**Dino Kos**
Head of Regulatory Affairs

**CLS Bank International**
Financial Square
32 Old Slip, 23rd Floor
New York, NY 10005

Tel: +1 212 510 4548
dkos@cls-bank.com

January 27, 2017

*Via email*

Robert deV. Frierson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW.
Washington, DC 20551
regs.comments@federalreserve.gov

**Re: Enhanced Cyber Risk Management Standards**
**Docket No. R-1550 / RIN 7100-AE-61**

Dear Mr. Frierson:

CLS Bank International ("CLS")[1] welcomes the opportunity to comment on the advance notice of proposed rulemaking, *Enhanced Cyber Risk Management Standards* (the "ANPR"), jointly issued by the Board of Governors of the Federal Reserve System (the "Board"), the Office of the Comptroller of the Currency (the "OCC"), and the Federal Deposit Insurance Corporation (together, "the Agencies"), and published in the Federal Register on October 26, 2016.[2]

As an Edge Act corporation under Section 25A of the United States Federal Reserve Act, CLS is regulated and supervised by the Board and the Federal Reserve Bank of New York (collectively, the "Federal Reserve") under a program of ongoing supervision, combining full-scope and targeted on-site examinations with a variety of off-site monitoring activities. Additionally, the central banks whose currencies are settled in the CLS system have established the CLS Oversight Committee, organized and administered by the Federal Reserve pursuant to the *Protocol for the Cooperative Oversight Arrangement of CLS,*[3] as a mechanism to carry out the central banks' individual responsibilities to promote safety, efficiency, and stability in the local markets and payments systems in which CLS participates.

In July 2012, CLS was designated a systemically important financial market utility ("DFMU") by the Financial Stability Oversight Council under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-Frank Act"). The Board is CLS's "Supervisory Agency" (as defined by the Dodd-Frank Act), and CLS is subject to the risk management standards set forth in Regulation HH. As a systemically important financial

[1] CLS was established by the private sector, in cooperation with a number of central banks, to mitigate settlement risk (loss of principal) associated with the settlement of payments relating to foreign exchange transactions. CLS operates the world's largest multicurrency cash settlement system (the "CLS system") and provides payment-versus-payment settlement in 18 currencies directly to 66 settlement members, some of which provide access to the CLS system for over 23,000 third-party institutions.

[2] 81 Fed. Reg. 74315 (Oct. 26, 2016).

[3] https://www.federalreserve.gov/paymentsystems/cls_protocol.htm.

market infrastructure ("FMI"), CLS is also subject to the *Principles for financial market infrastructures* (the "PFMI"), as applicable to payment systems.[4]

Under the scope set forth in the ANPR, CLS is a "covered entity" subject to the proposed enhanced cyber risk standards, and the CLS system may be identified as a "sector-critical system", subject to the proposed tier of more stringent "sector-critical standards" (collectively, the "Proposed Standards"). As such, CLS's comments focus primarily on the application of the Proposed Standards to DFMUs, and are directed to specific areas where CLS believes it can provide useful input. Section I provides general feedback and in particular, emphasizes the need for a flexible, risk-based approach to cyber risk management in line with existing regulatory guidance and requirements in the US, as well as globally. Section II responds to several of the Agencies' specific questions raised in the ANPR.

## I. General Comments on the Proposed Standards

CLS recognizes that cyber risk constitutes a significant and growing threat to the confidentiality, integrity, and availability of the global financial markets, and thus supports the Agencies' efforts to "provide a clear set of objectives for sound cyber risk management." The challenge of devising such guidance is all the more difficult given the international nature of the risk and the need for standards that are robust, yet sufficiently flexible to adapt to the dynamic and complex threat landscape. With this in mind, CLS submits three overarching principles to help guide the further development of the Proposed Standards.

*First*, cyber risks transcend sectors and sovereign borders; therefore, effective risk mitigation efforts require harmonization both within the US, as well as internationally. This is particularly important given the ANPR contemplates Proposed Standards for a broad range of covered entities and their third parties, most of whom are already subject to multiple legal and regulatory requirements and supervisory expectations.[5] Like CLS, most covered entities operate internationally and are subject to requirements in multiple jurisdictions. The proliferation of disparate cybersecurity terminology and frameworks requires firms to expend considerable resources to reconcile unique and potentially conflicting requirements, and makes effective communication and cooperation more difficult to achieve.[6] To the extent robust cybersecurity standards and practices are already established and embedded, the Agencies should avoid promulgating duplicative requirements that would impose significant costs on covered entities without providing commensurate benefits.

*Second*, the Proposed Standards should remain principles-based in order to afford covered entities the flexibility to adapt to the dynamic nature of cyber threats. As cyber threats evolve, so do best practices and technical standards to address them. Prescriptive regulation would be detrimental as the constant evolution of threats would render such requirements inefficient or even obsolete, potentially before full implementation. This concern was raised by the Board in the commentary accompanying its *Supervisory Rating System for Financial Market Infrastructures*, which states:

> "In assessing an FMI's performance under Regulation HH's requirements with respect to operational risk and cybersecurity policies and procedures, the Board will be guided by leading

[4] Committee on Payment and Settlement Systems ("CPSS") and Technical Committee of the International Organization of Securities Commissions ("IOSCO"), *Principles for financial market infrastructures* (Apr. 2012). Effective September 1, 2014, CPSS changed its name to the Committee on Payments and Market Infrastructures ("CPMI").

[5] For example, in assessing a DFMU's performance under Regulation HH, the Board is guided by information security and cyber risk standards such as the Federal Financial Institutions Examination Council Information Technology Examination Handbook (the "FFIEC Handbook") and the CPMI-IOSCO *Guidance on cyber resilience for financial market infrastructures* (June 2016) (the "CPMI-IOSCO cyber guidance"), both of which incorporate key concepts from the National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0* (Feb. 12, 2014) (the "NIST Framework") and other industry best practices.

[6] *C.f.* NIST Framework § 3.3 (explaining how the NIST Framework provides a common language to communicate requirements among independent stakeholders responsible for the delivery of essential critical infrastructure services); NIST, *Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1* §§ 3.3, 3.4 (Jan. 10, 2017) (the "Draft 2017 NIST Framework") (proposing additional guidance on communicating and verifying cybersecurity requirements with suppliers and technology partners).

information, communication and technology (ICT) and information and cyber security standards and guidelines. . . . The Board believes that *in light of the rapidly evolving IT and cyber risk landscapes, further specification of relevant industry guidance would date itself quickly.*"[7]

This view was similarly echoed in the final CPMI-IOSCO cyber guidance, which "is principles-based, recognising that the dynamic nature of cyber threats requires evolving methods to mitigate these threats. Guidance requiring specific measures today may quickly become ineffective in the future."[8] In the context of remarks addressing the (then draft) CPMI-IOSCO cyber guidance, a Federal Reserve Bank of New York official posited that "it may be preferable for market infrastructures to develop alternative solutions for responding to the cyber challenge, lest a monolithic solution result in an unintended concentration risk or an unhealthy 'groupthink'."[9] With this in mind, he offered a military analogy and cautioned against constructing "an inflexible Maginot line whose rigidities are easily subverted by a creative and nimble adversary." CLS recommends that the Agencies heed these concerns and develop regulatory guidance that allows covered entities to remain "creative and nimble" as well. The Proposed Standards should allow covered entities to adopt various elements of defense and in some cases, offense, but none of them exclusively.

