COMMODITY FUTURES TRADING COMMISSION

17 CFR Parts 1 and 23

RIN 3038–AF23

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

AGENCY: Commodity Futures Trading Commission.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Commodity Futures Trading Commission (CFTC or Commission) is proposing to require that futures commission merchants, swap dealers, and major swap participants establish, document, implement, and maintain an Operational Resilience Framework 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 framework would include three components—an information and technology security program, a third-party relationship program, and a business continuity and disaster recovery plan—supported by broad requirements relating to governance, training, testing, and recordkeeping. The proposed rule would also require certain notifications to the Commission and customers or counterparties. The Commission is further proposing guidance relating to the management of risks stemming from third-party relationships.

DATES: Comments must be received on or before March 2, 2024.

ADDRESSES: You may submit comments, identified by RIN number 3038–AF23, by any of the following methods:

- *CFTC Comments Portal: https://comments.cftc.gov.* Select the ''Submit Comments'' link for this rulemaking and follow the instructions on the Public Comment Form.
- *Mail:* Christopher Kirkpatrick, Secretary of the Commission, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581.
- *Hand Delivery/Courier:* Follow the same instructions as for Mail, above.

Please submit your comments using only one of these methods. Submissions through the CFTC Comments Portal are encouraged.

All comments must be submitted in English, or if not, accompanied by an English translation. Comments will be posted as received to *https://comments.cftc.gov.* You should submit only information that you wish to make available publicly. If you wish the Commission to consider information that you believe is exempt from disclosure under the Freedom of Information Act (FOIA), a petition for confidential treatment of the exempt information may be submitted according to the procedures established in Commission regulation 145.9.[1]

The Commission reserves the right, but shall have no obligation, to review, pre-screen, filter, redact, refuse or remove any or all of your submission from *https://comments.cftc.gov* that it may deem to be inappropriate for publication, such as obscene language. All submissions that have been redacted or removed that contain comments on the merits of the rulemaking will be retained in the public comment file and will be considered as required under the Administrative Procedure Act and other applicable laws, and may be accessible under the FOIA.

FOR FURTHER INFORMATION CONTACT: Amanda L. Olear, Director, at 202–418–5283 or *aolear@cftc.gov;* Pamela Geraghty, Deputy Director, at 202–418–5634 or *pgeraghty@cftc.gov;* Fern Simmons, Associate Director, at 202–418–5901 or *fsimmons@cftc.gov;* Elise Bruntel, Special Counsel, at 202–418–5577 or *ebruntel@cftc.gov;* Market Participants Division, Commodity Futures Trading Commission, Three Lafayette Centre, 1151 21st Street NW, Washington, DC 20581.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Introduction

In 2012 and 2013, the Commission adopted rules requiring that futures commission merchants (FCMs),[2] swap dealers (SDs) [3] and major swap

[1] 17 CFR 145.9. The Commission's regulations are found at 17 CFR chapter I (2022).

[2] *See* 7 U.S.C. 1a(28), 17 CFR 1.3 (defining ''futures commission merchant'').

[3] *See* 7 U.S.C. 1a(49), 17 CFR 1.3 (defining ''swap dealer'').

participants (MSPs)[4] establish risk management programs (RMPs).[5] The rules require that SDs and MSPs (together, swap entities) and FCMs design their RMPs to monitor and manage the risks associated with their activities as swap entities or FCMs.[6] Such risks include, but are not limited to, market, credit, liquidity, segregation, settlement, capital, and operational risk.[7] Taken together, the RMP rules support a unified Commission objective: to require FCMs and swap entities (collectively, covered entities) to establish comprehensive risk management practices to mitigate systemic risk and promote customer protection.[8] Recognizing that covered entities vary in size and complexity, the RMP rules identify certain elements that must, at a minimum, be included as part of the RMP, and require that certain risks must be taken into account; but the rules otherwise allow covered entities flexibility to design RMPs tailored to their circumstances and organizational structures.[9]

