April 1, 2024

Submitted via CFTC Comments Portal

Christopher Kirkpatrick
Secretary of the Commission
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, N.W., Washington, D.C. 20581

Re: Operational Resilience Framework for Futures Commission Merchants, Swap Dealers and Major Swap Participants

Dear Mr. Kirkpatrick,

The Securities Industry and Financial Markets Association ("SIFMA")[1] and the Institute of International Bankers (the "IIB")[2] (together, "the Associations")[3] appreciate the opportunity to comment on the Commodity Futures Trading Commission's ("CFTC" or the "Commission") rule proposal for requirements for an Operational Resilience Framework ("ORF") for Futures Commission Merchants ("FCMs"), Swap Dealers ("SDs"), and Major Swap Participants ("MSPs") (the "Proposal").[4]

---

1 SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's one million employees, we advocate on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association ("GFMA"). For more information, visit http://www.sifma.org.

2 The IIB represents the U.S. operations of internationally headquartered financial institutions from more than thirty-five countries around the world. The membership consists principally of international banks that operate branches, agencies, bank subsidiaries, and broker-dealer subsidiaries in the United States. The IIB works to ensure a level playing field for these institutions, which are an important source of credit for U.S. borrowers and comprise the majority of U.S. primary dealers. These institutions enhance the depth and liquidity of U.S. financial markets and contribute greatly to the U.S. economy through direct employment of U.S. citizens, as well as through other operating and capital expenditures.

3 This letter focuses on the Proposal as it applies to swap dealers and, as such, primarily uses the term "SDs" rather than "covered entities" and references the proposed 17 CFR § 23.603.

4 Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants, 89 Fed. Reg. 4706 (Jan. 24, 2024) [hereinafter *Proposing Release*].

The Associations commend the Commission's objective to introduce principles-based requirements that are robust, yet reasonably designed to identify, monitor, manage and assess risks relating to information and technology security, third-party relationships, and emergencies or other significant disruptions to normal business operations. The Associations agree with the Commission that any such requirements should be "sufficiently nimble to meet the challenges of the ever-evolving technological threat landscape and fit the unique business and risk profile of each covered entity."[5] Furthermore, the Associations welcome that, in general, the Proposal aligns with many existing practices that SDs have already successfully adopted to improve operational resilience and comply with current regulatory requirements that apply to the SD entities or the wider group structures within which they operate.[6]

While supportive of the approach, the Associations believe that parts of the Proposal undermine the Commission's stated objective of creating a principles-based rule on operational resilience, guided by proportionality and adopting a risk-based approach. Instead, because of a combination of the broad definitions[7] and certain prescriptive elements, the Proposal has the effect of creating a framework that diverts risk management resources and attention from areas that present bona fide risk to the covered entity. The current approach would also trigger significant workstreams for even relatively minor disruptions, which could materially detract from the efforts of SDs, FCMs, and MSPs to effectively manage significant operational challenges. Moreover, as the Commission recognizes, there are many regulators in the U.S. and internationally that are focusing on operational resilience. This expanded regulatory focus on operational resilience compounds the issues with the Proposal's broad-based definitions and prescriptive requirements given the risk of regulatory overlap and inconsistency. Thus, as these regulatory developments take shape, the need for harmonization and a principles-

---

5 *Proposing Release*, at 4710.

6 For example, performing risk assessments, creating incident response and business continuity plans, and establishing robust third-party risk management policies are standard practices for SDs. Moreover, these areas of focus are familiar to SDs through other regulatory regimes such as NFA Interpretive Notice 9070 and NFA Compliance Rules 2-9, 2-36 and 2-49. *See* National Futures Association, *Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49*, available at https://www.nfa.futures.org/rulebooksql/rules.aspx?RuleID=9070&Section=9.

7 The Associations agree with Commissioner Caroline Pham's statement that "it is very important for the Commission to be precise in the words that [it] use[s] for defined terms." CFTC, *Statement of Commissioner Caroline D. Pham on Operational Resilience Proposal for Swap Dealers and Futures Commission Merchants* (Dec. 18, 2023), available at https://www.cftc.gov/PressRoom/SpeechesTestimony/phamstatement121823b [hereinafter *Commissioner Pham's Statement*]. To that end, the Associations provide suggested definitions to certain defined terms in Appendix 1.

based approach increases so as to keep the target on standards and industry practices steady.

If the Commission is seeking to protect the industry from incidents that recently affected financial institutions, we recommend revisions that would help achieve that end. As much as possible, we have tailored our recommendations to reflect areas where the Proposal adds value to the operational resilience landscape as well as to identify areas that are duplicative of or inconsistent with other regulatory regimes and international standard setting bodies.

Unless the issues we discuss below are addressed, however, certain elements of the Proposal could ultimately inhibit an SD's ability to operate an effective, risk-based operational resilience program. In addition, such provisions could inundate the Commission with information that does not add value and could diminish the Commission's effective oversight of the ORF. The Associations believe the challenges the Proposal presents can be remedied and respectfully offer the following recommendations.

I. Overview of Recommendations

The Associations' recommendations generally focus on (i) enhancing the risk-based[8] foundation of the Proposal to focus on the delivery of critical operations and affording an appropriate level of flexibility, (ii) tightening the Proposal's definitions and (iii) harmonizing the Proposal with other existing and effective approaches to operational resilience. Ultimately, a risk-based approach is necessary to ensure the regulation provides sufficient flexibility for SDs to accommodate a wide range of operational, business, and management structures. For example, while many of the Proposal's requirements appear to limit obligations to the SD, in the context of consolidated programs or plans and for SDs for which only a small portion of the entity is performing SD activities, it is unclear how registered entities should adapt their existing enterprise-wide operational resilience programs that already cover the SD and are already aligned to other regulatory standards or standards of other international standard-setting bodies.

For ease of reference, the Associations' recommendations are generally organized according to the sections of the Proposal.

A. Operational Resilience Framework

The Associations believe that certain revisions to the General and Governance sections of the Proposal would provide much needed flexibility and make the ORF more

[8] Throughout this comment letter, the Associations use the term "risk-based" interchangeably with "principles-based."

risk-based. Specifically, the Associations urge the Commission to (i) future-proof the ORF standard to avoid the need for frequent revisions, (ii) define "operational resilience" in accordance with existing established and effective frameworks, (iii) confirm that SDs may rely on risk appetites and risk tolerance limits ("RTLs") set at the enterprise-wide level, (iv) provide greater flexibility for SDs relying on a consolidated program or plan, (v) adjust the approval of components requirement and (vi) clarify that SDs may use internal personnel to satisfy the reviews and testing requirements.

B. Information and Technology Security Program

The Proposal provides a risk-based approach for an information and technology security program by relating it to the proposed (b)(3)[9] standard but then deviates from that in setting out certain minimum requirements. The Associations understand the general need for certain baseline information and technology security requirements. However, the Associations are concerned that some of the minimum requirements conflict with the risk-based proposed (b)(3) standard. The Associations set out recommendations below to provide a more risk-based approach that is harmonized with other operational resilience and cybersecurity guidance and rules. Specifically, the Associations recommend changes to (i) requirements around specific controls, (ii) risk assessments, (iii) the definition of "incident" and the trigger for incident reporting, (iv) the timing requirement for incident reporting, (v) notifications to affected customers and (vi) escalation protocols.

C. Third-Party Relationship Program

The Associations agree with the Commission that SDs of varying sizes and complexities engage third parties in connection with a broad range of products, services and activities and that "the risks presented by individual third-party relationships may vary depending on the firm, the provider, or service."[10] The Associations appreciate the Commission's aim to establish regulations for third-party risk management ("TPRM") that adopt a risk-based approach and agree with its decisions to not prescribe more enhanced due diligence of subcontractors or affiliated third-party service providers but find that the Proposal in practice will impose overly broad requirements on SDs. However, the Associations believe that the existing requirements under NFA Interpretive Notice 9079[11] for the use of third-party service providers are sufficient and that the Commission should leverage such existing regulatory provisions instead of creating

---

[9] Proposed 17 CFR § 23.603(b)(3).

[10] *Proposing Release*, at 4722.

[11] National Futures Association, *Interpretive Notice to NFA Compliance Rules 2-9 and 2-36: Members' Use of Third-Party Service Providers*, available at https://www.nfa.futures.org/rulebooksql/rules.aspx?Section=9&RuleID=9079.

unnecessary regulatory overlap. To the extent the Commission believes it is necessary to augment the existing requirements, the Associations believe that any additional layers of regulation should be targeted towards particular high-risk services as we outline in our recommendations below.