A monolithic solution is likewise impractical given the diverse range of covered entities and third-party service providers potentially subject to the Proposed Standards. Large depository institutions, Board-supervised FMIs, and third-party service providers, for example, operate different businesses in different markets, and in turn, have materially different risk profiles. Rather than mandate a "one-size-fits-all" approach, CLS urges the Agencies to issue comprehensive, yet flexible, guidance and objectives that covered entities could then tailor to their specific operational and threat landscape, role in the sector, and legal and regulatory requirements.[10]

*Third*, proportionality should be given more prominence in the Proposed Standards, especially with regard to the relationship between covered entities and third-party service providers. Mandating prescriptive requirements for all service providers, without regard to criticality or interconnectivity risk would require covered entities to expend considerable resources to monitor compliance, and in turn, potentially divert attention from other activities aimed at improving cybersecurity prevention, detection, and response capabilities. Instead, covered entities should focus on service providers utilizing a tiered, risk-based approach that would promote a more efficient and effective means to enhance the overall cyber resilience of the sector.

## II. Specific Comments on the Proposed Standards

### Scope of Application

**Q2. What are the costs and benefits of applying the standards to covered entities on an enterprise-wide basis? If the agencies were to consider exempting certain subsidiaries within a covered entity from the standards, what criteria should be used to assess any such exemptions? What safeguards should the agencies require from a subsidiary seeking to be exempted from the standards to ensure that an exempted subsidiary does not expose the covered entity to material cyber risk?**

CLS believes it would be neither efficient nor effective to apply the Proposed Standards to all affiliated entities within a covered entity's corporate group without regard to the interconnectivity risk (or lack thereof) posed by

[7] 81 Fed. Reg. 58934 (Aug. 26, 2016) (emphasis added).

[8] CPMI-IOSCO cyber guidance § 1.2.2. *See also* Commission on Enhancing National Cybersecurity: Report on Securing and Growing the Digital Economy 8 (Dec. 1, 2016) (the "CENC report") (noting that the technology advances almost always outpace policy developments).

[9] Richard Dzina, Remarks at SIFMA's 43rd Annual Operations Conference: Toward a New Paradigm for Resiliency and Security (May 3, 2016).

[10] The *G7 Fundamental Elements of Cybersecurity for the Financial Sector* (Oct. 2016) exemplify this approach at a high-level. These non-binding, high-level fundamental elements build on the lexicon of Identify, Protect, Detect, Respond, and Recover used in the NIST Framework. They are designed to be universally applicable and dynamic, and can be tailored to the particular characteristics of, and specific cyber risks faced by, each entity.

the relationship. If a covered entity is exposed to cyber risk from an affiliate through a trusted connection or shared information infrastructure, then it would be appropriate to apply the applicable Proposed Standards to mitigate the risk from such connection or shared infrastructure. However, in such cases, the Proposed Standards should focus on measures that relate directly to the assets and processes that impose cyber risk on the covered entity, and not the affiliate's assets and activities more generally. For the avoidance of doubt, CLS recommends that the Agencies include language in the forthcoming proposals to state that the Proposed Standards would not apply to all affiliated entities within a covered entity's corporate group, except where expressly indicated.

**Q4. What are the most effective ways to ensure that services provided by third-party service providers to covered entities are performed in such a manner as to minimize cyber risk? What are the advantages and disadvantages of applying the standards to services by requiring covered entities to maintain appropriate service agreements or otherwise receive services only from third-party service providers that meet the standards with regard to the services provided, rather than applying the requirements directly to third-party service providers?**

CLS believes that direct application of the Proposed Standards to third-party service providers, where possible, would be the most effective and efficient means to ensure outsourced services are afforded the same level of cyber resilience that would be provided by the covered entity itself. Direct application would facilitate a consistent approach amongst covered entities and avoid costly and duplicative due diligence and reporting processes. However, where direct application is not possible, covered entities should be permitted to verify that third-party service providers meet the objectives of the Proposed Standards and adequately manage cyber risk related to the applicable services through contract provisions or other appropriate measures in accordance with their existing outsourcing or vendor risk management frameworks.[11,12] With respect to services provided by entities in other sectors or jurisdictions, CLS recommends that the Agencies coordinate with the relevant US government agencies and international authorities to ensure a comprehensive and harmonized approach. In all cases, CLS believes that requirements for third-party service providers should be tiered, risk-based, and focus on desired outcomes (*i.e.*, the intended level of cyber resilience afforded by the Proposed Standards), rather than impose a detailed checklist of requirements.

According to Section III of the ANPR, the Board is considering requiring nonbank financial companies and Board-supervised FMIs[13] to "verify that *any services* [such entity] 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" (emphasis added). Section IV further proposes that "*any services* provided by third parties that support a covered entity's sector-critical systems would be subject to the same sector-critical standards" (emphasis added). Whereas Section I of the ANPR explains that third parties that provide "payments processing, core banking, and other financial technology services" are vital to the financial sector, the Proposed Standards do not use this – or any other language – to limit the scope of such entities potentially subject to the Agencies' requirements. Instead, the Proposed Standards (including the proposed sector-critical standards) appear to apply to all third parties, providing *any services,* irrespective of the nature of the service and the interconnectivity risk (or lack thereof) posed by the relationship.

---

[11] *See* FFIEC Handbook, BCP, Appendix J (providing examples of contract terms that should be included to ensure risks incurred from third-party service providers are appropriately managed); CPMI-IOSCO cyber guidance § 4.3.1(b) (stating that "[c]yber considerations should be integral part of the FMI's arrangements for managing vendors and vendor products in areas of contracts, performance, relationships and risk"); Draft 2017 NIST Framework § 3.3 (proposing cyber supply chain risk management activities that include, *inter alia*, "[e]nacting cybersecurity requirements through formal agreement (e.g. contracts)"). *See also* PFMI Annex F (explaining that oversight expectations specifically targeted at critical service providers are "written at a broad level, allowing critical service providers flexibility in demonstrating they meet the expectations").

[12] To minimize duplicative reporting, to the extent the Agencies directly apply the Proposed Standards to certain services providers, covered entities should not be required to separately verify that such service providers satisfy the applicable requirements. Where covered entities receive covered services from third parties in support of sector-critical systems, and compliance with the sector-critical standards is not directly assessed by the Agencies, CLS submits that verification should only be required with respect to the additional tier of sector-critical standards, and not all Proposed Standards. In addition, covered entities should only be required to verify adherence related to the services provided by such third parties, and not the cyber risk management of such service providers generally.

[13] As used in the ANPR, the term "Board-supervised FMIs" includes, *inter alia*, DFMUs.