In the decade since the RMP rules were adopted, covered entities have encountered a wide variety of challenging conditions, including Brexit, the LIBOR transition, the COVID–19 pandemic stress period, the invasion of Ukraine, and general interest rate increases to tame inflation. Throughout this period, the Commission has, through its various oversight activities, observed that adherence to its RMP rules has supported covered entities' ability to withstand and recover from market challenges. The Commission therefore believes the RMP rules have helped establish a solid foundation of risk management among covered entities across various risk types, promoting a solid baseline standard of risk management that reduces overall systemic risk and enhances the Commission's customer protections.

Nevertheless, the Commission believes it has identified opportunities to adapt its regulations to further promote sound risk management practices, reduce risk to the U.S. financial system, and protect commodity interest customers and counterparties.[10] Specifically, as it relates to this proposal, the Commission believes that recent events, noted below, have highlighted the need for more particularized risk management requirements for covered entities designed to promote operational resilience. An outcome of the effective management of operational risk, ''operational resilience'' can be broadly defined as the ability of a firm to detect, resist, adapt to, respond to, and recover from operational disruptions.[11] As the use of technology and associated third-party service providers have expanded within the financial sector, so too have the sources of operational risk facing covered entities, notably the potential for technological failures and cyberattacks.[12] The Commission preliminarily believes that requirements for covered entities directed at promoting sound practices for managing these risks, as well as the risk of other potential physical disruptions to operations (*e.g.,* power outages, natural disasters, pandemics), and for mitigating their potential impact would not only strengthen individual covered entity operational resilience but would reduce risk to the U.S. financial system as a whole and help protect derivatives customers and counterparties.[13]

The importance of operational resilience in the financial industry has come into stark relief in the past few years, particularly following the COVID–19 pandemic. At the start of the pandemic, Commission staff initiated near daily in-depth discussions with covered entities as those registrants navigated the myriad challenges presented during that time. Through a combination of sustained intensive effort on the part of the covered entities, and targeted no-action positions and exemptive relief provided by Commission staff, covered entities generally continued to operate without material disruption to their CFTC-regulated activities. As a result of this unprecedented experience, the Commission considered whether there were additional opportunities for it to act to gain ongoing transparency into, and to provide further regulatory support to, covered entities' operational resilience practices outside of an unfolding crisis. Commission staff then began the work of assessing the current operational resilience landscape for covered entities and determining how the Commission could act to further the holistic consideration and adoption of operational resilience practices amongst covered entities to ensure that certain

[4] *See* 7 U.S.C. 1a(33), 17 CFR 1.3 (defining ''major swap participant'').''

[5] *See* 17 CFR 1.11; 17 CFR 23.600; Enhancing Protections Afforded Customers and Customer Funds Held by Futures Commission Merchants and Derivatives Clearing Organizations, 78 FR 68506 (Nov. 14, 2013) (Final FCM RMP Rule); Swap Dealer and Major Swap Participant Recordkeeping, Reporting, and Duties Rules; Futures Commission Merchant and Introducing Broker Conflicts of Interest Rules; and Chief Compliance Officer Rules for Swap Dealers, Major Swap Participants, and Futures Commission Merchants, 77 FR 20128 (Apr. 3, 2012) (Final Swap Entities RMP Rule).

[6] *See* 17 CFR 1.11(c); 17 CFR 23.600(b). The RMP rule for FCMs does not apply to FCMs that do not accept or hold customer assets. *See* 17 CFR 1.11(a).

[7] *See* 17 CFR 1.11(e); 17 CFR 23.600(c).

[8] *See* Final Swap Entities RMP Rule, 77 FR at 20128; Final FCM RMP Rule, 78 FR 68506.

