Via email

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

Date: 05 December 2022

Subject: Notice of Proposed Rulemaking – Regulation HH, Operational Risk (Docket No. R-1782)

Dear Ms. Misback,

CLS Bank International ("CLS") welcomes the opportunity to comment on the proposed amendments relating to operational risk management in Regulation HH issued by the Board of Governors of the Federal Reserve System (the "Board").

CLS is a special-purpose corporation organized under the laws of the United States of America and is regulated and supervised by the Board of Governors of the Federal Reserve System and the Federal Reserve Bank of New York (collectively, the "Federal Reserve"). CLS was designated a systemically important financial market utility ("DFMU") in 2012 by the United States Financial Stability Oversight Council under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-Frank Act")[1]. CLS is subject to the risk management standards set forth in Regulation HH.

1. General comments

CLS overall supports the Board's initiative to update the operational risk management requirements of Regulation HH given the changes in operational risk management practices, technology, and the regulatory landscape since it was last amended. CLS continually strives to adapt its own risk management framework to reflect fluctuations in risk severity and likelihood, changing environments, and industry best practices. It therefore believes that its risk management framework generally reflects the proposed requirements. However, there are several areas where CLS believes the proposals are drafted more broadly than is required to achieve the intended regulatory outcomes. This could lead to unintended consequences and therefore additional clarity in some areas would be beneficial. CLS encourages the Board to amend the proposed drafting of Regulation HH to clarify that DFMUs should apply a proportionate and risk-based approach with respect to all requirements and provides its specific observations below.

2. Effective date

CLS acknowledges the Board's proposal to have the changes become effective and require compliance 60 days from the date a final rule is published in the Federal Register. As noted above, while CLS believes that its risk management framework generally aligns with the proposed requirements, when the final rule is published further analysis will be required to identify the need for specific amendments to policies, procedures, and processes. In addition, time will be required to

[1] The Board of Governors of the Federal Reserve System is CLS's Supervisory Agent (as defined by the Dodd-Frank Act).

implement any required amendments, subject to CLS's governance processes. Furthermore, certain requirements may necessitate changes to contracts with third parties, which may require negotiation and agreement between CLS and the relevant third parties. Therefore, CLS suggests that the DFMUs be given a minimum of 180 days after publication to comply.

3. Review and testing

The draft proposal seeks to provide more specificity regarding the Board's expectations concerning the review and testing of a DFMU's systems, policies, procedures, and controls. While CLS welcomes additional clarity on the Board's expectations, CLS believes that the current drafting should be refined to provide for a risk-based approach to the design and management of a DFMU's testing program. CLS suggests that the proposed amendments should require DFMUs to have comprehensive documented risk-based testing frameworks that would incorporate the new requirements outlined of section § 234.3(a)(17)(i)(A), (B) and (C), contained in the draft proposal. DFMUs could then conduct review and testing activity on a proportionate basis in line with their documented risk-based programs that are subject to supervisory oversight.

With regards to the proposed requirements related to reviews to be conducted following material operational incidents or significant changes to the environment, for the avoidance of doubt, CLS suggests clarifying that required reviews relate **only** to systems, policies, procedures, and controls **relevant** to the incidents or significant changes.

Proposed § 234.3(a)(17)(i)(C) would require a DFMU to remediate "*as soon as possible, following established governance processes, any deficiencies in systems, policies, procedures or controls identified in the process of review and testing*". For several reasons, DFMUs may face limitations in their ability to remediate issues, and as acknowledged in the supplementary information of the notice of proposed rulemaking ("NPR"), the ("Supplementary Information"), and may need to make prioritization decisions with regards to the timing of remediation activity. While the current draft refers to DFMUs following "*established governance processes*" with regards to remediation, it is not clear whether this only relates to the need for validation of remediation work as mentioned in the Supplementary Information or is intended to be broader. CLS suggests that as a key element of a documented risk-based testing framework, a DFMU should set out its governance processes for managing and overseeing remediation, which would include processes for decision making on prioritization or remediation approaches, as well as validation as appropriate.

4. Incident management and notification

CLS has a documented framework for incident management which includes escalation and notification processes to stakeholders, including supervisory authorities. While CLS understands the importance of prompt notification of material operational events to relevant stakeholders, CLS is concerned that the notification requirements in the proposed regulation could lead to notifications that are unnecessary.

The proposed regulation requires DFMUs to immediately notify the Board when it invokes its business continuity plan ("BCP"), however it is worth noting that in some circumstances the invocation of a DFMU's BCP would not cause any disruption to critical services or operations. Examples might include invocation of BCP due to planned large scale public transport disruptions or severe weather events.