To align the Proposed Standards with existing risk-based regulatory frameworks,[14] CLS suggests that the Agencies refine the definition of "covered services"[15] or add a qualifying definition of "third-party service provider" that references a covered entity's "interconnected information infrastructure" and other "persons, processes, data, and information and common technologies, along with the environment and conditions that influence those interactions,"[16] rather than apply these terms in a way that would include parties with no link to or effect on the covered entity's cybersecurity posture. The scope of third parties potentially subject to the sector-critical standards is similarly ambiguous (*i.e.*, third parties that "support" a sector-critical system) and should be narrowly defined to include only those service providers essential to a sector-critical system's operations that maintain a trusted connection via shared information infrastructure.

Lastly, CLS notes that under the Proposed Standards, Board-supervised FMIs may be viewed as service providers to their participants, many of which are also covered entities. CLS therefore suggests that the Agencies specifically exclude covered entities from the definition of covered services so as not to inadvertently prescribe duplicative controls and reporting from such institutions. This approach would be consistent with the Agencies' objective to ensure services a covered entity receives from a third party are subject to the same Proposed Standards that would apply if the service was conducted by the covered entity itself.

**Q5. What are the advantages and disadvantages of applying the standards directly to service providers to covered entities? What challenges would such an approach pose?**

As noted above in response to Question 4, CLS believes that it would be more efficient for the Agencies to apply the Proposed Standards directly to third parties, which would also facilitate consistent application of the Proposed Standards and clarify potential ambiguity with regard to which third parties are in scope.

## Sector-critical Systems

**Q7. Do covered entities currently have access to sufficient information to determine whether any of their systems would be considered sector-critical systems for the purpose of the standards? If not, what additional information would be necessary for an entity to identify whether it has one or more sector-critical systems for the purposes of the standards?**

CLS believes that covered entities, and in particular, Board-supervised FMIs, have access to sufficient information to determine whether their systems would be considered sector-critical systems for purposes of the Proposed Standards. In fact, DFMUs subject to Regulation HH are already required to identify their critical operations and services related to payment, clearing and settlement.[17]

---

[14] According to the CPMI-IOSCO cyber guidance § 4.3.1, for example, "[t]he appropriate controls for each entity will depend on the risk that arises from the connected entity and the nature of the relationship with the entity." The FFIEC Handbook, Business Continuity Planning ("BCP") booklet Appendix J and the Board's Supervisory Letter 13-19, Guidance on Managing Outsourcing Risk (Dec. 5, 2013) similarly advise that a financial institution's service provider risk management program should be risk-focused and provide oversight and controls commensurate with the level of risk presented by the outsourcing arrangements.

[15] The ANPR defines "covered services" as "services provided to depository institutions and their affiliates that are covered entities." This definition does not include services provided to all covered entities, such as Board-supervised FMIs. Thus, to the extent the Agencies refine the definition of covered services, additional clarification may be warranted to provide a consistent, risk-based approach with regard to services provided to all covered entities.

[16] *See* National Initiative for Cybersecurity Careers and Studies, *Glossary of common cybersecurity terminology*, definition of "cyber ecosystem", http://niccs.us-cert.gov/glossary.

[17] *See* 12 CFR 234.3(a)(3)(iii)(A). All FMIs are similarly expected to identify their critical operations and services in accordance with PFMI Principle 3, Key Consideration 4. *See also* CPMI-IOSCO, *Recovery of financial market infrastructures* (Oct. 2014) (the "CPMI-IOSCO recovery guidance") § 2.4.2 ("An FMI should identify those services it provides that are critical"); § 2.4.3 ("In general, a systemically important FMI's payment, clearing, settlement or recording functions will be regarded as critical").

**Q8. What are the advantages and disadvantages of requiring covered entities to identify and report to the agencies their systems that support operations and meet the applicable thresholds to be considered sector-critical systems? Alternatively, what are the advantages and disadvantages of having the agencies develop a process to identify the systems of covered entities that support operations and meet the applicable thresholds to be considered sector-critical systems and to notify covered entities which of their systems would be subject to the sector-critical standards?**

The most efficient approach would be for covered entities to self-identify their sector-critical systems. The identification and reporting process should be conducted in close coordination with the covered entities' respective supervisory authorities and in line with existing regulatory requirements and guidance. Where covered entities are already required by the Agencies to identify critical services and operations, they should be allowed to utilize existing reporting channels so as not to introduce duplicative requirements.

Importantly, CLS notes that covered entities should not be required to publicly disclose which of their systems are determined to be sector-critical under the Proposed Standards to avoid inadvertently inviting attacks from malicious adversaries.

**Q11. What factors should the agencies consider in a measure of interconnectedness resulting in a system being determined as critical to the financial sector, and how should such factors be weighted? Commenters are asked to provide quantitative as well as qualitative support and analysis for proposed alternative methodologies, thresholds and/or factors.**

As noted above in response to Question 8, DFMUs subject to Regulation HH (as well as FMIs subject to the PFMI) already identify their critical operations and services with reference to the framework set forth in section 2.4.3 of the CPMI-IOSCO recovery guidance. CLS urges the Agencies to adopt a consistent approach, and implement Proposed Standards that consider:

- whether failure of a service is likely to have a material negative impact on participants or the financial market generally;
- whether failure of a service would give rise to contagion;
- whether failure of a service would undermine the general confidence of the market;
- the degree of substitutability and whether a service is provided by another [covered entity]; and
- whether users of a service can practically and effectively switch to an alternative service.

The ANPR contemplates the criteria for identifying "critical financial markets" in the *Sound Practices Paper*[18] as a starting point for designating systems that should be subject to a more stringent tier of cybersecurity standards; however, CLS notes that there are several regulatory frameworks in the financial sector that identify and prescribe requirements with regard to systemically important institutions and critical services and operations.[19] CLS therefore recommends that the Agencies rationalize their approach with existing frameworks and, to the extent a unique set of criteria is warranted, clearly differentiate the meaning of criticality for purposes of applying the sector-critical standards.

---

[18] Federal Reserve System, OCC, and the Securities and Exchange Commission ("SEC"), *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System,* 68 Fed. Reg. 17809 (Apr. 11, 2003) (the "*Sound Practices Paper*").

[19] *See* Exec. Order 13636, *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. 11,739 (Feb. 12, 2013) (directing the Department of Homeland Security to produce a list of critical infrastructure systems, drawing upon the expertise of Sector-Specific Agencies, including for the financial sector, the Department of the Treasury)); Financial Stability Oversight Council, *Authority to Designate Financial Market Utilities as Systemically Important*, 12 CFR 1320 (July 27, 2011) (establishing an analytical framework to identify DFMUs based on five categories and associated metrics that address specific considerations set forth in the Dodd-Frank Act); Federal Reserve System, *Enhanced Prudential Standards for Bank Holding Companies and Foreign Banking Organizations*, 12 CFR 252 (establishing a framework for the designation of systemically important financial institutions and critical operations for purposes of enhanced supervision and resolution planning).

