defined, and therefore, not workable. This definition must be clear and predictable in scope, and should provide financial institutions with sufficient predictability regarding whether a particular system or entity is "sector-critical."

In lieu of the proposed standard, The Clearing House urges the agencies to adopt a definition of "sector-critical systems" that is not only clear, but also both risk-based and narrow in scope, such that it only includes those systems where a cyber incident would truly have a significant impact on the marketplace. Even many systems that are critical to the clearing and settlement process are supported by readily-available substitutes and redundancies, such that downtime associated with a cyber attack would not necessarily be of such importance as to make further heightened standards appropriate. For example, while CHIPS serves an important role in settling payments, every participating bank could quickly re-route transactions through Fedwire if CHIPS were unavailable. In analyzing criticality, the agencies should take into consideration not only the roles that systems play in the ordinary course, but also institutions' ability to switch rapidly to alternative systems on a temporary basis. Unless a system directly provides non-fungible clearing and settlement services, operational downtime's impact due to a cyber event is simply unlikely to be so significant as to warrant further heightened standards.

The Clearing House further urges the agencies to ensure that each system determined to be "sector-critical" is designated using a risk-based standard that analyzes risks to the U.S. financial sector as a whole. For instance, if a system presents a great risk to an individual financial institution, but that system's compromise would not broadly affect the U.S. financial sector, it should not be considered "sector-critical." In light of the stringent requirements that would be imposed on sector-critical systems under the proposed regime, it is important that the definition of "sector-critical systems" appropriately capture the relevant systems and not unnecessarily sweep in other systems where a data security compromise would not pose a

[80] Specifically, Section VI of the ANPR says the term could include systems beyond "[c]ore clearing and settlement organizations" to include "other large, interconnected financial systems where a cyber-attack could have a significant impact on the U.S. financial sector." *See id.* at 74325.

systemic risk. This will allow financial institutions to properly focus resources where genuine risk exists rather than unnecessarily wasting resources on implementing controls that are out of sync with the actual risk profile.

The Clearing House's recommendations, therefore, are as follows:

- Rather than using an arbitrary, bright-line 5% threshold, the agencies should adopt a more targeted, multi-factor, risk-based inquiry and establish a process for designating systems falling within this category in order to provide financial institutions with predictability and certainty. To the extent possible, the framework should rely on existing frameworks used to determine systemic importance and risk, to avoid creating yet another separate category of entities subject to different requirements. This could include, for example, systems designated by the Financial Stability Oversight Council ("FSOC") as Systemically Important Financial Market Utilities ("SIFMUs") under Title VIII of Dodd-Frank,[81] or key systems used for settlement and clearing of payments maintained by entities identified by DHS and the Treasury Department as critical infrastructure at greatest risk pursuant to the Executive Order on Improving Critical Infrastructure Cybersecurity.[82]

- Systemic importance should be the driving factor in this analysis. While relative size could be one factor used in determining systemic importance, it should not be the definitive or even primary factor.[83] Instead, relative size should be analyzed in combination with other indicia of systemic importance, such as, (i) interconnectedness, (ii) function in clearing and settling payments, (iii) exposure to counterparties, and (iv) the effect of a failure on the financial system.

- Once a system is identified as systemically important, other risk-based factors can be used to determine whether the system is sufficiently sector critical to warrant applying additional standards. Such risk-based factors should include (i) absence of clear and redundant capability in the market, (ii) typical recovery time, and (iii) ability to recover up-to-date backup data.[84]

- To implement the proposed multi-factor test in a predictable and consistent manner, and to

---

81 12 U.S.C. § 5463.

82 Exec. Order No. 13,636 §8b (Feb. 12, 2013).

83 Risks could emerge from relatively small players such as financial technology firms, including data aggregators which leverage banks' data as part of their business model.

84 Notably, as drafted, the current definition limits sector-critical systems to those belonging to covered entities – meaning that a system could be systemically important and heavily interconnected, but because it is not maintained by an entity meeting the $50 billion asset-based cutoff in the proposed definition of covered entity, it would not be considered sector critical under the proposed standards. While, on the one hand, this is logical in that the standards for sector-critical systems are intended to be implemented in addition to the broader enhanced standards included in the ANPR, this underscores the need to apply a different, risk-based standard to the definitions of both "covered entities" and "sector-critical systems," since there may be systems that are systemically important that are maintained by entities that would not meet the definition of "covered entities."

ensure that any calculations regarding relative size are based on sector-wide visibility, the agencies should adopt a process – similar to the process developed by the FSOC in identifying SIFMUs[85] – to designate which systems will be deemed sector-critical systems. The Department of Treasury (perhaps through the Office of Critical Infrastructure Protection and Compliance Policy) may be the best-suited to make these designations in light of the Department's role and authorities regarding sector-wide cybersecurity.[86] Fundamentally, such a designation process should include compliance with minimal due process requirements, including notice and an opportunity to be heard, similar to the FSOC SIFMU designation process.[87] The Clearing House also encourages the Department to work with sector-wide industry groups, such as the CIPAC Working Group, FS-ISAC, or Financial Systemic Analysis & Resilience Center ("FSARC"), or via the FSSCC, in identifying which systems appropriately warrant this designation.