In particular, the Associations provide suggestions below on (i) imposing heightened duties with respect to risk management practices on critical services rather than critical providers, (ii) the sufficiency of requirements for due diligence of subcontractors, (iii) aligning the exit strategy guidance with the intended risk-based approach, (iv) maintaining the proposed risk-based approach for third-party service providers that are affiliated entities, (v) clarifying inventory obligations for consolidated third-party relationship programs, (vi) confirming the scope of "potential" critical third-party service providers and (vii) narrowing TPRM obligations with respect to the "covered information" definition.

D. BCDR Plan

The Proposal's third component of the ORF requires SDs to develop a business continuity and disaster recovery ("BCDR") plan. Members of the Associations are already subject to current BCDR requirements under 17 CFR § 23.603[12] and NFA Interpretive Notice 9052.[13] While the Associations agree with the Commission that BCDR planning is essential to operational resilience, we also believe the existing requirements for BCDR planning are sufficient and that the Commission should leverage existing regulatory provisions instead of creating unnecessary overlap. Should the Commission find that it is necessary to enhance the existing requirements, the Associations believe the Proposal could benefit from certain practical changes and clarifications to components that involve BCDR. Specifically, the Commission should (i) adjust the trigger for notifications regarding BCDR activation to distinguish between major and minor disruptions, (ii) uniformly describe the core components individually as a "program" as opposed to, for BCDR, "plans," (iii) make the BCDR testing requirement more risk-based and (iv) maintain a flexible approach to BCDR recovery time.

E. Implementation Period

The Proposal's six-month implementation period is too short. The Proposal provides for complex requirements related to processes that often run on annual or other

---

[12] Members are also subject to BCDR requirements under the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System. Interagency Paper, 68 Fed. Reg. 17809 (Apr. 11, 2003).

[13] National Futures Association, *Interpretive Notice to NFA Compliance Rule 2-38: Business Continuity and Disaster Recovery Plan*, available at https://www.nfa.futures.org/rulebooksql/rules.aspx?RuleID=9052&Section=9.

periodic cycles, which makes implementation within six months challenging and, in some cases, impossible. In addition, based on past practice, non-U.S. entities that may seek to utilize the substituted compliance regime are unlikely to see that process completed within six months, creating uncertainty and inefficiency from having to implement temporary measures that may later prove redundant. The Associations urge the Commission to adopt a tiered implementation approach across a one- to two-year timeline at a minimum to enable a systematic program of mapping, testing, identification of risks and associated mitigation, with extended time frames for requirements that covered entities would be unable to implement either at all or meaningfully within the proposed time frame and to accommodate the substituted compliance determination process.

II. Recommendations

A. Operational Resilience Framework

As noted above in Section I.A., the Associations urge the Commission to (i) future-proof the ORF standard, (ii) define "operational resilience," (iii) confirm that SDs may rely on risk appetites and RTLs set at the enterprise-wide level, (iv) provide greater flexibility for SDs relying on a consolidated program or plan, (v) adjust the approval of components requirement and (vi) clarify that SDs may use internal personnel to satisfy the reviews and testing requirements.

1. *ORF standard – proposed paragraph (b)(3)*

The Proposal provides that covered entities' ORFs must be "appropriate and proportionate to the nature, size, scope, complexity and risk profile of its business activities as a swap entity, following generally accepted standards and best practices." Proposed 17 CFR § 23.603(b)(3) (emphasis added). The Proposal already requires SDs to create an ORF that is risk-based. Risk-based approaches invariably account for accepted standards and practices that best fit the entity. Moreover, requiring adherence to "generally standards and practices" is a vague reference and is likely to create uncertainty and confusion, particularly in the context of a rapidly developing landscape for operational resilience practices where consensus on what is considered generally accepted standards and best practices may be lacking. We propose deleting the underlined language as the Associations view the "appropriate and proportionate" standard to already include consideration for following accepted standards and industry practices.

2. *Operational resilience definition – proposed paragraph (a)*

The Associations recommend that the Commission define "operational resilience" to establish a common baseline understanding of the Proposal's scope and ensure a risk-based approach. The Proposal does not define "operational resilience" in the proposed

rule, notwithstanding that the Commission defines it as "the ability of a firm to detect, resist, adapt to, respond to, and recover from operational disruptions" in its surrounding commentary.[14] Specifically, the Associations recommend that the Commission define "operational resilience" in line with the Basel Committee on Banking Supervision ("BCBS") definition: "the ability of a [covered entity] to deliver critical operations through disruption" (emphasis added),[15] as cited by the Commission.[16] Should the Commission accept the Associations' recommended definition of "Operational Resilience," the Associations would urge the Commission to clarify that the usage of "Critical Operations" here is not intended to be consistent with or equivalent to Regulation QQ's[17] use of "Critical Operations."

As the Basel Committee explains, "[t]his ability enables a [covered entity] to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical operations through disruption." The Basel Committee further notes that, "[i]n considering its operational resilience, a [covered entity] should assume that disruptions will occur, and take into account its overall risk appetite and tolerance for disruption." The Basel Committee's limiting the definition to "critical operations" is consistent with the Associations' view that such a definition would better focus the regulation on true operational resilience, as opposed to broader business continuity which is already well regulated.

Accordingly, the Associations recommend that the Commission adopt an operative definition of "operational resilience" of: "the ability of a firm to deliver critical operations through disruption." To operationalize this definition, the Associations also recommend that the Commission adjust the scope of proposed paragraphs (b)(1) and (b)(3) by adding "To ensure operational resilience …" at the beginning of both provisions.

---

14 *Proposing Release*, at 4707.

15 *See* Basel Committee on Banking Supervision, *Principles for Operational Resilience*, at 3 (Mar. 2021), https://www.bis.org/bcbs/publ/d516.pdf. This definition also aligns with description of operational resilience in the Interagency Paper on Sound Practices to Strengthen Operational Resilience. SR 20-24, *Sound Practices to Strengthen Operational Resilience* (Nov. 2, 2020), available at https://www.federalreserve.gov/supervisionreg/srletters/SR2024.htm ("Operational resilience is the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard. It is the outcome of effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions.").

16 *Proposing Release*, at 4707 n.11.

17 12 CFR § 243.2.

3. *Risk appetite and risk tolerance limits – proposed paragraph (c)(2)*

The Proposal provides that, as used in the proposed rule, RTLs would be limited to the context of the risks identified in proposed paragraph (b)(1) of the proposed rule, rather than as the term is used in the Commission's Risk Management Program ("RMP").[18] In contrast to RTLs that SDs have set for RMP purposes, reliance on RTLs set at the enterprise level makes sense in the context of the ORF. In fact, considering RTLs at the enterprise level can help facilitate more effective management of risks to operational resilience that have potential impact beyond swap dealing activities. For example, natural disasters or cybersecurity attacks that impact business operations throughout the firm are more effectively managed in a firmwide manner that is agnostic to specific SD activities.

The Associations therefore strongly believe that, for SDs that opt under proposed paragraph (c)(4) to follow an enterprise-wide program in setting their risk appetites and RTLs, the SDs should be able to rely on the enterprise-wide program's risk appetites and RTLs and that the SD does not need to create risk appetites and RTLs specific to the SD so long as the enterprise-wide risk appetite and RTLs are "appropriate to" the SD.[19] This position would not compromise the SD's ability to effectively establish, document, implement and maintain operational resilience and would align with the Commission's objective in producing a risk-based regulation.

4. *Consolidated programs, plans and attestations – proposed paragraph (c)(4)*

The Associations welcome the Proposal's inclusion of the provision permitting SDs to rely on an enterprise-wide consolidated program or plan to satisfy the ORF requirements. We understand that this provision would apply to consolidated programs or plans of both U.S. and non-U.S. entities.

Indeed, the Commission rightly points out that many SDs function as a division or affiliate of a larger entity or holding company structure, which generally monitors and manages relevant operational risks at the enterprise level to address the risks holistically and to achieve economies of scale. The Proposal helpfully recognizes the benefits of

---

[18] *Proposing Release*, at 4715 n.93.

[19] For the sake of clarity, the Associations would also recommend that proposed paragraph (c)(4)(i) specify that an SD may also satisfy the requirements of paragraph (c)(2)(i), in addition to paragraph (b)(2), in the manner described in such paragraph.

such a consolidated approach and does not appear intended to interfere with an SD's operational structure.[20]

However, the Proposal would require SDs to have their senior officer, an oversight body or a senior-level official attest annually in writing that the consolidated plan or program meets the rule requirements and reflects risk appetite and risk tolerance limits appropriate to the SD. Proposed 17 CFR § 23.603(c)(4)(ii).