## Cyber Risk Governance

**Q14. What are the incremental costs and benefits of establishing the contemplated standards for the roles, responsibilities, and adequate cybersecurity expertise (or access to adequate cybersecurity expertise) of the board of directors? To what extent do covered entities already have governance structures in place that are broadly consistent with the proposed cyber risk governance standards?**

The Proposed Standards in the *cyber risk governance* category regarding a covered entity's board of directors appear to be generally consistent with existing regulatory expectations for Board-supervised FMIs. As such, CLS expects that the costs to implement such measures will be reasonable.[20]

CLS welcomes the Agencies' flexibility with respect to the governance arrangements of third-party service providers. In particular, footnote 14 indicates that for these entities, it may be appropriate for some oversight functions to be performed by the business line executive management, rather than a board of directors or committee thereof. Accordingly, "enterprise-wide" is defined to encompass "the governance processes, policies, procedures, and controls related to or impacting the performance of services by a third party for a *depository institution, its subsidiaries, or affiliates*" (emphasis added). CLS believes that the same flexibility should be afforded to third-party service providers of all covered entities and suggests that the language in the ANPR be updated accordingly.

For the avoidance of doubt, to the extent the Agencies agree that the Proposed Standards in the *cyber risk governance* category are consistent with the requirements for DFMUs in Regulation HH, CLS requests that this be explicitly indicated. To this end, footnote 15 in the ANPR cites existing risk governance requirements applicable to OCC-regulated covered entities and Board-regulated large bank holding companies and nonbank financial companies, and clarifies that these covered entities would be expected to incorporate their cyber risk management strategy and framework into their overall risk management framework or risk appetite statement, as applicable. However, footnote 15 fails to refer to the requirements for DFMUs in Regulation HH, which among other things, state that the board of directors of the DFMU should establish a clear, documented risk management framework that includes the DFMU's risk-tolerance policy; assigns responsibilities and accountability for risk decisions; and addresses decision-making in crisis and emergencies.[21,22] The most efficient approach would be for a DFMU to embed its cyber risk management strategy and framework into its existing risk management framework and not segregate them into separate frameworks and documents unless there is a practical reason for doing so.[23] In addition, CLS suggests that the Agencies affirm that these concepts can be contained in the covered entity's existing frameworks wherever practicable, and separate documents would not be required, assuming such documents achieve the objectives of the Proposed Standards.

## Cyber Risk Management

**Q16. The agencies seek comment on requiring covered entities to organize themselves in a manner that is consistent with the contemplated enhanced standards for cyber risk management. Besides the**

---

[20] This assumes that the final guidance does not prescribe additional criteria deemed necessary to demonstrate "adequate cybersecurity expertise" or the ability to provide a "credible challenge" to management, and instead maintains deference to a covered entity's' particular governance arrangements.

[21] 12 CFR 234.3(a)(2)(F).

[22] *See also* ANPR footnote 17, which indicates that for Board-regulated covered entities, the Proposed Standard to "develop a written, board-approved, enterprise-wide cyber risk management strategy that is incorporated into the overall business strategy and risk management of the firm" would be part of the global risk management framework required by 12 CFR 252.33. Although similar requirements for DFMUs are set forth in Regulation HH, the ANPR does not specifically cite 12 CFR 234 in this respect.

[23] This treatment would be consistent with the CPMI-IOSCO cyber guidance § 2.2.3, which states that "[a]t the broader level, the FMI's cyber resilience framework should be consistent with its enterprise operational risk management framework. Such consistency is important and recognises that an FMI's cyber resilience framework is likely to share common elements with the policies, procedures and controls that it has established to manage other areas of risk."

**approach outlined in the ANPR, what other approaches could ensure that entities are effectively identifying, monitoring, measuring, managing, and reporting on cyber risk?**

In further developing the Proposed Standards in this category, CLS encourages the Agencies to maintain a principles-based approach so that covered entities can embed the appropriate measures into their existing enterprise risk management and governance frameworks.

In regard to the Proposed Standards for Business Units, as noted below in response to Question 17, CLS suggests that the Agencies revise the definition of "internal dependency" in line with existing regulatory guidance to refer to internal "technology assets", rather than "business assets."

With respect to the Proposed Standards for the Independent Risk Management function, CLS encourages the Agencies to adopt a flexible approach in developing requirements for a covered entity to quantitatively measure its cybersecurity posture. As noted in the CENC report, "the devil is in the metrics" – when it comes to assessing cybersecurity preparedness, there are no currently agreed standards in measurement.[24] Most current efforts to measure cybersecurity effectiveness focus on actions taken by an organization, rather than the effectiveness of such actions.[25] In fact, the Agencies concede that developments in this area are nascent, stating in Section VII of the ANPR that "[a]t this time [they] are not aware of any consistent methodologies to measure cyber risk across the financial sector."[26] Furthermore, as explained in NIST Special Publication ("SP") 800-184, *Guide to Cybersecurity Event Recovery,* certain areas of cybersecurity are highly subjective and comparing metrics among organizations or even within a single entity could produce misleading results.[27] As such, CLS believes it would be premature for the Agencies to prescribe specific quantitative requirements. Instead, covered entities should be expected to align themselves with leading standards, guidelines, and recommendations, reflecting current industry best approaches to measure and manage cyber risk.[28]

## Internal and External Dependency Management

**Q17. The agencies request comment on the comprehensiveness and effectiveness of the proposed standards for internal and external dependency management in achieving the agencies' objective of increasing the resilience of covered entities, third-party service providers to covered entities, and the financial sector.**

In general, the Proposed Standards in the *internal dependency management* ("IDM") and *external dependency management* ("EDM") categories are comprehensive; however, as described below, CLS suggests several clarifications and refinements to facilitate a consistent, flexible, and risk-based approach.

1. Terminology

CLS recommends that the Agencies clarify the definitions of "internal dependency" and "external dependency" to avoid any potential ambiguity and harmonize its approach with existing risk-based frameworks. In the ANPR, both terms are defined with reference to a dependency – that is, but for the given internal asset or external relationship (or associated information flows and interconnections), the covered entity would not be able to deliver its services, smoothly operate its systems, or achieve its business functions or mission. However, CLS is concerned that, as drafted, these terms could also be interpreted broadly to refer to *all* assets and relationships

[24] CENC report at 43. *See also* Center for Strategic and International Studies Cyber Policy Task Force, *From Awareness to Action: A Cybersecurity Agenda for the 45th President* 15 (Jan. 2017) (similarly noting that "[t]he lack of measurements on adoption and effectiveness remains a problem for assessing the framework", and recommending that NIST work with the industry to develop cybersecurity metrics).

[25] CENC report at 20.

[26] ANPR at 74326.

[27] NIST SP 800-184, *Guide to Cybersecurity Event Recovery* § 4 (Dec. 2016) (the "NIST Recovery Guide").