Finally, based on the ANPR, it is unclear whether the standards for sector-critical systems would also apply to the third parties supporting those systems. To the extent these standards would apply to third-parties, The Clearing House recommends that they should apply using the same standards and process outlined above, with any heightened standards applicable directly to the service providers rather than as vendor management requirements for covered entities.

2. A Requirement To Use the Most Effective, Commercially Available Controls Would Be Subjective and Overly Prescriptive, and Would Discourage Innovation.

The ANPR states that, among potential additional requirements for sector-critical systems, the agencies are "considering a requirement that covered entities minimize the residual cyber risk of sector-critical systems by implementing the most effective, commercially available controls."[88] This proposed requirement would be subjective and overly prescriptive, and would have an adverse effect by discouraging financial institutions from developing and implementing innovative custom tools.

First, such a requirement would be subjective, and would raise numerous questions regarding how financial institutions are expected to evaluate a particular control's effectiveness. For example:

- Would covered entities be required to go through the labor-intensive and costly process of

---

85 12 U.S.C. § 5463(a).

86 *See, e.g.*, Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (Feb. 12, 2013) (designating the Department of Treasury as the Sector-Specific Agency for the Financial Sector); Exec. Order No. 13,636 §8b (providing that Sector-Specific Agencies "shall coordinate with the Sector Coordinating Councils to review the [NIST] Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments").

87 *See* 12 U.S.C. § 5463(c).

88 ANPR at 74325.

testing every newly-available control to determine whether current controls or new controls are more effective?

- Would covered entities be allowed to share information with each other about newly-available tools without running afoul of other legal restrictions, such as antitrust laws?
- What metrics would covered entities use to determine a control's relative effectiveness?
- What is the scope of controls that would be required to meet this requirement?
- What if the best-available controls overlap with, and are duplicative of, each other?
- How can financial institutions ensure they have leverage with vendors to obtain appropriate vendor oversight and security contractual provisions where the financial institution may be required to use those vendors' services?

These questions would make this standard difficult, if not impossible, to implement in a consistent and reasonable manner.

Second, the proposed requirement is a very prescriptive approach, which is different than the more flexible "reasonableness"- and/or risk-based approach the Government has taken elsewhere. The NIST Cybersecurity Framework, for example, emphasizes risk-based approaches, while the *Interagency Guidelines* focus on reasonableness, providing companies with flexibility in assessing and improving their controls.

Third, while the focus on "commercially-available" controls is likely intended to avoid imposing requirements on covered entities to use non-commercially-available controls, the proposed requirement's prescriptive nature, as written, appears to actually limit covered entities' ability to develop and use their own, custom, in-house tools that are not commercially available. To the extent this requirement remains in any final standard, it should be written in a manner that provides financial institutions with the flexibility necessary to be innovative, while still recognizing that most entities will continue to rely on commercially-available tools and technology.

As such, The Clearing House recommends that the agencies revise this requirement to instead require operators of sector-critical systems to implement controls (either commercially-available or custom-developed) that are appropriate to control the applicable risks. The standard proposed in the ANPR would be difficult to implement and, in fact, erect numerous other barriers to innovation and vendor management such that efforts to comply with it could actually harm financial institution's cybersecurity posture. By contrast, The Clearing House's recommendation will provide operators of sector-critical systems with the necessary flexibility to manage their risks by determining (i) which risks apply to them, and thus need to be mitigated, and (ii) which combination of commercially-available or custom-developed controls would be most appropriate to reasonably mitigate present risks.

3. A Mandatory Two-Hour Recovery Time Objective Would Be Impractical, Risky, and Unnecessary.

The ANPR notes that the agencies are also "considering requiring covered entities to establish a two hour RTO for their sector-critical systems, validated by testing, to recover from a disruptive, corruptive, or destructive cyber event."[89] RTO is defined with reference to the *Sound Practices Paper*, as the "amount of time in which a firm aims to recover clearing and settlement activities after a wide-scale disruption with the overall goal of completing material pending transactions on the scheduled settlement day."[90] While a two-hour RTO may sound desirable or reasonable in the abstract, applying an inflexible requirement for resuming operations, irrespective of the circumstances, would be problematic for various reasons.