We believe this is not the right standard and is overly prescriptive for several reasons.[21] As an initial matter, "meets the rule requirements" is a standard that fails to build in any level of deference to the consolidated program established to meet a number of other regulatory requirements, essentially imposing the CFTC's terms on the group program for that program to qualify. Instead, the standard should be "comparable" or "achieves the same policy outcomes."

Second, any broad-based program that fully encompasses the SD should be able to be assessed under proposed paragraph (c)(4), regardless of whether it applies "enterprise-wide" on a "consolidated" basis. For instance, if the program were applicable to the global bank of which the SD is one division but is not also applicable to each of the bank's affiliates, some of which may instead have their own programs, this should not disqualify the program. Similarly, to avoid uncertainty and potential enforcement risk, proposed paragraph (c)(4)(i) should clearly state that SDs are not required to build out separate requirements or processes specific to SD activities, *e.g.*, setting risk appetites and RTLs as discussed above, as long as such activities are covered in the consolidated program. If this is not the Commission's position, the proposal must provide clarity on precisely which requirements would continue to apply separately to SDs that would rely on a consolidated program in order to be considered compliant with the Proposal's requirements.

Third, the current language could be read as requiring full reliance on a program or plan, whereas partial reliance should equally be possible if a firm prefers to demonstrate some elements of the CFTC rule at the level of the registrant and others in reliance on proposed paragraph (c)(4).[22]

---

[20] *See Proposing Release*, at 4715.

[21] The Associations appreciate Commissioner Pham's request for suggestions on appropriate attestation language and respectfully offer this feedback. *See Commissioner Pham's Statement*, *supra* n.7.

[22] For example, NYDFS Part 500.2(d) allows covered entities to meet Part 500 requirements "by adopting the relevant and applicable provisions of a cybersecurity program maintained by an affiliate" (emphasis added).

Furthermore, the Commission currently requires chief compliance officers ("CCOs") to prepare an annual report that describes, *inter alia*, the SDs' written policies and procedures that are required to be established pursuant to Commission regulations, as well as the effectiveness of such policies and procedures, areas for improvement and material noncompliance issues.[23] Given this existing reporting mechanism, we recommend the Commission provide greater flexibility for SDs to demonstrate that the consolidated program, to the extent it is being relied on, is "comparable" or "achieves the same policy outcomes" by allowing SDs to either (i) cover compliance with the proposed ORF requirements in the CCO report in lieu of an attestation or (ii) to elect to submit an attestation.[24]

Finally, the Associations also recommend allowing SDs that are part of a foreign enterprise to have the flexibility to select an appropriate senior management officer of the U.S. operations of the foreign enterprise who is located in the U.S. to provide the attestation.[25]

5. *Approval of components – proposed paragraph (c)(1)*

Under the Proposal, the senior officer, an oversight body or a senior-level official of an SD would have to approve each component program or plan required as part of the ORF at least annually. Proposed 17 CFR § 23.603(c)(1). This requirement to have "senior leadership" approve each component program or plan for the ORF presents significant challenges and fails to provide flexibility. The engagement required of senior leadership and the CCO may be challenging, particularly in the context of firms' cyber risk management programs (*e.g.*, since information about unrealized threats is typically tightly held for operational security reasons) and the need to have a single individual or group that is responsible for all three prongs. Individuals and groups that sit across the three prongs would not typically engage at the level suggested by the Commission (*e.g.*, they would not approve specific business line risk limits or detailed risk assessments). As such, the Associations urge the Commission to adjust this requirement to provide

---

23 *See* 17 CFR § 3.3(d), (e)(1), (e)(2) and (e)(5).

24 For example, SDs that currently rely on a substituted compliance determination regarding the CCO report may wish to provide an attestation in this circumstance.

25 *See, e.g.*, 17 CFR § 75.20(c) (providing that, for a U.S. branch or agency of a foreign banking entity, the annual CEO attestation may be provided for the entire U.S. operations of the foreign banking entity by the senior management officer of the U.S. operations of the foreign banking entity who is located in the United States).

greater flexibility so that senior leadership or an appropriate delegate can approve each component program or plan.

6. *Independence in reviews and testing – proposed paragraph (h)*

The Proposal requires "regular reviews and risk-based testing" of the ORF and further provides that such reviews and testing must be "conducted by qualified personnel who are independent of the aspect of the [ORF] being reviewed or tested." Proposed 17 CFR § 23.603(h), (h)(3). In practice, some firms consult independent personnel before, during and after certain types of testing. However, as discussed in the context of risk assessments on information and technology security programs below in Section II.B., the Associations believe that personnel who are actively engaged, including the first and second lines of defense, are better situated and qualified to review and test the effectiveness of the ORF as they have a deeper understanding of the processes and related risks. For example, BCDR testing is, by nature, performed by the individuals and teams involved with BCDR plans in order to exercise the capabilities of individuals who will do the work in the event of an actual outage. As such, the Associations urge the Commission to strike that testing by qualified personnel must be conducted by those "who are independent of the aspect of the [ORF] being reviewed or tested" to clarify that SDs may use internal personnel to satisfy the reviews and testing requirements.

B. Information and Technology Security Program

As noted above in Section I.B., the Associations recommend changes to (i) requirements around specific controls, (ii) risk assessments, (iii) the definition of "incident" and the trigger for incident reporting, (iv) the timing requirement for incident reporting, (v) notifications to affected customers and (vi) escalation protocols. The Associations would like to particularly highlight their recommended changes on incident reporting. Specifically, the Associations believe that the definition of incident, and an incident that is reportable to the Commission, must be tied to actual harm and subject to a materiality threshold. Additionally, the Associations urge the Commission to change the timing requirement for notifying the Commission about an incident from 24 hours to 72 hours to align with other notification obligations such as the forthcoming Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA").

1. *Effective controls – proposed paragraph (d)(2)*

The Associations appreciate that the Proposal sets risk-based requirements to "establish, document, implement, and maintain controls reasonably designed to prevent, detect, and mitigate identified risks to information and technology security." Proposed 17 CFR § 23.603(d)(2). This requirement on its own provides SDs the flexibility to determine, under the proposed (b)(3) standard, controls that will be "reasonably designed

to prevent, detect, and mitigate identified risks."[26] However, proposed paragraph (d)(2) goes on to enumerate eleven different types of controls that SDs must "consider, at a minimum … and adopt those consistent with the standard set forth in [proposed] paragraph (b)(3)."

The Associations urge the Commission to remove the second sentence of proposed paragraph (d)(2) and the 11 controls listed thereafter. Given the fluid nature of the technology controls landscape, what constitutes appropriate controls for a given SD will vary depending on context and will evolve over time. As such, the Commission should not set out specific controls through a rulemaking procedure that may become obsolete in a few years. Instead, the Commission should retain the risk-based requirement provided in the first sentence of proposed paragraph (d)(2) and discard the remainder.

However, should the Commission choose to retain the controls listed in proposed paragraph (d)(2)(i)-(xi), the Associations urge the Commission to not prescribe the use of any specific controls and instead retain the requirement to "consider" the enumerated controls[27] and provide the option for SDs to use compensating controls that align with a given SD's risk assessment and tolerance. The ability to utilize compensating controls exists in other regulations and would allow entities to achieve the same outcome while providing greater flexibility.[28] Finally, if the Commission retains the minimum effective controls, the Associations urge the Commission to amend the use of "flaw remediation" in proposed paragraph (d)(2)(vii) to a more commonly used term such as "vulnerability management" or "patch management."

Additionally, the broad definitions of "covered technology" and "covered information" directly impact the effective controls requirements, in addition to other aspects of the Proposal.[29] As such, the Associations offer the following recommendations on these defined terms.

---

26 *Proposing Release*, at 4718.

27 *Proposing Release*, at 4721 (asking if the Commission should "mandate the use of any specific controls, including firewalls, antivirus, and/or MFA?").

28 For example, NYDFS Part 500 provides covered entities the option to use alternative compensating controls for privileged access activity (500.7(c)(2)), multi-factor authentication (500.12(b)), monitoring and training (500.14(b)) and encryption (500.15(b)).

29 The Associations urge the Commission to adopt its proposed changes to these definitions, regardless of whether it removes the enumerated effective controls. The Associations note that these definitions impact other aspects of the Proposal, such as the risk assessment requirement under proposed 17 CFR § 23.603(d)(1), the purpose of the BCDR plan in proposed 17 CFR § 23.603(f)(1), and counterparty

(a) "Covered technology"

The Proposal defines "covered technology" in an overly broad manner as "any application, device, information technology asset, network service, system, and other information-handling component, including the operating environment, that is used by a swap entity to conduct its business activities, or to meet its regulatory obligations, as a swap entity." Proposed 17 CFR § 23.603(a).