[28] *See* CPMI-IOSCO cyber guidance § 2.2.5 (recommending this approach for FMIs).

cited in the ANPR. For example, a covered entity may rely on certain vendors to perform their contractual obligations generally, yet failure to perform would not impact the smooth functioning of a covered entity's systems or prevent the covered entity from delivering its services. This latter interpretation would exponentially expand the required mapping, prioritization, and monitoring activities required in the IDM and EDM categories without regard to risk or criticality. In order to avoid such a potentially significant adverse unintended consequence, CLS believes that the Agencies must clarify the intended scope. This could be achieved by adding a footnote following the introduction of these terms in Section V of the ANPR, stating:

> "The terms 'internal dependency' and 'external dependency' refer to internal assets and external relationships (or associated information flows and interconnections), respectively, to which the covered entity is dependent upon to deliver its services, smoothly operate its systems, or achieve its business functions or mission. These terms are not intended to refer to all of a covered entity's assets and external relationships more generally."[29]

Alternatively (or additionally), the Agencies could clarify these terms separately. For example, the Agencies could supplement the current definition of external dependency to explain that the term is intended to refer to "external parties that the covered entity is dependent upon to deliver its services, smoothly operate its systems, or achieve its business functions or mission; and not outside vendors, suppliers, customers, utilities, or external organizations generally." Similarly, explanatory language could be added to the current definition of internal dependency to make clear the Proposed Standards are intended to address "assets that the covered entity is dependent upon to deliver its services, smoothly operate its systems, or achieve its business functions or mission; and not all internal assets generally."

With regard to the definition of internal dependency in particular, CLS also notes that the FFIEC Handbook's guidance on inventory and classification of assets does not use the term "business assets"; and instead refers to "technology assets", such as "hardware, software, information, and connections."[30] The NIST Recovery Guide similarly recommends that organizations "[c]reate and maintain a list of people, processes, and *technology* assets"[31]; and NIST SP 800-53 (Rev. 4) describes controls for organizations to implement in developing and documenting an inventory of "system components", which, in turn, are defined as "discrete, identifiable *information technology asset[s]* (e.g. hardware, software, firmware) that represent a building block of a[ ] system."[32] Absent any overriding reason to redefine the scope of assets subject to the IDM Proposed Standards, CLS underscores the importance of using consistent terminology to avoid confusing, duplicative, and potentially conflicting requirements.

2. Governance

CLS generally agrees that a covered entity's IDM and EDM strategies should be integrated into existing governance documents, where possible. However, the ANPR does not otherwise refer to a covered entity's "overall strategic risk management plan"; and it is not clear whether this term is intended to be used interchangeably with a covered entity's "overall risk management framework",[33] or "overall business strategy".[34] For the avoidance of doubt, CLS requests that the Agencies adopt uniform terminology.

---

[29] This proposed language is adapted from the definition of "interdependency" in the CPMI glossary (which refers to the "smooth functioning" of payment, clearing, and settlement systems based on direct and indirect interconnections), as well as from NIST SP 800-53 (Rev. 4), *Security Controls and Assessment Procedures for Federal Information Systems and Organizations* (Apr. 2013, *rev'd* Jan. 2015) (which describes security controls related to information technology assets in the context of an organization's business functions and mission).

[30] *See* FFIEC Handbook, Information Security § II.C.5.

[31] NIST Recovery Guide § 2.6 (emphasis added).

[32] NIST SP 800-53 (Rev. 4) CM-8 (emphasis added). *See also* NIST SP 800-171 (Rev. 1), *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (Dec. 2016) (definition of "system component").

[33] *See* ANPR at 74320.

[34] *See* ANPR at 74321.

To the extent that the Agencies contemplate certain policies, standards, and procedures for EDM throughout the lifespan of the relationship (*i.e.*, for due diligence, contracting and sub-contracting, onboarding, ongoing monitoring, change management, and off-boarding); CLS recommends that the Proposed Standards clearly indicate that separate documents with specific titles would not be required, so long as the relevant Proposed Standards are incorporated into a covered entity's existing documentation.

CLS appreciates the Agencies' emphasis on policies, plans, and procedures to identify and manage cyber risks associated with internal assets and external dependencies connected to or supporting sector-critical systems or operations. However, CLS notes that the term "sector-critical operations" used in the EDM category is not defined in the ANPR and requests that the Agencies clarify how this term is distinguishable from "sector-critical systems."

3. Inventory mapping and prioritization

CLS notes that the Proposed Standards in both the IDM and EDM categories regarding inventory mapping and prioritization are sufficiently comprehensive. CLS recommends that the Agencies' final guidance remain high-level and afford deference to covered entities to best determine how to categorize, map, and prioritize their applicable assets, external dependencies, and trusted connections. A prescriptive formula would not be appropriate or effective given the broad range of covered entities and third-party service providers potentially subject to the Proposed Standards. This intent could be conveyed by adding the words "as appropriate" to the respective Proposed Standards in the ANPR.

**Q18. What challenges and burdens would covered entities encounter in maintaining an internal and external dependency management strategy consistent with that described by the agencies?**

CLS references the clarifications and revisions suggested above in response to Question 17. Absent these changes, the Proposed Standards could impose significant costs on covered entities to the extent they require compliance with duplicative, and in some cases, conflicting, requirements and prescribe controls for internal assets and external parties without regard to risk or criticality.

## Incident Response, Cyber Resilience, and Situational Awareness

**Q23. How well do the proposed standards for incident response, cyber resilience, and situational awareness address the safety and soundness of individual financial institutions and potential systemic cyber risk to the financial sector, including with respect to the testing strategies and approaches? How could they be improved?**

As the Agencies further refine these proposals, CLS recommends that due consideration be given to ensure the Proposed Standards provide covered entities with sufficient flexibility to reevaluate and improve strategies based on lessons learned and routinely adapt to ever-changing tactics of illicit actors. As described above and in response to Question 37, CLS also urges the Agencies to avoid prescriptive requirements given the broad range of covered entities and third-party service providers, many of which operate internationally and are subject to numerous legal and regulatory requirements.

The ANPR states that due to the interconnectedness of the US financial system, a cyber incident at one interconnected entity may impact the safety and soundness of other entities with potentially systemic consequences.[35] As such, the Proposed Standards in this category would impose requirements on covered entities to consider the risks they bear from and pose to interconnected parties and the broader sector. However, comprehensive sector-wide resilience requires a strong private-public partnership, including meaningful collaboration amongst government agencies and international authorities. As explained in the CENC

[35] ANPR at 74316.

report, the private sector and government agencies must team up and take advantage of their respective capabilities and real time information about malicious actors, adversaries, threats, and vulnerabilities.

1. Transition plans

Although resiliency is an important goal, transfer of business is typically a response to financial distress and moral hazard, whereas portability of service better addresses cyber risks.

2. Testing strategies

With regard to the Proposed Standard for covered entities to conduct "specific testing that addresses disruptive, destructive, corruptive, or any other cyber event that could affect their ability to service clients", CLS suggests that the Agencies make clear that such testing should not be done in a way to cause disruption to a covered entity's normal functions or operations.[36] In line with existing regulatory expectations, management should determine the particular level and types of tests employed to ensure effective and comprehensive coverage, and the frequency and scope of tests should be a function of the level of assurance needed by an institution, as determined through the risk assessment process.[37] Additionally, reference to "any other cyber event" implies that covered entities would be required to test an infinite range of scenarios. CLS therefore suggests that this language be removed from the Proposed Standard, or in the alternative, qualified to refer to "any other *severe but plausible* cyber event *identified by the covered entity.*" This would provide a more reasonable, risk-based approach, consistent with existing regulatory expectations for FMIs,[38] as well as the proposed testing requirements in Section VI for sector-critical systems.[39]

CLS broadly supports the Proposed Standards for testing external interdependencies, which are generally consistent with existing regulatory expectations, but notes that joint testing may not be feasible in all circumstances. In certain cases, confirmations, table-top exercises, attestations, and other types of assurances from key partners and/or vendors may be the appropriate means of verification.