[9] *See, e.g.,* Regulations Establishing and Governing the Duties of Swap Dealers and Major Swap Participants, 75 FR 71397, 71399 (Nov. 23, 2010) (Proposed Swap Entities RMP Rule) (''The Commission's rule has been designed such that the specific elements of a risk management program will vary depending on the size and complexity of a [swap entity's] business operations.'').

[10] The Commission recently solicited public comment on an advanced notice of proposed rulemaking regarding potential amendments to the RMP requirements. *See* Risk Management Program Regulations for Swap Dealers, Major Swap Participants, and Futures Commission Merchants, 88 FR 45826 (Jul. 18, 2023) (RMP ANPRM). The comment file is available at *https://comments.cftc.gov/PublicComments/CommentList.aspx?id=7412.*

[11] *See* Proposed Swap Entities RMP Rule, 75 FR 71399, n.12 (defining ''operational risk'' as including ''the risk of loss due to deficiencies in information systems, internal processes and staffing, or disruptions from external events that result in the reduction, deterioration, or breakdown in services or controls within the firm.''). Several sources have produced definitions of ''operational resilience'' relevant to the financial sector. *See e.g.,* Board of Governors of the Federal Reserve System (FRB), the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) (together, the prudential regulators), *Sound Practices to Strengthen Operational Resilience* at 2 (Oct. 30, 2020) (Prudential Operational Resilience Paper) (defining ''operational resilience'' as the ''ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard.''); Basel Committee on Banking Supervision (BCBS), *Principles for Operational Resilience* at 2, 3 (Mar. 31, 2021) (BCBS Operational Resilience Principles) (''ability of a bank to deliver critical operations through disruption''); National Institute of Standards and Technology (NIST), *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach,* SP 800–160, Vol. 2, Rev. 1 at 76 (Dec. 2021) (''ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions.''). Core to each of these definitions is the notion of being able to continue to operate or perform despite a disruption.

[12] *See* Jason Harrell, Depository Trust & Clearing Corporation (DTCC) Managing Director, Head of External Engagements, ''Operational and Technology Risk, Evolving Cybersecurity Risks in a Digitalized Era'' (Sept. 20, 2023) (''While partnerships with third parties offer rapid solutions for institutions to access the latest technologies and capabilities, they also increase the surface area for potential threat actors to gain access to an institution, causing cyber incidents that can impact the institution's operations and potentially create additional sector impacts.'').

[13] Responding to the RMP ANPRM, several commenters suggested the Commission consider addressing cybersecurity risk independently. *See* Americans for Financial Reform Education Fund (AFREF) and Public Citizen Letter at 6 (Sept. 18, 2023) (AFREF&PC Letter); Better Markets Letter Re: Risk Management Program Regulations for Swap Dealers, Major Swap Participants, and Futures Commission Merchants (RIN 3038–AE59) at 6–9 (Sept. 18, 2023) (Better Markets Letter); R.J. O'Brien & Associates LLC Letter at 5–6 (Sept. 18, 2023) (R.J. O'Brien Letter). AFRF and Public Citizen also recommended that the Commission consider extending its risk management regulations to encompass third-party service providers for information technology services. *See* AFREF&PC Letter at 2.

operational risks impacting their CFTC-regulated activities were being addressed on an ongoing basis.

In particular, one area of increased focus is cyber risk. In 2022, cyber intelligence firms reported that the financial sector was among the most impacted by malicious emails, and was ultimately the most breached over the course of the year, with more than 566 successful attacks resulting in 254 million leaked records by early December 2022.[14] For the past two years, financial institutions responding to a DTCC risk survey have identified cyber risk as one of the top five risks to global financial markets, highlighting the increased sophistication of cyber criminals and the industry's growing digital footprint as key drivers.[15] Given that remote access and cloud computing may become permanent features of the financial markets, the need for financial institutions to strengthen, adapt, and prioritize their information and technology risk practices would seem critical to preserving the continued integrity and stability of U.S. financial markets.[16]