For example, the Proposal requires SDs to consider adopting "[a]ccess controls on covered technology, including controls to authenticate and permit access only by authorized individuals and controls preventing misappropriation or misuse of covered information by employees." Proposed 17 CFR § 23.603(d)(2)(i). The Associations believe that the broad definition of "covered technology" would exacerbate confusion about the Commission's expectations with respect to access control requirements. A narrower definition of covered technology would better align with the Commission's stated desire for a risk-based approach and would better allow SDs to determine which systems require enhanced access controls based on a risk assessment.

We believe that the Commission deviates from a risk-based approach when it proposes regulating SDs' use of systems that, if compromised or otherwise unavailable, would not have a reasonably foreseeable impact on an SD's operations or ability to meet regulatory requirements. Instead, the definition should cover technology that, if affected by an incident, could have a material adverse impact on the SD's operational resilience, as the term is defined above in Section II.A.2. We similarly believe that the ability of an SD to meet its regulatory obligations is most appropriately framed in the context of achieving operational resilience.

Accordingly, we propose that the Commission adjust the definition of covered technology to read "any application, device, information technology asset, network service, system, and other information-handling component, including the operating environment, where, as reasonably determined by the swap entity, if an incident occurred involving it, the incident could[30] have a material adverse impact on the swap entity's ability to deliver critical operations through disruption, including its ability to meet its regulatory obligations as a swap entity."

---

notification requirements under proposed 17 CFR § 23.603(j)(1). The Associations' recommendations consider these uses and are appropriate in light of these additional references.

30 We use "could" here instead of "would" in the context of our proposals to narrow the definition of incident and the trigger for incident reporting requirements. However, if the Commission were to reject those recommendations while accepting this proposed definition, we would urge the Commission to consider changing "could" to "would" to narrow the scope of covered technology as it relates to incidents.

(b) "Covered information"

The Proposal defines "covered information" as "any sensitive or confidential data or information maintained by a swap entity in connection with its business activities as a swap entity" without defining "sensitive." Proposed 17 CFR § 23.603(a). The Associations believe this definition is overly broad, lacks clarity present in other regulatory definitions and could benefit from further specifying the importance of the information as it relates to the broader rule.

The proposed definition sweeps in business information, regardless of the impact to the SD if the information were to be compromised or become unavailable. SDs would be obligated to adopt and implement effective controls and TPRM for "covered information," which involves at least the consideration of, among other controls, access controls, encryption, "[d]ual control procedures, segregation of duties, and background checks for employees or third-part[ies]"; "[m]easures to protect against destruction, loss, or damage"; and "[m]easures to promptly recover and secure" the information if compromised and, for TPRM, contractual negotiations and oversight. Proposed 17 CFR § 23.603(d)(2); Appendix A to Subpart J of Part 23. Additionally, SDs would need to notify counterparties of incidents involving a "counterparty's covered information, assets, or positions." Proposed 17 CFR § 23.603(j)(1). These are onerous requirements that are not proportional or risk-based to the defined term.

In contrast to the Proposal's definition, the NYDFS defines "nonpublic information" as "business related information of a covered entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the covered entity." Part 500.1(k)(1).

The Associations urge the Commission to adopt similar clarifications and define "covered information" as "any sensitive or confidential data that, as reasonably determined by the swap entity, relates to its business activities as a swap entity, residing on the swap entity's covered technology, the tampering with which, or unauthorized disclosure, access or use of which, could cause a material adverse impact on the swap entity's ability to deliver critical operations through disruption."

Alternatively, if the Commission declines to adopt this proposed definition, we urge the Commission to adjust the definition to read "any sensitive or confidential data or information required to be maintained according to applicable regulatory requirements …" to limit the scope of "covered information."

2. *Independence requirement for risk assessments – proposed paragraph (d)(1)*

The Proposal includes prescriptive requirements for conducting risk assessments, including the requirement that risk assessments be conducted by independent personnel and at least annually. Proposed 17 CFR § 23.603(d)(1). Such requirements could impose a significant burden on registrants, as they differ from existing standards for risk control self-assessment and would require firms to retool their programs and related governance. The extra burden would have little, if any, added benefit.

The independence requirement is also not aligned with other operational resilience frameworks, such as the Federal Financial Institutions Examination Council's Booklet on Information Security, which does not require that risk assessments be conducted by independent personnel.[31] The Associations believe that personnel who are actively engaged, including the first and second lines of defense, are better situated and qualified to conduct risk assessments, as they have a deeper understanding of the processes and related risks. As such, the Associations urge the Commission to remove the independence requirement.

Additionally, the annual cadence for risk assessments is unnecessarily prescriptive and not aligned with other applicable frameworks. Companies should have the flexibility to place resources in areas that need them rather than maintain an indiscriminate requirement for an annual cadence. Instead, the Associations urge the Commission to remove the annual cadence and replace it with a more flexible, risk-based cadence of "periodic," which aligns with comparable regulations and industry requirements for risk assessments.[32]

3. *Incident reporting (trigger) – proposed paragraph (i)(1)(i)*

The Proposal includes standards for incident notifications to the Commission. Proposed 17 CFR § 23.603(i)(1)(i). To begin, the Associations note that SDs are already required to notify the NFA of cybersecurity incidents under NFA Interpretive Notice 9070.[33] The Associations believe that these existing notification requirements are

---

31 *See* FFIEC Examination Handbook Infobase, *Information Security – Risk Measurement*, available at https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iib-risk-measurement/.

32 For example, NFA's Interpretive Notice 9070 imposes on SDs a "supervisory obligation to assess and prioritize the risks associated with the use of information technology systems" but does not provide a prescriptive cadence. National Futures Association, *Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs*, available at https://www.nfa.futures.org/rulebooksql/rules.aspx?RuleID=9070&Section=9.

33 *Id.*

sufficient and therefore recommend that the Commission leverage these requirements instead of establishing separate notification requirements. To the extent the Commission finds it necessary to impose its own notification requirements, the Associations make the following recommendations to change the definition of "incident," add a materiality threshold and extend the time frame for reporting.

The notification trigger for incidents is overly broad and would benefit from a materiality threshold. Specifically, the Proposal's notification standard would require SDs to notify the Commission of "any incident that adversely impacts, or is reasonably likely to adversely impact: (A) information and technology security; (B) the ability of the [SD] to continue its business activities as a swap entity; or (C) the assets of a counterparty of the SD." Proposed 17 CFR § 23.603(i)(1)(i). While the Associations appreciate the Commission's effort to distinguish between the proposed definition of "incident" and the proposed notification standard,[34] the Associations disagree with the Commission's expectation that "covered entities may experience one reportable incident per year."[35] Even if the Commission revises the definition of "covered information" and "covered technology" as we recommend above and "incident" as we recommend below, we still believe that the notification trigger is too broad and would result in a significant volume of low criticality incident reporting.

For example, the current threshold for an incident reportable to the Commission could be met by a malware infection on a single-end user system, which has been auto-detected by an end-user antivirus solution and subsequently cleaned and quarantined because these circumstances could jeopardize information and technology security. Similarly, an SD may think the current notification trigger requires them to notify the Commission when an employee loses a corporate-issued device that has corporate-issued encryption controls in place because such an occurrence could jeopardize information and technology security. Moreover, in combination with the expansive definition of critical third-party service provider, a third-party incident may trigger notification even if the third-party incident affects a service incidental to the SD because such circumstances that occur at a third-party service provider could jeopardize information and technology security and could be considered reasonably likely to adversely impact the assets or positions of a counterparty of the SD. The Associations believe that such lower-severity occurrences are not reflective of the type of incidents that the Commission wishes to be informed of and, for many organizations, may occur much more often than once per year, which would result in unhelpful overreporting of incidents.

To narrow the scope of incidents that are reportable to the Commission, the Associations urge the Commission to require notification only for incidents that "actually

---

34 *Proposing Release*, at 4732.

35 *Proposing Release*, at 4737.

cause or are reasonably likely to actually cause[36] material adverse impact," similar to what other regulators require.[37] Doing so would align with the Commission's stated reasoning for required reporting, namely to provide warnings of a "systemic threat, either to the markets due to the severity of the impact of the incident or to other covered entities due to the nature of the incident."[38]

In addition to adding a materiality threshold to incidents that are reportable, the Associations are concerned with the breadth of the Proposal's definition of "incident" in light of the obligations that flow from the occurrence of an "incident." The Proposal defines "incident" as "any event, occurrence, or circumstance that could jeopardize information and technology security, including if it occurs at a third-party service provider." Proposed 17 CFR § 23.603(a) (emphasis added). The Commission's proposed definition, including the term "could," more closely aligns with the standard definition of an "event," rather than an "incident." Virtually every common malware infection "could" result in information loss, for example, meaning they could jeopardize information and technology security, as illustrated above. The difference between an event and an incident is actual impact, not potential impact.