**Q24. What is the extent to which it would be operationally and/or commercially feasible to comply with requirements to use certain defined data standards in order to increase the substitutability of third-party relationships to reduce recovery times for systems impacted by a significant cyber event?**

CLS appreciates the importance of preserving data to facilitate safe and efficient resolution or recovery processes after a catastrophic event; however, requiring the use of certain defined data standards would not be an operationally or commercially feasible means to achieve these objectives. This is particularly true given the diverse range of covered entities and third-party service providers contemplated by the Proposed Standards, most of which operate not only in the US, but in the global financial sector. In some markets, transferring critical services from one entity to another is not a practical recovery option (*i.e.,* where there is only one entity that performs a specific service);[40] in which case requiring defined data standards may not improve recovery times or better facilitate substitutability for systems impacted by a significant cyber event. Even assuming the use of certain defined data standards were operationally and commercially feasible, mandating a prescriptive approach could have the unintended consequence of increasing systemic risk in the financial sector by proliferating a uniform solution that could be exploited by sophisticated adversaries.[41]

---

[36] *See* NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* § 6.4 (Sept. 2006).

[37] FFIEC Handbook, Information Security § IV.A.2.

[38] *See* CPMI-IOSCO cyber guidance § 7.2.1 (advising FMIs to design tests to simulate "extreme but plausible scenarios").

[39] Given the dynamic nature of cybersecurity and the ever-changing threat landscape, absent any qualifying language (*i.e.* "identified by the covered entity"), the range of "severe but plausible scenarios" could similarly impose a requirement for covered entities to test an infinite range of scenarios. Therefore, CLS recommends that the Agencies indicate in their forthcoming proposals that covered entities should utilize a tiered, risk-based approach in applying the testing standards (including requirements for sector-critical systems).

[40] CPMI-IOSCO recovery guidance § 2.1.3.

[41] The Agencies recognize that existing regulatory guidance calls for examiners to determine whether covered entities have plans to address recovery and resilience strategies for cyber-attacks that may disrupt access, corrupt data, or destroy data or systems. ANPR at 74324. *See*

## Standards for Sector-Critical Systems of Covered Entities

**Q29. The agencies request comment on the appropriateness and feasibility of establishing a two-hour RTO for all sector-critical systems. What would be the incremental costs to covered entities of moving toward a two-hour RTO objective for these systems?**

1. Appropriateness and Feasibility

CLS recognizes that sector-critical systems vital to the financial sector should endeavour to return to operational capacity as quickly as possible if a disruption occurs. CLS also understands the value of having target recovery time objectives ("RTOs") in place to provide consistent industry-wide goals to plan for and test against. However, with regard to feasibility, the Agencies should consider the challenges associated with a two-hour RTO in severe but plausible scenarios, as covered entities cannot test an infinite number of scenarios[42] or certify or guarantee that sector-critical systems will be resumed within a certain period of time in every case.[43] Indeed, in adopting Regulation HH, the Board recognized that following certain extreme cyber-attacks, it may not be possible for a DFMU to recover within two hours. In such cases, the Board indicated it would work with a DFMU through the supervisory process to prepare for and recover from such attacks.[44] The Agencies should also take into account that there may be severe scenarios that involve multiple institutions and that in such scenarios, an extended timeline may be appropriate to facilitate the extensive coordination efforts needed for safe and effective sector-wide recovery. CLS suggests that the Agencies address the inherent limitations of individual covered entities in this context and make clear in its forthcoming proposals that there may be cases where additional time would be appropriate for resumption of sector-critical systems.

In addition, it would be particularly challenging to require recovery within two hours given the inherent ambiguity around when this period should commence. Unlike physical disruptions, cyber events are difficult to detect and threat vectors are often present for a period of time before the disruption becomes apparent. A cyber event may involve software and data, as well as communication infrastructure, and it may not be immediately known to which extent they are affected. Applying a two-hour RTO necessarily requires the determination of a point from which this timeframe could be measured, which could only reasonably commence after the point of detection and identification.

In terms of appropriateness, a two-hour RTO may provide an appropriate target for covered entities to plan for and test against; however, RTOs "should not be regarded as hard and fast deadlines that must be met in every emergency situation."[45] In other words, the RTO should remain a recovery time *objective*, and not a mandate. The NIST Recovery Guide, for example, emphasizes the need for a balanced approach to conduct an effective

---

FFIEC Handbook, BCP, Appendix J (indicating that institutions should have a contingency plan in place that identifies alternate third-party service providers or in-house arrangements, as practicable, and addresses preparations required for such a conversion to the extent possible). *See also* CPMI-IOSCO cyber guidance § 6.4.1 (suggesting FMIs set up data-sharing agreements with relevant third parties to facilitate the quick recovery of uncorrupted data following a successful cyber-attack). A more feasible and effective approach would be for the Agencies to provide that each covered entity, together with the appropriate regulatory and/or supervisory authorities, should assess the options to improve cyber resilience and plans to recover from a significant cyber event, including cyber-attacks that may disrupt or destroy data, while respecting the general objectives of the Proposed Standards. Such assessment would take into account each covered entity's unique circumstances and requirements, including contingency plans and data sharing agreements.

[42] With regard to the proposed requirement that RTOs be validated by testing, as noted in response to Question 23, such testing should not disrupt normal functions and the costs and risks should be balanced against the effectiveness of the test.

[43] *See* CPMI-IOSCO cyber guidance § 6.2.3 (acknowledging that FMIs may not be able to safely resume critical operations within two hours and therefore advising FMIs to plan for scenarios in which the two-hour RTO is not achieved).

[44] 79 Fed. Reg. 65552 (Nov. 5, 2014).

[45] *See* the *Sound Practices Paper* at 17809. *See also* SEC, *Regulation Systems Compliance and Integrity*, 79 Fed. Reg. 72296 (Dec. 5, 2014) (explaining that in consideration of the views expressed during the consultation process, as well as the language cited above from the *Sound Practices Paper*, the SEC had revised the two-hour RTO provision to indicate that "stated recovery timeframes in Regulation SCI are goals, rather than inflexible requirements").

forensic investigation and rapidly restore systems to operational status.[46] Commencing recovery activities before an adversary's footprint and objectives are understood could trigger a change in tactics that would defeat the recovery operation and result in a reduced ability to discover impacted resources. Likewise, the CPMI-IOSCO cyber guidance explains that trade-offs may be required, and advises that notwithstanding the technological capability to resume critical operations within two hours, institutions should exercise judgment in effecting resumption so that risks to itself or the ecosystem do not escalate.[47] Covered entities must be afforded sufficient time to perform analysis and ensure the ability to recover to a stable state, so as to avoid merely recovering systems to the same vulnerable state that permitted the successful attack in the first place.[48] Resumption should also be balanced against other priorities, such as the necessity to preserve data or contain corruption.[49] The Agencies refer to cyber-attacks that may potentially corrupt or destroy critical data in Section V of the ANPR, but do not propose a set recovery point objective ("RPO") for all covered entities. Instead, the ANPR indicates that recovery strategies should be designed to achieve RPOs based on the criticality of data necessary to keep the institution operational. CLS believes a similarly flexible, risk-based approach should be applied in the context of the two-hour RTO, and particularly in cases where a forensic investigation is ongoing and/or resumption within two hours could potentially propagate malware or corrupted data through interconnected systems.