Covered entities have experienced firsthand how breaches of information and technology security can reduce their ability to protect customers. In 2016, for instance, a hacker was able to access customer records held on an FCM's backup storage device after a default configuration of that device left it open to infiltration via the internet.[17] In 2018, a successful phishing attack on an FCM compromised customer information and resulted in the FCM's acceptance of a fraudulent wire request that took $1 million in funds from a customer's account.[18] Other regulators have also taken action against banks registered as swap entities where failed controls and third-party service providers intersected to result in the significant exposure of customer information.[19] Even more recently, a ransomware attack on a U.S. broker-dealer in November 2023 was so significant, news reports indicate that the brokerage required a capital injection from a parent entity to settle $9 billion in trades, an amount many times larger than its net capital.[20]

Against the backdrop of that work, a recent and well-documented incident serves as an important cautionary tale about the potential systemic impact of an operational event at a third-party service provider. On January 30, 2023, a ransomware attack on ION Markets, a division of UK-based third-party service provider ION Group LLC (ION), resulted in a two-week disruption in mid-office activities at several FCMs. ION provides order management, execution, trading, and trade processing services for several FCMs, including about 20 percent of clearing members at the Chicago Mercantile Exchange (CME), but also provides software services to many other financial institutions, notably many systemically important banks.[21] FCMs affected by the attack had to process trades manually, leading to delays in the timely and accurate reporting of trade data to the CFTC, and consequently a temporary lag in production of the Commission's weekly Commitments of Traders report.[22] The incident was initially so concerning that Japan cut off all connectivity with ION.[23] Within a couple days of the attack, however, regulators, including the CFTC, coordinated efforts to determine that the attack was limited to a small number of software applications relied on within the cleared derivatives space by about forty-two (42) institutions, with no significant impact to systemically important banks.[24]

During a March 8, 2023, meeting of the CFTC's Market Risk Advisory Committee (MRAC), panelists discussed how the collaborative work of the CFTC, industry, and self-regulatory organizations (including CME, the National Futures Association (NFA), and the Financial Industry Regulatory Authority (FINRA)) helped mitigate the impact of the ION incident, allowing affected firms to return to business as usual within a couple weeks.[25] Nevertheless, panelists agreed that the incident highlighted the interconnectedness of the derivatives markets and the need for firms to continue to adapt safeguards to address the ever-evolving threat landscape.[26] As the ION incident demonstrates, a

[14] *See* Trellix, *The Threat Report Fall 2022* at 11 (Nov. 2022) (noting that the financial services sector was the most targeted by malicious emails in Q3 of 2022); Flashpoint, *Flashpoint Year In Review: 2022 Financial Threat Landscape* (Dec. 20, 2022) (citing finance and insurance as the most-breached sector in 2022).

[15] *See* DTCC, Systemic Risk Barometer Survey: 2023 Risk Forecast (Dec. 7, 2022); DTCC, Systemic Risk Barometer Survey: 2022 Risk Forecast (Dec. 13, 2021) (naming cyber risk as the top risk to the economy). *See also* Bank for International Settlements (BIS), Financial Stability Institute (FSI), FSI Insights on policy implementation No. 50, Banks' cyber security—a second generation of regulatory approaches (June 12, 2023) (FSI Cybersecurity Paper) (citing a 2023 report that most chief risk officers consider cyber risk the top threat to the banking industry and the most likely to result in a crisis or major operational disruption); Federal Bureau of Investigation, internet Crime Complaint Center Releases 2022 Statistics (Mar. 22, 2023) (''Cyber-enabled crime has been around for many years, but methods used by perpetrators continue to increase in scope and sophistication emanating from around the world.'').

[16] *See* FRB, *Cybersecurity and Financial System Resilience Report* at 15 (Aug. 2023) (''The rising number of advanced persistent threats increases the potential for malicious cyber activity within the financial sector. Combined with the increased internet-based interconnectedness between financial institutions and the increasing dependence on third-party service providers, these threats may result in incidents that affect one or more participants in the financial services sector simultaneously and have potentially systemic consequences.'').