The Proposal later requires escalation of incidents within an organization for incidents that require notification to the Commission and notification of incidents to the Commission within 24 hours and to affected customers "as soon as possible." Proposed 17 CFR § 23.603(d)(3)(ii), (i)(1)(i) and (j)(i). This will create a disproportionate administrative burden for the Commission and customers as a result of receiving an unmanageable number of incident reports. Additionally, the Proposal requires that SDs' information and technology security program include a written incident response plan that is "reasonably designed to detect, assess, contain, mitigate the impact of, and recover from an incident." Proposed 17 CFR § 23.603(d)(3). If the proposed definition of "incident" stands, the regulation would require the activation of the incident response plan and attendant resources and personnel in an overbroad range of "events,"

---

[36] While the Associations believe the focus on incident reporting should remain on actual harm or confirmed impact, the Associations understand there are instances where it may be prudent for an entity to inform an authority that an incident is reasonably likely to have an actual material impact on the entity. The Associations urge the Commission to clarify that, in such instances, the use of "reasonably likely" covers incidents in which there is indeed actual impact but where the circumstances are such that the incident has not yet crossed a materiality threshold.

[37] *See, e.g.*, 12 C.F.R. §§ 53.2(b)(4), (b)(7), 53.3 (establishing notification requirements for computer security incidents that consider whether an incident has resulted in "actual harm" and whether the incident has "materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade," certain aspects of a banking organization's business).

[38] *Proposing Release*, at 4731.

"occurrences" and "circumstances" that are more appropriately handled by existing processes for lower severity matters.

Moreover, the current reportable incident trigger under proposed paragraph (i)(1)(i) has three prongs for possible impact: (A) information and technology security; (B) the ability of the swap entity to continue its business activities as a swap entity; and (C) the assets or positions of a counterparty of the swap entity. These three prongs are incongruous with the proposed definition of incident, which only references "information and technology security," meaning there are more categories of "reportable incidents" than are necessarily "incidents" in the first place.

To address these issues, we propose defining "incident" as: "any unplanned, single or linked event(s), occurrence(s), or circumstance(s), that actually causes an adverse impact to: (A) information and technology security; (B) the ability of the swap entity to continue its business activities as a swap entity; or (C) the assets or positions of a counterparty of the swap entity."[39, 40] This would better align the definition with those of similar concepts under other leading frameworks including the Financial Stability Board's ("FSB") *Cyber Lexicon*[41] and the FDIC, FRB and OCC's (together, the "Federal Bank Regulators") Computer-Security Incident Notification Rule.[42]

4. *Incident reporting (timing) – proposed paragraph (i)(1)(iii)*

Additionally, the Proposal would require SDs to notify the Commission, within 24 hours, of any incident that adversely impacts, or is reasonably likely to adversely impact, certain parts of the SD. Proposed 17 CFR § 23.603(i)(1)(iii). The Associations

---

39 Regardless of whether the Commission accepts the proposed modifications to the definition of "incident," the Associations strongly urge the Commission to adopt their recommended modifications to the notification trigger standard, as discussed in this section, which the Associations think is necessary to minimize high volumes of low criticality incident reporting.

40 The Associations' use of "covered information" and "covered technology" in their proposed definition depends on the Commission also accepting the Associations' recommendations to revise those defined terms as well, as discussed further in Section II.B.1.

41 *See* FSB, *Cyber Lexicon*, at 10 (2023), https://www.fsb.org/wp-content/uploads/P130423-3.pdf; NISTIR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementation Guide, Volume 3*, Appendix B (Sept. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8183A-3.pdf. The FSB *Cyber Lexicon* defines "Cyber Incident" as "a cyber event that adversely affects the cyber security of an information system or the information the system processes, stores or transmits whether resulting from malicious activity or not."

42 *See, e.g.*, 12 CFR § 53.2(b)(4) ("Computer-security incident is an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits.").

believe that this timing requirement is too short, and, given the proposed definition of "incident," the timing requirement will mean repeated notifications at a very early stage.

Moreover, the Associations find that the notification timing requirement does not align with other regulatory notification obligations. For example, the Federal Bank Regulators require banking organizations to report more narrowly defined cybersecurity incidents "no later than 36 hours after the banking organization determines" that a "notification incident" (defined to get at systemic problems and not routine incidents) has occurred,[43] while CIRCIA specifies that the Director of the Cybersecurity and Infrastructure Security Agency "may not require reporting [of covered cyber incidents] any earlier than 72 hours after the covered entity reasonably believes that a covered cyber incident has occurred." 6 U.S.C. § 681b(a)(1)(B) (emphasis added).

To prevent overreporting at an early stage and to align with other regulatory reporting requirements, the Associations suggest extending the time frame during which SDs may notify the Commission of an incident to the more standard 72 hours, with the notification timing running from an SD's determining that an incident requiring notification to the Commission[44] has occurred.

5. *Notification (affected counterparties) – proposed paragraph (j)(1)-(2)*

The Proposal requires SDs to notify counterparties of an incident "as soon as possible." Proposed 17 CFR § 23.603(j)(1). The Associations believe this timing requirement for notifying affected customers is unreasonable in that it provides urgency while lacking specificity, and places undue pressure on SDs, especially in light of the absence of a materiality threshold relating to the effect on the customer. Without further clarification from the Commission, the time frame requirement risks SDs having to consider whether to prioritize notifications on an immediate basis over taking essential containment actions during an ongoing incident. Additionally, the proposed timing requirement would present significant litigation risks for SDs and does not allow for registered entities to create sensible incident response plans that focus resources on essential mitigation and containment steps prior to coordinating notifications. The Associations urge the Commission to adjust this timing requirement to "without undue delay after determining" that an incident requiring notification to affected counterparties has occurred or a similarly more flexible time frame. Consistent with the arguments to include materiality thresholds discussed above in Section II.B.3. for incidents and

---

43 *See* 12 CFR § 53.3.

44 The Associations continue to urge the Commission to accept their proposal for what constitutes an incident requiring notification to the Commission, *see supra* Section II.B.3. but would urge the Commission to extend the time frame to notify the Commission under proposed 17 CFR § 23.603(i)(1)(iii) regardless of whether the Commission indeed accepts such proposal.

incidents that are reportable to the Commission, the Associations also urge the Commission to adjust the notification trigger for affected counterparties to be "any incident that actually causes, or is reasonably likely to cause, material adverse impact to the confidentiality or integrity of the counterparty's covered information, assets, or positions." Such a standard will ensure counterparty notification occurs for higher-severity incidents while leaving the boundaries of counterparty notification for lower-severity incidents that pose less risk to operational resilience to contractual negotiations between parties or at SD's reasonable discretion.

Additionally, and in contrast to the paragraphs outlining the notification to the Commission, the Proposal does not identify permissible methods of notifying customers. This omission is likely to cause confusion and potentially disputes between SDs and customers over the appropriate means of notification. The Associations encourage the Commission to clarify that SDs have flexibility in making customer notifications to facilitate prompt and timely notifications, including under our proposed standard of "without undue delay." The process of creating, approving and delivering customized, written notifications is time-, resource- and cost-intensive and will amplify the concerns raised above that SDs will be forced to prioritize notifications over essential mitigation and containment steps. To remedy this concern, while also future-proofing the language to be adaptable to innovations in communications, the Associations propose that proposed paragraph (j)(2) be modified to state explicitly that the notification can occur "in person, by telephone, mail, email or any other customary or reasonable form of customer communication."

6. *Escalation protocols – proposed paragraphs (d)(3)(ii); (a)*

The Proposal requires incident response plans to include escalation protocols to three roles: (1) either the senior officer, governing board or the senior level officer responsible for IT; (2) CCO; and (3) any other relevant personnel. Proposed 17 CFR § 23.603(d)(3)(ii). The Associations find the requirement to have escalation protocols to the CCO to be overly prescriptive in light of the variety of incident response and escalation structures in use by covered entities. Further, these escalation protocols do not consider varying management structures for non-U.S. regimes and should be adjusted to reflect that, under certain non-U.S. regulatory regimes, officers or senior individuals other than the CCO are charged with operational resilience oversight and compliance. As such, the Associations urge the Commission to remove the requirement to escalate to the CCO in proposed paragraph (d)(3)(ii) and replace it with "appropriate senior management."