First, it is unclear from what time the recovery point is to be calculated. Cyber operations, unlike natural disasters, may not always be easy to detect, and a disruption, depending on how defined, may go unnoticed for some time. The Clearing House recommends that any RTO should be calculated from the time a cyber breach is confirmed and scoped with a high degree of confidence. This will allow covered entities to fully scope an incident – a critical step to ensuring the incident is contained and successfully remediated – prior to resuming operations.

Second, the standard has the potential to subject covered entities to inconsistent goals. Rather than meeting a two-hour standard, a covered entity's greatest concern should be resuming critical operations in a safe and sound manner, which, depending on the nature of the cyberattack and the state of the institution's forensic investigation, may or may not be possible in two hours. If an inflexible two-hour window is imposed, covered entities would run the risk of hastily applying short-term or ineffective solutions to resume operations. While a two-hour recovery period and completing settlement by the end of day is feasible on a fail-forward basis, covered entities should have the flexibility to determine the best recovery time based on factors such as the threat's magnitude, the covered entity's current business needs, and the availability of substitute vectors and alternative providers in the market.

Third, covered entities should have the flexibility to prioritize their systems and processes based on criticality. Depending on the scope of systems covered by the definition of "sector-critical systems," a covered entity's organic, risk-based prioritization may not be consistent with the agencies' application of increased standards.

Finally, the ANPR's consideration of a mandatory two-hour RTO does not acknowledge the possibility of compensating practices, such as stand-in processing or parallel analogue systems, such as the ability to switch from CHIPS to Fedwire, as described in Section IV.C.1, above. This is particularly puzzling in light of the reference to the *Sound Practices Paper* definition of RTO – which focuses on resumption of *activities*, whereas the proposed RTO in the ANPR appears to be focused on resumption of operation for particular systems.[91] Similarly, the

---

89 *Id.*

90 *Id.*

91 *Id.* ("With advances in technology and consistent with the two-hour RTO for core clearing and settlement

proposed RTO does not take into account variations based on time of day. For example, when a compromise occurs after close of business, such that settlement of transactions would not be affected as long as the system resumes operation by the following morning, there is no meaningful benefit to a two-hour RTO, particularly where speed is prioritized over safety.

Fundamentally, it is important to ensure that systems are brought back online in a safe and sound manner, and one that ensures that the systems will be sufficiently trusted by the rest of the industry to allow for full resumption of operations. This may be possible in two hours, but it may take longer. Standards should provide flexibility to allow covered entities to focus on resuming operations correctly rather than favoring speed over all other considerations.

Recognizing these concerns, other guidance provides flexibility in applying RTOs. Specifically, the recently-issued CPMI IOSCO cyber resilience guidance provides: "[n]otwithstanding [the] capability to resume critical operations within two hours, FMIs should exercise judgment in effecting resumption so that risks to itself or its ecosystem do not thereby escalate, while taking into account that completion of settlement by the end of day is crucial."[92] The *Sound Practices Paper* similarly provides:

> [F]irms that play significant roles in critical financial markets should plan to recover clearing and settlement activities for those markets *as soon as possible* after the core clearing and settlement organizations have recovered and resumed their operations and within the business day on which a disruption occurs. In some markets, such as wholesale payments, the banking industry has had long-established recovery *benchmarks* of four hours and the largest participants in the wholesale payments market have actively discussed the need for a two-hour recovery *standard* by such organizations. Firms that play significant roles in the other critical financial markets should *strive* to achieve a four-hour recovery time capability for clearing and settlement activities in order to ensure that they will be able to meet a within the business day recovery target.[93]

As proposed, however, the two hour RTO in the ANPR (i) would potentially be binding on certain covered entities, rather than guidance, (ii) could apply to more systems than the *Sound Practices Paper*,[94] and (iii) would provide far less flexibility than either the *Sound Practices Paper* or the CPMI IOSCO guidance. Accordingly, The Clearing House recommends that the RTO requirement be removed.

---

activities in the Sound Practices Paper, the agencies are considering establishing a two-hour RTO for the sector-critical *systems* of covered entities." (emphasis added)).

92 CMPI IOSCO Guidance on cyber resilience in the financial market at 16.

93 *Interagency Paper on Sound Practices To Strengthen the Resilience of the U.S. Financial System*, 68 Fed. Reg. 17809, 17813-14 (Apr. 11, 2003) (emphasis added).

94 ANPR at 74325 ("The scope of application of this proposed sector-critical standard could go beyond the core clearing and settlement organizations discussed in the Sound Practices Paper to include other large, interconnected financial systems where a cyber-attack or disruption also could have a significant impact on the U.S. financial sector.").