[17] *See In re AMP Global Clearing LLC*, CFTC Docket No. 18–10 (Feb. 12, 2018).

[18] *See In re Phillip Capital Inc.,* CFTC Docket No. 19–22 (Sept. 12, 2019).

[19] *See, e.g., In re Capital One, N.A. and Capital One Bank (USA), N.A.,* AA–EC–20–49 (Aug. 5, 2020) (OCC finding that failed risk management practices resulted in exposure of 100 million individual credit card applications, including approximately 140,000 social security numbers, by a former cloud servicer employee); *In re Morgan Stanley Smith Barney LLC,* File No. 3–17280 (Jun. 8, 2016) (Securities and Exchange Commission (SEC) finding that failed risk management controls allowed an employee to impermissibly access and transfer data regarding 730,000 accounts to a personal server, which was ultimately hacked by third parties).

[20] *See* Paritosh Bansal, Reuters, ''Inside Wall Street's scramble after ICBC hack'' (Nov. 13, 2023) (reporting that the firm asked clients to temporarily suspend business with them and clear trades elsewhere).

[21] *See* Luke Clancy, Risk.net, ''One-fifth of CME clearing members hit by Ion hack'' (Mar. 9, 2023); *see also* Statement of Todd Conklin, Deputy Assistant Secretary, Department of the Treasury (Treasury), Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), *The Cyber Threat Landscape for Financial Markets: Lessons Learned from ION Markets, Cloud Use in Financial Services, and Beyond,* CFTC Technology Advisory Committee Meeting Transcript at 160–166 (Mar. 22, 2023) (Conklin TAC Presentation) (describing the potential ''sprawling impact zone'' had the ION incident not been limited to its derivatives software services), *available at https://www.cftc.gov/sites/default/files/2023/07/1688400024/tac_032223_transcript.pdf.*

[22] CFTC, Statement on ION and the Impact to the Derivatives Markets (Feb. 2, 2023), *available at https://www.cftc.gov/PressRoom/Speeches Testimony/cftcstatement020223.* The Commitment of Traders report is widely relied on by market participants for insight into positions held on exchange-traded futures and options.

[23] *See* Conklin TAC Presentation (Mar. 22, 2023).

[24] *Id.*

[25] *See* CFTC, The Market Risk Advisory Committee to Meet on March 8 (Mar. 8, 2023) (MRAC Meeting), *available at https://www.cftc.gov/PressRoom/Events/opaeventmrac030823; see also* Conklin TAC Presentation (discussing how Treasury implemented its cyber incident response playbook in the days following the ION incident to mitigate the potential for panic after news reports began circulating information that the incident was more significant than regulators had initially determined it was).

[26] *See* Statement of Walt Lukken, President and Chief Executive Officer, Futures Industry Association (FIA), MRAC Meeting Transcript at 41 (''While the number of clearing firms that use ION's suite of clearing products is limited, the interconnectedness of our markets made the outage impactful throughout the entirety of our marketplace.''); *see also* Statement of Tom W. Sexton, III, President and Chief Executive Officer, NFA, MRAC Meeting Transcript at 46 (''[O]ur member firms have adopted robust safeguards already that need to be adapted in light of today's and tomorrow's ongoing challenges and threats.'').

disruptive cyber event can reach beyond particular financial institutions directly experiencing events to other institutions in the financial markets or to others doing business with an impacted financial institution, and could potentially impact financial stability.[27]

In light of these and other events, the Commission believes that customer protection and the broader stability of the derivatives markets at large warrant more targeted CFTC requirements relating to the management of operational risk designed to promote operational resilience.[28] Specifically, the Commission believes that the absence of CFTC-specific requirements for covered entities that explicitly address information and technology security, as well as third-party risk, could impede the Commission's ability to fulfill its regulatory oversight obligations with respect to covered entities and ultimately weaken its ability to address systemic risk, protect customer assets, and promote responsible innovation.[29] The Commission further believes that enhanced CFTC oversight of covered entities with respect to operational resilience would help improve outcomes following operational disruptions by giving the Commission the ability to ensure that covered entities have actionable plans in place to address key operational risks.