Additionally, given the proposed definition of "incident," this escalation protocol will lead to a burdensome volume of events escalated to senior roles and will drown out the important incidents that most warrant senior officer and board involvement. As

described above in Section II.B.3, it is important for the Commission to narrow the definition of "incident" to establish an effective ORF.

C. Third-Party Relationship Program

As noted in Section I.C., the Associations provide the following suggestions regarding (i) imposing heightened duties with respect to risk management practices on critical services rather than critical providers, (ii) the sufficiency of requirements for due diligence of subcontractors, (iii) aligning the exit strategy guidance with the intended risk-based approach, (iv) maintaining the proposed approach for third-party service providers that are affiliated entities, (v) clarifying inventory obligations for consolidated third-party relationship programs, (vi) confirming the scope of "potential" critical third-party service providers and (vii) narrowing TPRM obligations with respect to the "covered information" definition.

1. *Critical third-party service provider – proposed paragraph (a)*

The Proposal requires SDs to implement enhanced third-party risk management practices for "critical third-party service providers." The Proposal defines "critical third-party service provider" as "a third-party service provider, the disruption of whose performance would be reasonably likely to (a) significantly disrupt a swap entity's business operations as a swap entity; or (b) significantly and adversely impact the swap entity's counterparties." Proposed 17 CFR § 23.603(a). While the Associations support the intent of the general requirement that certain situations warrant heightened due diligence, the use of the term "critical third-party service provider" and the criteria used to define the term are overly broad and the resulting application of heightened requirements materially diverges from leading domestic and international standards in this area, *e.g.*, the Federal Bank Regulators' approach.

The Commission's proposed approach would result in covered entities focusing on a significant number of third-party services that present minimal risk to their operations. While certain services provided by a third-party service provider may indeed be "critical" to the covered entity, it is also quite common for that same third-party service provider to supply the covered entity with a range of services, many of which carry minimal inherent risk, importance or resilience implications to the covered entity. To account for this, a more targeted approach is needed to identify third-party relationships that require heightened requirements and avoid unnecessarily scoping in lower risk or less important services also provided by that same third-party service provider.

To remedy this, and to bring the Commission's framework in line with global third-party risk management regulatory approaches, the definition should be modified by shifting the focus of criticality from the provider level, *i.e.*, from the third-party service provider, to the actual service that is provided by the third party. This would result in the

enhanced diligence requirements applying to only the "critical services" provided by third parties rather than potentially any service provided by third parties.

The shift in focus to critical services would align the Proposal with recent guidance on third-party risk management issued by the Federal Bank Regulators. The Federal Bank Regulators call for banking organizations to focus their oversight on third-party relationships that support "critical activities" within the banking organization.[45] As such, the Federal Bank Regulators indicate that "[c]haracteristics of critical activities may include those activities that could: [(i) c]ause a banking organization to face significant risk if the third party fails to meet expectations; [(ii) h]ave significant customer impacts; or [(iii) h]ave a significant impact on a banking organization's financial condition or operations."[46] Notably, this criticality assessment focuses on the specifics of a service provided by a third party (rather than any service provided by a "critical third-party service provider") in support of the critical activity. Furthermore, the FSB focuses the application of heightened requirements on "critical services" as these are the services "whose failure or disruption could significantly impair a financial institution's viability, critical operations, or its ability to meet key legal and regulatory obligations."[47] The FSB states that noncritical services should be subject to proportionate risk management.[48]

We therefore propose that the Commission align its third-party risk management requirements by replacing the term "critical third-party service provider" with "critical third-party service." We understand that this approach more closely aligns to SDs' existing criticality assessments and indexing and avoids the overbroad capture of noncritical services provided by a third-party service provider that is "critical" as a result of some other service(s) because, as discussed in the Federal Banking Regulators' Guidance on Third-Party Risk Management, "not every relationship involving critical activities is necessarily a critical third-party relationship."[49] Specifically, we think the Commission should revise the definition as follows: "Critical third-party service means a third-party service, the disruption of which would be reasonably likely to:

---

45 FRB, OCC, FDIC, *Interagency Guidance on Third-Party Relationships: Risk Management*, 88 Fed. Reg. 37920, 37927–37928.

46 *Id.*

47 FSB, *Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities*, 6 (2023), https://www.fsb.org/wp-content/uploads/P041223-1.pdf [hereinafter *FSB Toolkit*].

48 *FSB Toolkit*, at 7.

49 88 Fed. Reg. 37920, at 37922.

(a) Significantly disrupt a swap entity's critical business operations as a swap entity; or
(b) Significantly and adversely impact the swap entity's counterparties."

2. *Due diligence of subcontractors – proposed paragraph (e)*

The Associations believe the Commission should not recommend more enhanced due diligence of subcontractors. The Proposal asks whether the Commission should recommend more enhanced due diligence of subcontractors.[50] The Associations suggest that, consistent with the intended risk-based approach of the guidance in the Proposal's Appendix A, swap entities consider a third-party service provider's use of subcontractors and ability to manage the risks associated with using subcontractors in its selection, contracting and monitoring of third-party service providers in a manner commensurate with the risks presented by the third-party relationship.

The FSB recently produced a toolkit that promotes interoperability across various regulatory regimes.[51] The FSB Toolkit acknowledges that it is difficult and impractical for financial institutions to assess all possible risks in a supply chain, while emphasizing that effective due diligence and ongoing monitoring should incorporate assessing a third-party service provider's process for addressing supply chain risks.[52] As such, the FSB encourages financial institutions and service providers to adopt a risk-based, proportionate approach in developing risk management strategies.[53] While the role of a subcontractor may be a factor in this determination, it is not dispositive of heightened due diligence and other factors such as the criticality of services or sensitivity of data that the provider has access to, which may impact the level of diligence and monitoring required.[54] Similarly, the Federal Bank Regulators in their joint guidance also emphasize that third-party relationships, including a third-party's use of subcontractors, should be evaluated on a risk-based approach, and banking organizations should adopt mitigating factors as appropriate.[55] As such, the Associations urge the Commission to similarly consider a risk-based approach with respect to subcontractors providing critical services.

---

50 *Proposing Release*, at 4724–25.

51 *FSB Toolkit.*

52 *Id.* at 22–23.

53 *See id.*

54 *See id.*

55 88 Fed. Reg. 37290, at 37925.

3. *Exit strategy guidance – proposed paragraph Appendix A*

The Associations believe that the termination guidance and the exit strategy guidance in proposed Appendix A[56] should include language that clearly indicates that SDs should facilitate termination in a manner that is "appropriate to the degree of risk and complexity of the third-party relationship and service provided." As the FSB Toolkit notes, "[t]here is no one-size-fits-all approach to exit planning" and "[t]he feasibility of an exit plan may depend on the circumstances of the financial institution, the relevant critical service and the service provider."[57] The Federal Bank Regulators' Guidance on Third-Party Relationships instructs "management to terminate relationships in an efficient manner" and lists a number of factors that may be considered "[d]epending on the degree of risk and complexity of the third-party relationship."[58]

Appendix A of the Proposal similarly indicates that "[t]he degree to which the guidance would be applicable to a particular swap entity would depend on its unique facts and circumstances and may vary from relationship to relationship." Consistent with the approach that the FSB and Federal Banking Regulators take, the Associations read this as providing that adoption of the Commission's guidance should be risk-based, therefore lending support to the belief that exit strategies should depend on the level of complexity the third-party relationship and service presents.[59]

4. *Third-party service providers that are affiliated entities – proposed paragraph (e)*

The Proposal asks whether the Commission should consider including any additional guidance with respect to the management of third-party service providers that are affiliated entities. Consistent with a risk-based approach to third-party risk management, the Associations believe that the Commission should not prescribe any further requirements on affiliated third-party service providers, albeit we note that under

---

[56] The Associations support references to guidance but urge the Commission to issue this guidance on third-party relationship lifecycle stages separately from the final binding regulation rather than including the guidance as an appendix.

[57] *FSB Toolkit* at 27–28.

[58] 88 Fed. Reg. 37920, at 37935.

[59] Alternatively, the Associations agree with Commissioner Pham's perspective that staff guidance is preferable to Commission guidance, as staff guidance "can be kept up-to-date more easily to address changes in best practices or to adapt to emerging risks." *Commissioner Pham's Statement*, *supra* n.7. The Associations appreciate Commissioner Pham's comments on this topic and would support the removal of Commission guidance from the Proposal in favor of staff guidance, which is more flexible and in line with the Commission's risk-based approach.

many existing regimes, arrangements with intragroup service providers are still covered by the regulatory requirements.