Lastly, CLS notes that there may be some ambiguity as to the meaning of recovery, as this term is not defined in the ANPR. According to the CPMI-IOSCO cyber guidance, to "recover" means to restore any capabilities or services that have been impaired due to a cyber event. The 2014 CPMI cyber report further explains that recovery "encompasses both the resumption of activities at a level which is considered 'good enough for a certain period of time' and full recovery, i.e. an eventual return to full service." The NIST Recovery Guide similarly recognizes that recovery is not a binary state, and in most cases "is far more complex [than simply rebuilding a system or restoring data from a backup], involving combinations of people, processes, and technologies."[50] Full recovery or restoration may not always be the immediate goal, and in such circumstances the most effective solution might include "an alternative or partial restoration as an interim measure."[51] In contrast, complete recovery or resumption would include any reconciliation required to address the potential data loss caused by the event, which, for international entities like CLS, would require concerted efforts with members across jurisdictions and time zones. Accordingly, to provide a clear, appropriate, and realistic approach, CLS recommends that the Agencies clarify the meaning of recovery for purposes of the Proposed Standards and in particular, the two-hour RTO. Specifically, CLS proposes the following language:

> "The term 'recover' means, for purposes of §§ [ ], to restore any capabilities or systems that have been impaired due to a cyber event. In applying the two-hour RTO, covered entities are expected to recover critical [clearing and settlement][52] activities performed by their sector-critical systems with the overall goal of completing material pending transactions on the scheduled settlement date. In all cases, a covered entity should resume sector-critical systems as soon as it is safe and practicable to do so without causing unnecessary risk to the sector or further detriment to financial stability."

---

[46] NIST Recovery Guide § 2.3.3.

[47] CPMI-IOSCO cyber guidance §§ 6.2.2, 6.4.2. This trade-off is similarly recognized in other jurisdictions. *See e.g.*, European Commission Delegated Regulation (EU) .../...of 11 November 2016 supplementing Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 with regard to regulatory technical standards on authorisation, supervisory and operational requirements for central securities depositories art. 78(2) (the "EU CSDR") (stating that in determining recovery times for each operation, a CSD should take into account the potential overall impact on market efficiency).

[48] *See* CPMI, *Cyber resilience in financial market infrastructures* 11 (Nov. 2016) (the "2014 CPMI cyber report").

[49] *See also* EU CSDR art. 78(2) (indicating CSDs should commence processing following a disruption to meet the two-hour RTO, unless doing so would jeopardise the integrity of the securities issues or confidentiality of the data maintained by the CSD).

[50] NIST Recovery Guide § 1. ("The status of recovery is usually better expressed as a gradient with different degrees of progress toward recovery at any given time for different systems or system components.").

[51] The NIST Recovery Guide further notes that "[a]chieving resilience might mean that a given resource is able to continue operation in a diminished capacity." *Id.*

[52] Or other applicable critical activities, based on the scope of the Agencies' forthcoming definition of sector-critical systems.

2. Incremental costs

Covered entities would likely incur significant incremental costs to implement this sector-critical standard, as concerted redesign strategies and improvements may be necessary to plan for and test against a two-hour RTO. As discussed below in response to Question 30, these costs may increase to the extent that covered entities would need to renegotiate existing contractual provisions with third-party service providers or seek alternative arrangements. CLS also expects that covered entities would incur significant costs to continue to meet the two-hour RTO following initial implementation given the comprehensive ongoing testing requirements, as well as the dynamic cybersecurity threat landscape and, in turn, constantly evolving and potentially infinite range of "severe but plausible scenarios."

**Q30. What impact would a two-hour RTO have on covered entities' use of third-party service providers? What challenges or burdens would be presented by the requirement of a two-hour RTO for covered entities who rely on third-party service providers for their critical systems? How should the agencies weigh such costs against other costs associated with implementing the enhanced standards outlined in this ANPR?**

To comply with the two-hour RTO, as set forth in the ANPR, covered entities would need to verify that all third-party service providers that support their sector-critical systems have adequate capabilities to resume operations within this timeframe.[53] For third-party providers of "covered services" that support sector-critical systems, the Agencies could assess compliance with the two-hour RTO directly. In either case, the meaning of services provided by third parties that "support" sector-critical systems is not clear. CLS believes this ambiguity must be addressed in the forthcoming proposals and, as noted in response to Question 4, recommends that the Agencies define the scope of third parties subject to the sector-critical standards to include only those who provide services essential to a sector-critical system's operations and maintain a trusted connected via shared information infrastructure. Such definition would be appropriate in the context of the two-hour RTO. Under existing regulatory frameworks, institutions are expected to identify, prearrange, and test comprehensive alternative measures to provide full resilience to their critical systems in the event a third party is not capable of meeting its obligations.[54] If a covered entity can meet the proposed two-hour RTO using alternative arrangements, then they should be permitted to utilize a given third-party service provider, even if that service provider cannot guarantee resumption within two hours in all cases. A third-party service provider should only be required to meet the two-hour RTO if there is a critical dependency and contingency arrangements are not readily available (*i.e.,* where a given service is unique and not offered by another provider and/or the timeframe to convert to an alternate system or implement in-house arrangements would exceed the RTO). Applying a tailored, risk-based approach would allow covered entities to focus monitoring and risk mitigation efforts on critical service providers in line with the Proposed Standards for EDM in Section V of the ANPR.

CLS also notes that the ANPR does not specifically address how covered entities must respond if a critical third-party service provider cannot sufficiently demonstrate adequate capabilities to resume operations within two hours. For example, must a covered entity disavow itself of the third party's services, even where a contractual relationship does not currently require compliance with a two-hour RTO (and if so, within what timeframe would this be expected)? Additional information is needed to assess the potential impact and practical implications on covered entities' existing arrangements. A flexible phase-in period should be permitted as covered entities may need to renegotiate existing contracts or make alternate arrangements.

---

[53] Section IV of the ANPR indicates that "any services provided by third parties that support a covered entity's sector-critical systems would be subject to the same sector-critical standards." Section V further explains that for a given Proposed Standard, references to covered entities "is intended to include application of the [Proposed Standards] to services provided to the covered entities, unless otherwise specified." The ANPR does not specify that the proposed two-hour RTO would only apply to covered entities; therefore, it appears covered entities would need to verify that all third-party service providers that support their sector-critical systems have adequate capabilities to resume operations in this timeframe.