CLS is particularly concerned by the inclusion of "likely" and "potential" in the NPR. CLS suggests amending the proposed regulation to allow DFMUs a level of discretion in determining whether a notification is appropriate by considering the probability of the event happening, as well as the severity

of the outcome should it happen. In addition, with respect to the proposed requirement in §234.3(a)(17)(vi)(A)(2), CLS also suggests adding an additional condition to notification as follows: "*...where unauthorized entry, or the potential for unauthorized entry, into the designated financial market utility's computer, network, electronic, technical, automated, or similar systems that affects or has the potential to affect its critical operations or services and which could result in a serious detriment to participants or other relevant entities*"[2]. This language ensures that "*immediate*" notifications are limited appropriately with the understanding that DFMUs continue to adhere to other existing notification arrangements and communicate openly with supervisors in relation to incidents. Furthermore, as this provision is linked to the requirement to notify participants and relevant entities in §234.3(a)(17)(vi)(B)(2), it is important to ensure that notifications to participants and relevant entities are limited to avoid causing undue alarm. Finally, CLS suggests adding "*and which could result in a serious detriment to participants or other relevant entities*" to §234.3(a)(17)(vi)(B)(1). The provision of discretionary language in the regulation would allow DFMUs to comply with the letter of the regulatory requirement while at the same time liaising with their supervisors to ensure that the approach taken to assess the appropriateness of a notification meets supervisory expectations.

CLS welcomes the clarification of the requirement for "*immediate*" notification in the Supplementary Information but would encourage the Board to consider whether this could be incorporated expressly in Regulation HH to ensure participants and relevant entities have appropriate clarity. With respect to the practicalities of the notification process, CLS would support a process whereby it notifies its supervisory team, who in turn notify the Board as required. CLS suggests that such an arrangement, in addition to affording some discretion to DFMUs with regards to notifications (as described above), could provide a mechanism for monitoring and delivering feedback on mutual expectations.

In addition, CLS has some comments regarding the reference to "*disconnection*" in the Supplementary Information with respect to proposed §234.3(a)(17)(vi), which provides that in a cyberattack scenario, a DFMU should be operationally prepared to take, and should have a legal basis to take, appropriate steps to mitigate the risk of contagion to itself or other participants, including but not limited to disconnecting the participant from the DFMU if necessary. CLS notes that to protect CLS and/or its participants in certain scenarios, including a cyberattack, CLS has the ability to limit or restrict a participant's access to CLS, including the participant's access to functionality, as opposed to simply "disconnecting" the participant. To reflect this point, CLS strongly recommends corresponding changes to the relevant Supplementary Information.

5. Business continuity management and planning

CLS appreciates that the proposal would not change existing recovery and resumption objectives, specifically that a DFMU's BCP be designed to enable recovery and resumption no later than two hours following disruptive events and completion of settlement by the end of the day of the disruption, even in extreme circumstances. CLS suggests, however, that the amended regulation reflect the guidance provided by the Federal Reserve in the Supplementary Information, namely that "*these recovery time objectives should not be interpreted as a requirement for a designated FMU to resume operations in a compromised or otherwise untrusted state.*" The Supplementary Information recognizes that business continuity planning is a dynamic process, requiring that DFMUs work with supervisors to prepare for attacks and plan for contingency scenarios in which recovery and resumption objectives cannot be achieved. The amended regulation would greatly benefit from such additional color.

[2] See CLS's suggestion on the term "relevant entities" in Section VII of this response.

In addition, for the sake of clarity, CLS suggests some changes to the current reference to "*reconnection,*" set forth in §234.3(a)(17)(viii). CLS notes that there are various potential types of disruptions that may not result in the "*disconnection*" of external parties, including participants, from a critical service; in these circumstances, access to a critical service, or certain aspects thereof, may be unavailable or limited, including access to certain functionalities. Accordingly, CLS suggests the following amendments to proposed §234.3(a)(17)(viii)(D), which requires the DFMU to have a BCP that:

"*Sets out criteria and processes that address the ~~reconnection~~ resumption of access to ~~of~~ the designated financial market utility ~~to~~ by participants and other entities, including relevant functionalities, following a disruption to the designated financial market utility's critical operations or services.*"

6. Third-party risk management

CLS appreciates the inclusion of third-party risk management in the proposed regulation, as CLS has in place robust third-party risk management practices. However, for the reasons set forth below, CLS has proposed some important clarifying changes to the text of proposed §234.3(a)(17)(ix).

Firstly, the definition of "third-party" is overly broad and may unintentionally capture entities with which CLS may have a "business relationship" but does not treat as a traditional vendor providing services to CLS, for example CLS participants or employees. Further examples include central banks as well as RTGS systems and their respective operators (who may or may not be central banks)[3]. It is highly unlikely that CLS would be able to enforce bi-lateral information sharing relationships, or bi-laterally engage in business continuity management and testing, with these entities. CLS therefore suggests a narrower definition of third-party that, (i) expressly excludes central banks and operators of RTGS systems (and any other entities the Board deems appropriate); and (ii) is limited to those entities from which CLS receives services necessary for the performance of its designated services[4]. CLS notes that the latter point is captured in the Supplementary Information, which notes that third-party services in scope are those that "are essential to executing the designated FMU's payment, clearing, or settlement activities." Furthermore, as discussed above, CLS suggests that applying the requirements in a proportionate manner and using a risk-based approach is of paramount importance. CLS applies its most stringent risk management activity to those third parties that provide services that are critical to performing its designated services. Although the amended regulation states that the requirements should be applied "as appropriate," for the avoidance of doubt, CLS strongly recommends the inclusion of the concepts of criticality and proportionate applicability within the definition.