5. *Inventory for consolidated third-party relationship programs – proposed paragraph (e)(3)*

The Proposal requires SDs to create, maintain and regularly update an inventory of third-party service providers the SD has engaged to support its activities as a swap entity, identifying whether each third-party service provider in the inventory is a critical third-party service provider. Proposed 17 CFR § 23.603(e)(3). The Associations urge the Commission to take the view and clarify this proposed paragraph to state, that SDs that rely on a consolidated third-party relationship program would not be required to separately identify the services and providers that an SD uses as long as the enterprise-wide inventory covers services and providers used by the SD.

6. *Potential critical third-party service providers – proposed paragraph (e)(2)*

Under the third-party relationship program, SDs must "establish heightened due diligence practices for potential critical third-party service providers and heightened monitoring for critical third-party service providers." Proposed 17 CFR § 23.603(e)(2) (emphasis added). The Associations note that the meaning of "potential" is unclear as to whether it is intended to (i) refer to a future third-party service provider, not yet formally engaged, that will be "critical" if engaged or (ii) to a third party that could potentially become critical at a future point in time. If the latter, the Associations believe the requirement to be overbroad, that it would not be reasonably practicable for SDs to identify such third parties accurately and that such an interpretation would significantly expand the scope of heightened due diligence obligations. In keeping with the risk-based approach and to ensure that only critical third-party relationships are subject to heightened requirements, the Associations ask the Commission to clarify that its use of "potential" refers to the interpretation in (i) above by striking the term and revising the Proposal's language to read: "establish heightened due diligence practices and monitoring for the provision of critical third-party services."

7. *Covered information definition – proposed paragraph (a)*

As discussed above, the Proposal's definition of "covered information" is overly broad, sweeping in business information regardless of the impact to the SD if the information were to be compromised or become unavailable. Nevertheless, under the proposed definition, SDs would be obligated to adopt and implement TPRM for covered information, which involves at least the consideration of contractual negotiations and oversight. Proposed Appendix A to Subpart J of Part 23. As such, the Associations reiterate their recommendation from Section II.B.1 here as it related to TPRM.

D. BCDR Plan

As noted above in Section I.D., the Associations recommend the Commission (i) adjust the trigger for notifications regarding BCDR activation to distinguish between major and minor disruptions, (ii) uniformly describe the core components individually as a "program" as opposed to, for BCDR, "plans," (iii) make the BCDR testing requirement more risk-based and (iv) maintain a flexible approach to BCDR recovery time.

1. *Notification of BCDR activation to the commission – proposed paragraphs (i)(2)(i) and (iii)*

The notification trigger for BCDR activation does not account for broad BCDR practices and similarly should have a materiality threshold that distinguishes between minor and major disruptions. The Proposal requires that SDs notify the Commission of any determination to activate the BCDR plan. Proposed 17 CFR § 23.603(i)(2)(i). The Associations urge the Commission to consider adding a materiality threshold to reporting BCDR plan activation such that SDs would only need to notify the Commission of a determination to activate the BCDR plan in the context of a major disruption. Doing so would align with existing requirements for commission notification under the CFTC's existing BCDR requirements for swap entities.[60]

The Proposal would also require an SD to notify the Commission within 24 hours of determining to activate its BCDR plan. Proposed 17 CFR § 23.603(i)(2)(iii). As with the incident notification timeline, the Associations believe the 24-hour reporting window for BCDR plan activation is too short and misaligned with other regulatory notification obligations. Consistent with the arguments discussed above in Section II.B.4., the Associations urge the Commission to provide a 72-hour time frame for reporting BCDR plan activation that begins after the SD has confirmed material impact to the firm's operations.

2. "*Programs" versus "Plans"*

The Associations note the Commission's use of "programs" in connection with operational resilience and third-party risk management and "plan" in connection with BCDR. Depending on the size and scale of the SD, BCDR provisions may operate across several programs, and there may be multiple BCDR "plans" within an overarching "program" or set of "programs." The Associations find that the use of "program" provides greater flexibility and urge the Commission to adjust references from BCDR plans to BCDR programs.

---

[60] *See* 17 CFR § 23.603(d) (requiring swap entities to notify the Commission of an emergency or disruption that "would have a significant adverse effect" on the swap entity).

3. *BCDR tabletop exercises – proposed paragraph (h)(2)(ii)*

The Proposal requires that BCDR testing "include, at a minimum, a walk-through or tabletop exercise designed to test the effectiveness of backup facilities and capabilities at least annually." Proposed 17 CFR § 23.603(h)(2)(ii). As discussed above in Section II.A.6., while the Associations believe in the importance and efficacy of testing, the particular method of testing is more appropriately determined by the entity. As such, the Associations urge the Commission to make this component of BCDR testing more risk-based by removing "walk-through or tabletop exercise" from proposed paragraph (h)(2)(ii).

4. *BCDR recovery time – proposed paragraph (f)(1)(i)*

The Proposal requires SDs to include in their ORFs a BCDR plan that is "reasonably designed to enable the swap entity to: [c]ontinue or resume normal business operations with minimal disruption to counterparties and the markets." Proposed 17 CFR § 23.603(f)(1)(i). The Associations are supportive of the Commission's decision to not include a recovery time objective in its BCDR requirements.[61]

As the Commission indicated, a strict, prescriptive recovery time objective could pose several challenges.[62] First, strict timelines for recovery may motivate SDs to resume operations before the SD has fully remediated the risk, which could lead to even greater market disruption than if the SD was to remain offline. Second, a strict recovery time objective might not allow for situations where a minimal viable product is resumed, but not the full service. In such cases, both a specific time requirement and the use of "resume any operations" in current Commission Regulation 17 CFR § 23.603 would present significant challenges. SDs may also choose not to resume a specific operation but instead provide a given service in a different way or rely on a substitutable option on the market. As such, the Associations urge the Commission to stand by its decision to not include a recovery time objective in its BCDR requirements.

E. Implementation Period

As noted above in Section I.E., the Proposal's six-month implementation period is too short because it (1) does not account for the need to assess and reconcile existing structures and practices against the Proposal's requirements, (2) does not provide adequate time to obtain substituted compliance and (3) is out of step with other regulatory

61 *See Proposing Release*, at 4727.

62 *See Proposing Release*, at 4726.

requirements. As such, the Associations urge the Commission to provide a tiered implementation period that provides more time for particularly onerous components.

1. *The Proposal's implementation period is impractical given the need to reconcile existing structures and practices against the Proposal's requirements*

The Proposal provides for complex requirements related to processes that often run on annual or other periodic cycles and that would be challenging, and in some cases impossible, to implement or sufficiently enhance within six months. For example, many SDs sit within larger institutions that already set risk appetite and RTLs (or substantially equivalent thresholds) on an annual basis. As such, a six-month implementation period for provisions that the Proposal would prescribe to be on an annual cadence, when SDs may already have processes for such provisions that happens to occur outside of a six-month implementation window, would not make sense. In addition, SDs have existing processes in place to obtain approvals at the senior management and/or board levels that may require additional time not accounted for in the proposed implementation time frame.

Furthermore, because no single person within an SD has all the requisite knowledge to develop and implement policies and procedures, this work would require extensive coordination with various departments and separate business units, including legal, compliance, vendor management and information technology. Additionally, even if the entity already has many of these components in place, implementation invariably involves a long process; may require adequate time to procure consultants, undertake consultant reviews and conduct internal reviews of consultant recommendations; and could necessitate engagement in additional procurement processes to implement such recommendations.

Finally, to avoid duplication and achieve compliance with overlapping regulatory requirements, the Proposal's requirements must be understood in relation to similar rules, which makes it complicated to reconcile these competing frameworks into a workable set of ORF components. For example, NFA Interpretive Notice 9070 requires policies and procedures related to, *e.g.*, risk assessments, third-party risk management and incident response that are similar but not identical to the ORF's requirements.[63] As such, a six-month implementation period could force SDs to fall out of step with existing, well-established processes, unnecessarily increasing the cost of compliance with no concomitant improvement in operational resilience. Additionally, many entities are

---

63 National Futures Association, *Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs*, available at https://www.nfa.futures.org/rulebooksql/rules.aspx?RuleID=9070&Section=9.

already implementing components of the Proposal in ways that implicate existing negotiated contractual terms.

A tiered implementation period, as suggested below, would alleviate some of these concerns, particularly for components of the Proposal that would require an annual cadence. Similarly, to the extent the Commission leverages existing NFA requirements, as discussed above in Sections I.C., I.D. and II.B.3., some of the concerns that the Associations have about the implementation timeline will also be reduced as there will be fewer changes for SDs to make in order to comply with the Proposal's requirements.