If the agencies include an RTO standard beyond the current guidance, The Clearing House recommends that the proposed standard be revised as follows:

First, The Clearing House recommends that, similar to how this standard is addressed in the CPMI IOSCO guidance and the *Sound Practices Paper*, any RTO should be framed as a goal, rather than a mandatory requirement that must be met regardless of competing considerations (such as safety). Covered entities have every incentive to reduce RTOs as much as technically feasible and prudent, and an unnecessarily prescriptive requirement is unlikely to further minimize RTOs without compromising safety.

Second, the definition of RTO and scope of application of any RTO standard should be revised. Currently, the proposed standard focuses on resumption of the particular systems at issue, even though the agencies' goal (based on the proposed scope of "sector critical systems") appears to be resumption of functionality sufficient to complete material pending transactions on the settlement date. Meeting this goal does not necessarily require either (i) resumption of operation for a particular system or (ii) full resumption of a particular system's entire functionality. Rather than taking an established term that does not fit with the agencies' proposal, the agencies should ensure that any standard is focused on their particular concerns (e.g., payment settlement) rather than unnecessarily relying on broad-brush terminology. Doing so would allow covered entities to focus on efforts that are actually tied to the agencies' goals.

As such, The Clearing House proposes defining RTO as the amount of time in which an operator of a sector-critical system aims to recover and/or resume the payment clearing or settlement functionality for which that system is used to working capability. This would (i) provide flexibility for financial institutions to rely on alternative systems, and (ii) limit the need to resume functionality only to those parts of the sector-critical systems that resulted in the system being designated as sector-critical.

Third, rather than establishing a mandatory, across-the-board, two-hour RTO, The Clearing House recommends that the agencies work with industry (such as through the CIPAC Working Group) to develop reasonable, tailored RTOs for specific high-impact plausible scenarios. The agencies should work with industry in a collaborative manner, both in identifying and developing the scenarios and determining what is a reasonable RTO for such scenarios, recognizing that both the available technology and threat landscapes may evolve over time.

Finally, rather than simply establishing an RTO, the agencies could serve a useful role in facilitating discussions with industry (such as through the CIPAC Working Group) to develop sector-wide protocols for returning interconnected, sector-critical systems to operation. The sector currently lacks agreed-upon protocols for resumption of operation following significant cyber attacks or data losses, such that, in the event of a major attack against a heavily interconnected and critical system, it is unclear whether or how – even if the system resumed operation within a prescribed RTO – the system operator would alleviate broader sector concerns regarding containment. This problem would be exacerbated if financial institutions understood that sector-critical system operators were being strong-armed by regulatory mandates to meet a prescriptive and arbitrary two-hour deadline rather than prioritizing safety and soundness. As such, The Clearing House recommends that the agencies work proactively with industry (such as through the CIPAC) to build protocols that can be (i) agreed upon by industry and (ii) applied

sector-wide, thereby allowing sector-critical systems to rejoin the sector community with confidence that the damage from such an event would not spread through inadequate understanding of the event, unintentional spread of corrupted data, or otherwise compromised systems or connections.

D. In Light of the Lack of Well-Developed Cyber Metrics, Adopting a Single Prescriptive Approach to Quantifying Cyber Risk Would be Premature.

Section VII of the ANPR states that the agencies "are seeking to develop a consistent, repeatable methodology to support the ongoing measurement of cyber risk," noting that "the agencies are not aware of any consistent methodologies to measure cyber risk across the financial sector using specific cyber risk management objectives."[95] As the agencies acknowledge, there is currently no single risk quantification model for cyber risks. Metrics for quantifying cyber risks are not developed or well understood in the marketplace and continue to evolve. What has become clear, however, is that such a determination would be subjective and require balancing considerations that vary, sometimes significantly so, by entity. In other words, cyber risk quantification is an "art," not a "science." These metrics continue to evolve, and experts have yet to identify best practices that are not only consistent and repeatable, but also applicable across companies or sectors.

As such, The Clearing House submits that adopting a single cyber risk quantification methodology, particularly in light of the prescriptive nature of the remainder of the proposed standards in the ANPR, is premature. Adopting a methodology prematurely could increase risk by forcing covered entities into an untested process, thereby using scarce resources without necessarily providing any accompanying benefit. To the extent the agencies do adopt a cyber risk methodology in the final standards, The Clearing House recommends that any such methodology be included only as flexible guidance, with the recognition that it may need to be modified, perhaps significantly, by individual institutions to adequately reflect emerging best practices and their needs and risks, thereby mitigating the potential for wasting resources on efforts that do not necessarily improve cyber risk management.

* * * * *

The Clearing House appreciates the opportunity to comment on the proposal. If you have any questions, please contact the undersigned by phone at (336) 769-5314 or by email at *Rob.Hunter@theclearinghouse.org*.

Respectfully submitted,

/S/

Robert C. Hunter
Executive Managing Director & Deputy General Counsel
The Clearing House Association L.L.C.

---

95 *Id.* at 74326.