In the alternative, if the intent of the Board is to retain a broad definition of third-party, CLS would recommend that the general requirement to have in place third-party risk management practices could be applied broadly, but that specific requirements (information sharing relationships and inclusion in business continuity management and testing) should be applied, as appropriate, to those services that are considered critical.

Secondly, CLS suggests additional clarity to be provided regarding the intended scope of information sharing relationships. Depending on the risks presented by a service offering from a third-party, CLS may impose several notification requirements and governance practices, as appropriate, with a focus on ensuring these are more stringent with respect to its critical third parties. It would be beneficial to

[3] These RTGS systems are utilized by participants to fund their pay-ins to CLS in 18 currencies, as applicable, including but not limited to Fedwire, which is operated by the Federal Reserve Banks.
[4] For example, see the European Banking Authority. *EBA Guidelines on Outsourcing Arrangements, EBA/GL/2019/02. 25 February 2019. p.26 (as revised).*

clarify any specific expectations or relevant objectives as to the nature of such information sharing relationships. CLS also suggests additional clarity regarding expectations in connection with the inclusion of third parties in its business continuity testing. CLS notes that its ability to implement any new requirements will be contingent upon the agreement of the relevant third-party (and therefore may require negotiation and amendment of the relevant agreements with third parties, contingent upon the consent of the third parties); moreover, many third parties are established in jurisdictions outside the United States, and the agreements may be governed by the laws of those jurisdictions. Accordingly, as noted, it is possible that certain third parties will not agree to amendments that are proposed by CLS and CLS may not have sufficient leverage to request bi-lateral, bespoke amendments to terms (for example the amendment of standardized terms and conditions with utility companies) or to impose requirements to conduct bi-lateral, bespoke business continuity testing exercises. Moreover, even for third parties that agree to the amendments, the process of negotiating and amending agreements may take longer than 60 days and therefore, as previously noted, CLS supports a minimum of 180 days for compliance. CLS believes that it is important for Regulation HH to acknowledge these practical constraints.

Finally, CLS notes that certain third parties (e.g., SWIFT) provide critical services to multiple DFMUs and to systemically important financial market infrastructures located outside the United States (collectively "FMIs"). For those third parties, it is even less likely that CLS would be able to impose bi-lateral, bespoke requirements for information sharing and business continuity testing. For the sake of efficiency, CLS suggests that it would be beneficial for the Board to liaise with its counterparts in other jurisdictions to arrange for scenario exercises involving multiple FMIs, taking into account feedback from relevant stakeholders regarding the most relevant scenarios and key concerns, In addition, the Board may wish to consider whether direct or collective oversight of certain third parties may be appropriate in specific circumstances; CLS notes that this approach is under consideration by other regulators in other jurisdictions.

7. Technical revisions

CLS has reviewed the proposed technical revisions and provides the following comments:

I. Definition of operational risk
CLS is supportive of the proposed definition of operational risk which generally aligns to the PFMI and other best practices.

II. Definition of critical operations and critical services
CLS is supportive of the proposal to define and streamline references to "critical operations" and "critical services".

III. Cross-reference to "Other Entities" identified in § 234.3(a)(3) on Comprehensive Management of Risk
CLS notes the Board's proposal to add "*trade repositories*" to the list of "*relevant entities*" and has no objection to the addition, or the cross referencing included in the proposal; however, CLS suggests amending the term "*relevant entities*" to "*identified entities*" as this would allow the word "relevant" to be incorporated as needed, for example "The DFMU establishes criteria and processes providing for timely communication and responsible disclosure of material operational incidents to the designated financial market utility's participants and other identified entities as relevant."

IV. Operational capabilities to ensure high degree of security and operational reliability
CLS notes the proposed addition of the term "operational capabilities." However, CLS questions the need for additional terminology and instead suggests adding a reference to

"processes and controls" in addition to" policies and systems" to better align the overall terminology in Regulation HH. CLS is of the view that the proposed amendments in § 234.3(a)(17)(i)(A)(2) would apply to systems, policies, processes, and controls and the objective to have them function as intended would be achieved without the proposed additional terminology.

V. **Identify, Monitor, and Manage Potential and Evolving Vulnerabilities and Threats**
CLS welcomes the clarity provided by the proposed change and supports the amendment.

CLS appreciates the opportunity to comment and hopes its feedback is helpful to the Board in implementing a final rule that supports its desired regulatory outcome and ensures that DFMUs continue to apply the requirements of Regulation HH in an effective and risk-based manner.

We would be pleased to discuss any of these points in additional detail or to provide additional drafting suggestions.

Yours faithfully,

Marc Bayle De Jesse
Chief Executive Officer

CC: Gaynor Wood, General Counsel
Deb Hrvatin, Chief Risk Officer
Michelle Curtin, Head of UK & Corporate Compliance
Lauren Alter-Baumann, Head of Legal and Regulatory Projects
Craig Rubin, Senior Legal Counsel
Olivia Sirett, Legal Counsel and Commercial Specialist