2. *The Proposal's implementation period would not allow SDs to achieve substituted compliance*

Many of the Associations' members are already subject to existing international regulatory regimes and may wish to obtain substituted compliance determinations.[64] Recent experience has demonstrated that the process takes significantly more than six months. For example, the Commission's process for determining substituted compliance for the capital and financial reporting requirements under 17 CFR § 23.100-23.106, which began prior to those requirements going live in October 2021, remains pending. The Associations expect the process for substituted compliance for the ORF Proposal will be similar. A six-month implementation period for substituted compliance for the ORF Proposal will create uncertainty and inefficiency from having to implement temporary measures that may later prove redundant once substituted compliance is granted. As such, in addition to providing a longer implementation period, the Associations urge the Commission to include an explanation in any potential Adopting Release that the Commission anticipates providing "no-action" or other relief to SDs that make a good-faith request for substituted compliance.

3. *The Proposal's implementation period conflicts with comparable regulations*

The six-month implementation period is out of step with that adopted by other comparable regimes both domestically and internationally. For example, internationally, the UK Prudential Regulation Authority's operational resilience requirements adopted a tiered approach, which has given firms up to three years to ensure they are able to meet

---

64 The Associations note and appreciate Commissioner Pham's request for comments on substituted compliance. *Commissioner Pham's Statement*. In implementing a substituted compliance process, the Associations urge the Commission to provide a principles-based approach that focuses on outcomes rather than exact matches and will result in the entity adhering to necessary home country requirements in lieu of the Proposal's provisions. For example, the provisions within the EU's Digital Operation Resilience Act should offer SDs operating under that regime to apply for substituted compliance with many of the Proposal's components, despite the possibility that such provisions may not exactly match the Proposal, *e.g.*, in terms of scope and implementation timing.

their obligation to ensure they are able to remain within their "impact tolerance" for each "important business service."[65] Domestically, the NYDFS provided a tiered implementation period, which gives firms up to two years to build out technical requirements.

4. *The Commission should provide a tiered implementation approach*

Given the challenges that a six-month implementation period would pose, the Associations urge the Commission to instead provide a tiered implementation timeline. The Associations believe the Commission can retain a six-month timeline for SDs to update their incident response plans under proposed paragraph (d)(3) and BCDR plans under proposed paragraph (f), as well as the associated notification protocol under proposed paragraphs (i)(2), particularly if the Commission adopts the above-proposed revisions to these respective sections in order to narrow the scope of definitions and notification requirements necessitating adjustments.

The Associations urge the Commission to provide a one-year timeline for parts of the Proposal that may require SDs to establish new provisions or enhance processes, particularly those that are likely to involve coordination amongst numerous areas of the enterprise, multiple layers of management review and may involve consultant input. This includes requirements for training under proposed paragraph (g), creating a third-party inventory and diligence program under proposed paragraphs (e)(2) and (e)(3),[66] establishing controls under proposed paragraph (d)(2), establishing risk appetite and RTLs under proposed paragraph (c)(2) and notifying customers or clients of certain incidents under proposed paragraph (j).

Following the completion of the one-year implementation timeline described above, SDs would then have one full calendar year to perform the Proposal's cyclical oversight mechanisms. These mechanisms include the approval of components under proposed paragraph (c)(1), attestations (or proposed alternatives) under proposed paragraph (c)(3), risk assessments under proposed paragraph (d)(1) and reviews and testing under proposed paragraph (h). By phasing the requirements in this manner, provisions that come into effect at the one-year mark can then be appropriately and thoroughly reviewed by the end of the second year without interrupting review and

---

65 Bank of England Prudential Regulation Authority, *Operational Resilience: Impact Tolerances for Important Business Services*, at 17 (March 2021), available at https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/policy-statement/2021/march/ps621.pdf.

66 The Associations recommend that, where enhancements to third-party contracts may be required based on the Proposal requirements, SDs address such enhancements to contracts on a rolling basis according to the contract's renewal cycle rather than having to potentially renegotiate service provider contracts and lose leverage during such negotiations in light of an imminent implementation deadline.

oversight processes that are often set at the group or enterprise level and may conflict with a shorter implementation period.

***

As we noted at the outset, the Associations are supportive of the Commission's objective to introduce a principles-based framework to identify, monitor, manage and assess risks relating to information and technology security, third-party relationships and other core areas of operational resilience. However, we respectfully submit that the Proposal can be improved by enhancing the emphasis on risk-based obligations, harmonizing provisions with other existing or forthcoming regulatory models and refining definitions to align on a common baseline framework.

The Associations greatly appreciate the Commission's consideration of our comments and hope that they serve as an aid to the Commission's deliberations. The Associations would welcome the opportunity to continue to participate in this valuable process. Please feel free to contact the undersigned to discuss these issues further.

Sincerely,

Beth Zorc
CEO
IIB

Kenneth E. Bentsen, Jr.
President and CEO
SIFMA

cc: The Honorable Rostin Behnam, Chairman
The Honorable Kristin N. Johnson, Commissioner
The Honorable Christy Goldsmith Romero, Commissioner
The Honorable Summer K. Mersinger, Commissioner
The Honorable Caroline D. Pham, Commissioner
Ms. Amanda Olear, Director, Market Participants Division
Ms. Pamela Geraghty, Deputy Director

Appendix 1 – Proposed Revisions to Definitions

The Associations' recommendations for substantive changes to definitions in the Proposal are outlined in the chart below. This chart does not represent all of the Associations' recommendations, only those that relate specifically to defined terms.

Term	Proposal Section	Proposed Revision	Cited in This Letter
Operational resilience standard	17 CFR § 23.603(b)(3)	The Operational Resilience Framework shall be appropriate and proportionate to the nature, size, scope, complexity, and risk profile of its business activities as a swap entity~~, following generally accepted standards and best practices~~.	Section II.A.1.
Operational resilience	N/A	the ability of a firm to deliver critical operations through disruption	Section II.A.2.
Covered technology	17 CFR § 23.603(a)	any application, device, information technology asset, network service, system, and other information-handling component, including the operating environment, ~~that is used by a swap dealer to conduct its business activities~~, where, as reasonably determined by the swap entity, if an incident occurred involving it, the incident could have a material adverse impact on the swap entity's ability to deliver critical operations through disruption; ~~or~~ including its ability to meet its regulatory obligations as a swap entity	Section II.B.1.a.
Covered information	17 CFR § 23.603(a)	any sensitive or confidential data ~~or information maintained by a swap entity in connection with~~ that, as reasonably determined by the swap entity, relates to its business activities as a swap entity, residing on the swap entity's covered technology, the tampering with which, or unauthorized disclosure, access or use of which, could cause a material adverse impact on the swap entity's ability to deliver critical operations through disruption or, in the alternative: any sensitive or confidential data or information required to be maintained according to applicable regulatory	Section II.B.1.b.

Term	Proposal Section	Proposed Revision	Cited in This Letter
		requirements by a swap entity in connection with its business activities as a swap entity	
Incident	17 CFR § 23.603(a)	any unplanned, single or linked event(s), occurrence(s), or circumstance(s), that ~~could jeopardize~~ actually causes an adverse impact to: (A) information and technology security; (B) the ability of the swap entity to continue its business activities as a swap entity; or (C) the assets or positions of a counterparty of the swap entity. ~~including if it occurs at a third-party service provider~~	Section II.B.3.
Incident notification trigger (to Commission)	17 CFR § 23.603(i)(1)(i)	Each swap entity shall notify the Commission of any incident that actually causes, or is reasonably likely to actually cause material adverse~~ly~~ impact~~s,~~ to: (A) information and technology security; (B) the ability of the swap entity to continue its business activities as a swap entity; or (C) the assets or positions of a counterparty of the swap entity.	Section II.B.3.
Incident notification trigger (to affected counterparties)	17 CFR § 23.603(j)(1)	Each swap entity shall notify a counterparty ~~as soon as possible~~ without undue delay of any incident that actually causes, or is reasonably likely to cause material ~~have~~ adverse~~ly affected~~ impact to the confidentiality or integrity of the counterparty's covered information, assets, or positions.	Section II.B.5.
Critical third-party service ~~provider~~	17 CFR § 23.603(a)	Critical third-party service ~~provider~~ means a third-party service ~~provider~~, the disruption of ~~whose~~ which ~~performance~~ would be reasonably likely to: (a) Significantly disrupt a swap entity's critical business operations as a swap entity; or (b) Significantly and adversely impact the swap entity's counterparties.	Section II.C.1.
Heightened duties for critical third-party service providers	17 CFR § 23.603(e)(2)	The third-party relationship program shall establish heightened due diligence practices and monitoring for ~~potential~~ the provision of critical third-party service~~s~~. ~~providers and heightened monitoring for critical third-party service providers~~	Section II.C.6.