[54] *See e.g.*, FFIEC Handbook, BCP, Appendix J ("A financial institution should have contingency plans in place to address alternatives for the resilience of services supporting critical operations if the current [technology service provider] cannot continue to provide the service.").

**Q31. How should the agencies implement the two-hour RTO objective? For example, would an extended implementation timeline help to mitigate costs, and if so, what timeline would be reasonable?**

An extended timeline would help mitigate costs, and more importantly, enable the safe and appropriately phased implementation of any new strategies and improvements that may be necessary for a covered entity to meet the two-hour RTO. Flexibility is essential as new solutions meant to decrease resumption time may comfort their own risks. In addition, an extended implementation timeline would be particularly helpful because, as discussed above, covered entities may need to renegotiate existing contractual provisions with third-party service providers or seek alternative arrangements.

As noted in response to Question 29, in adopting Regulation HH, the Board recognized that following certain extreme cyber-attacks, it may not be possible for a DFMU to recover within two hours. In such cases, the Board indicated it would work with a DFMU through the supervisory process to prepare for and recover from such attacks.[55] CLS encourages the Agencies to adopt this approach and work with covered entities through the iterative supervisory process to implement the two-hour RTO in a manner and within a timeline that is appropriate for a particular institution.

**Q32. Should different RTOs be set for different types of operations and, if so, how? Should RTOs be expected to become more stringent over time as technology advances?**

CLS believes it would be more effective for the Agencies to allow different RTOs for different types of systems and operations, especially given the broad range of covered entities (and their third-party service providers) potentially subject to the sector-critical standards. For example, for CLS, settlement of FX payment instructions and associated funding occurs within a five-hour period on business days, and thus, priorities in terms of resumption would vary according to whether a given disruption occurs during or prior to this window.

In addition, as noted in response to Question 29, there is some ambiguity around how the two-hour RTO should be calculated and when the period should apply. Unlike physical disruptions, cyber events are difficult to detect and threat vectors are often present for a period of time before the disruption becomes apparent. Thus, covered entities, in consultation with their supervisors, should be permitted to appropriately define when the two-hour RTO would apply and how it should be calculated for their sector-critical systems. These definitions should be iterative and take into account changes in technology and the cybersecurity threat landscape.

As technology evolves, it may be possible for covered entities to meet more stringent RTOs; however, as noted in response to Question 31, regardless of technological capability, new solutions to improve a covered entity's resumption capabilities should always be properly balanced against pragmatic and appropriately phased implementation to safely manage and mitigate any new and different risks that may be introduced.

**Q33. The Board requests comment on the benefits of requiring Board-supervised covered entities, at the holding company level, to measure the residual cyber risk of their sector-critical systems on a quantitative basis. How would this approach to measuring cyber risk compare with efforts already underway at holding companies to manage and measure their cyber risk? For example, what processes do holding companies already have in place to measure their residual cyber risk? What challenges and costs would holding companies face in measuring their residual cyber risk quantitatively? What are the benefits of requiring holding companies to reduce the residual risk of their sector-critical systems to a minimal level, taking into account the risks associated with internal and external dependencies connected to or supporting their sector-critical systems?**

CLS notes that for certain Board-supervised covered entities (*i.e.*, DFMUs for which the Board is the Supervisory Agency), a requirement to quantitatively assess cyber risk at the holding company level would conflict with the Proposed Standard in the *cyber risk governance* category for covered entities to incorporate

[55] 79 Fed. Reg. 65552 (Nov. 5, 2014).

their cyber risk management strategy into their broader risk management framework. Although such assessment may be practical for Board-supervised bank holding companies subject to 12 CFR 252.33, DFMUs subject to Regulation HH (12 CFR 234) do not necessarily maintain a comprehensive risk management framework or perform risk assessments thereunder at the holding company level. CLS therefore suggests that the Agencies' forthcoming proposals afford covered entities sufficient flexibility to determine the most effective and efficient means to assess cyber risk, in accordance with applicable regulatory requirements and in consultation with their respective supervisory authorities.

In addition, as noted above in response to Question 16, given the lack of mature measurement tools and agreed standards, it would be premature for the Agencies to implement prescriptive quantitative standards for purposes of determining what constitutes the "most effective controls." CLS recommends that the Agencies develop a more dynamic approach, similar to that set forth in the CPMI-IOSCO cyber guidance,[56] and require covered entities to implement appropriate controls in line with leading cyber risk standards, guidelines, and best practices to meet the objectives set forth in the ANPR. Such controls should be proportionate to a covered entity's threat landscape and systemic role in the financial sector, and consistent with its risk tolerance.[57]

## Considerations for Implementation of the Enhanced Standards

**Q37. What are the potential benefits or drawbacks associated with each of the options for implementing the standards discussed above?**

CLS strongly recommends that the Agencies implement the Proposed Standards through a policy statement or guidance. As noted in Section I of this comment letter, principles-based guidance would provide covered entities the flexibility to develop innovative, adaptive approaches and adopt industry best-practices to effectively respond to a dynamic cybersecurity threat landscape. In contrast, prescriptive regulation would be detrimental because the constant evolution of threats would render such requirements inefficient or obsolete, potentially before full implementation. This concern was specifically highlighted by the Board in its August 2016 commentary to its final supervisory rating system for FMIs,[58] as well as by the CPMI-IOSCO cyber guidance.[59]

Implementation of principles-based guidance would allow the Agencies to harmonize their approach with existing cybersecurity frameworks. This is important given the broad range of covered entities and third-party service providers covered by the Proposed Standards, and in particular, covered entities like CLS that operate internationally and are subject to requirements in multiple jurisdictions. A more prescriptive approach would increase the burden of complying with duplicative and potentially conflicting requirements, which would be neither cost effective nor necessary to achieve the desired level of cybersecurity.

**Q39. Which approach has the potential to most effectively implement the agencies' expectations for enhanced cyber risk management?**

For the reasons indicated in Section I of this comment letter, as well as above in response to Question 37, CLS believes that implementing the Proposed Standards through a policy statement or guidance has the potential to most effectively implement the Agencies' expectations for enhanced cyber risk management.

* * *

[56] *See* CPMI-IOSCO cyber guidance § 2.2.5.

[57] *See* CPMI-IOSCO cyber guidance § 4.2.1.

[58] 81 Fed. Reg. 58934 (Aug. 26, 2016) ("The Board believes that in light of the rapidly evolving IT and cyber risk landscapes, further specification of relevant industry guidance would date itself quickly.").

[59] CPMI-IOSCO cyber guidance § 1.2.2 ("Guidance requiring specific measures today may quickly become ineffective in the future.").

We appreciate the Agencies' consideration of the views set forth in this letter and would welcome the opportunity to discuss any of these comments in further detail.

Sincerely,

Dino Kos

cc: Naresh Nagia, Chief Risk Officer, CLS Bank International
Tom Zschach, Head of Technology and Operations, CLS Bank International
Vas Rajan, Chief Information Security Officer, CLS Bank International
Andrea Gildea, Assistant General Counsel, CLS Bank International
Kerry Denerstein, Regulatory Affairs, CLS Bank International