II. Proposal

Section 4s(j)(2) of the Commodity Exchange Act (CEA or Act) expressly requires swap entities to establish robust and professional risk management systems adequate for managing their day-to-day business.[30] Section 4s(j)(7) further directs the Commission to prescribe rules governing the duties of swap entities, including the duty to establish risk management systems, which would include the management of operational risk.[31] The Commission is authorized to promulgate operational risk management requirements for FCMs pursuant to section 8a(5) of the CEA, which authorizes the Commission to make and promulgate such rules and regulations as, in the judgment of the Commission, are reasonably necessary to effectuate any of the provisions of, or to accomplish any of the purposes of, the CEA.[32] This general rulemaking authority may be used to prevent problems before they arise in the agency's blind spots,[33] and may be exercised to regulate circumstances or parties beyond those explicated in a statute.[34] Accordingly, the Commission has broad authority to promulgate regulations provided that such regulations are supported by a sufficient nexus to the CFTC's delegated authority. Specifically, Congress expressly empowered the Commission to prescribe certain requirements with respect to FCMs, namely, to require FCMs to register (sections 8a(1), 4d(a)(1), and 4f(a)(1) of the CEA [35]); to segregate customer funds (section 4d of the CEA [36]); to establish safeguards to minimize conflicts of interest (section 4d of the CEA [37]); to meet minimum financial requirements (section 4f of the CEA [38]); to manage and maintain records and reporting on the financial and operational risks of affiliates (section 4f of the CEA [39]); and to establish administrative, technical, and physical safeguards to protect the security and confidentiality of certain nonpublic personal information (section 5g of the CEA [40]), among other requirements.

The Commission believes that more particularized operational risk management requirements are reasonably necessary to help effectuate these statutory requirements for FCMs and to accomplish the purposes of the CEA. FCMs play an important role in the derivatives markets, serving as both the primary point of access to the cleared commodity interest markets for customers and the custodian of the funds used to maintain their positions. Given their position at the center of the derivatives market ecosystem, FCMs' operational resilience is essential to well-functioning derivatives markets and to ensuring that customers receive the protections provided by the CEA. However, as discussed above, operational risks, notably cyber and third-party risks, have become an increasing threat to financial institutions, including FCMs. These risks can cause major disruptions to FCMs' operations, and consequently impact the ability of FCMs to fulfill their obligations as Commission registrants. In particular, information security threats and operational disruptions can place an FCM's financial resources at risk; disrupt an FCM's ability to segregate and protect customer funds; impede accurate recordkeeping, including records related to customer funds; and cause a host of other issues for FCMs, which ultimately inure to the detriment of their customers and the derivatives markets. Accordingly, the Commission believes a comprehensive operational resilience regime is reasonably necessary to ensure that an FCM adequately addresses and mitigates risks that could adversely impact its ability to operate and fulfill its statutory obligations and duties as an FCM.

As discussed in detail in subsequent sections of this release, the Commission is proposing to require that FCMs and swap entities establish an Operational Resilience Framework (ORF) that is 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. At its core, the ORF would have three key components: an

[27] *See* FIA, FIA Taskforce on Cyber Risk, *After Action Report and Findings* at 3 (Sept. 2023) (FIA Taskforce Report) (''The [ION incident] demonstrated that an outage at a single service provider can have damaging effects across a wide range of firms and threaten the orderly functioning of markets. The attack also demonstrated in vivid detail the complexities of restoring normal service.'').

[28] Existing CFTC requirements for covered entities relating to operational risk or information security are more general in nature or limited in application. *See, e.g.,* 17 CFR 1.11(e)(3)(ii) (providing, with respect to operational risk, that FCMs have automated financial risk management controls reasonably designed to prevent the placing of erroneous orders); Enhancing Protections Afforded Customers and Customer Funds Held by Futures Commission Merchants and Derivatives Clearing Organizations, 77 FR 67866, 67906 (Nov. 14, 2012) (describing Commission regulation 1.11(e)(3)(ii) as requiring an FCM's RMP to include automated financial risk management controls in order to reduce operational risk that could result from ''fat finger'' errors when submitting trades, or from technological ''glitches'' using automated trading); 17 CFR 23.600(c)(4)(vi) (requiring swap entities to take into account, among other things, secure and reliable operating and information systems with adequate, scalable capacity, and independence from the business trading unit; safeguards to detect, identify, and promptly correct deficiencies in operating and information systems; and reconciliation of all data and information in operating and information systems); 17 CFR 162.21 and 17 CFR 160.30 (requiring covered entities to adopt written policies and procedures addressing administrative, technical, and physical safeguards with respect to the information of consumers).

[29] *See* 7 U.S.C. 5 (establishing among the purposes of the Commodity Exchange Act to deter disruptions to market integrity, to ensure the financial integrity of covered transactions and the avoidance of systemic risk, and to promote responsible innovation and fair competition among market participants).

[30] *See* 7 U.S.C. 6s(j)(2).

[31] *See* 7 U.S.C. 6s(j)(7).

[32] 7 U.S.C. 12a(5).

[33] *Inv. Co. Inst.* v. *CFTC,* 891 F. Supp. 2d 162, 193 (D.D.C. 2012), *as amended* (Jan. 2, 2013) (citing *Stilwell* v. *Office of Thrift Supervision,* 569 F.3d 514, 519 (D.C. Cir. 2009)).

[34] Nat'l Ass'n of Mfrs. v. SEC, 748 F.3d 359, 366 (D.C. Cir. 2014), overruled on other grounds by Am. Meat Inst. v. U.S. Dept. of Agric., 760 F.3d 18 (D.C. Cir. 2014) (en banc).

[35] 7 U.S.C. 12a(1); 7 U.S.C. 6d(a)(1); 7 U.S.C. 6f(a)(1).

[36] 7 U.S.C. 6d.

[37] *Id.*

[38] 7 U.S.C. 6f.

[39] *Id.*

[40] *See* 7 U.S.C. 7b–2; 15 U.S.C. 6801.

information and technology security program, a third-party relationship program, and a business continuity and disaster recovery plan. The proposed ORF rule reflects a principles-based approach buttressed by certain minimum requirements specific to each of the component programs or plans, such as requiring an annual risk assessment and controls relating to information and technology security, and due diligence and monitoring requirements for third-party service providers. Proposed requirements relating to governance, training, testing, and recordkeeping would apply broadly and support the ORF as a whole. The proposed rule would further require covered entities to notify the Commission (and, in certain instances, customers or counterparties) of certain ORF-related events. Detailed guidance intended to assist covered entities in designing and implementing their third-party relationship program would be included in appendices to the rule.

In developing the proposed rule, the Commission endeavored to incorporate general directives to federal agencies articulated in the White House's March 2023 National Cybersecurity Strategy: Leverage existing standards and guidance, harmonize where sensible and appropriate to achieve better outcomes, and demonstrate an approach that is 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.[41] To that end, the proposal builds on the Commission's experience establishing system safeguard requirements for registered entities, as well as the approaches adopted by self-regulatory organizations and other regulatory authorities.[42] Notably, the proposal draws on approaches adopted by NFA, whose rules and interpretative notices relating to information systems security, third-party risk, and business continuity and disaster recovery planning apply to covered entities by virtue of being NFA members, and prudential regulators, who also regulate many covered entities, and have recently issued interagency positions on operational resilience and third-party relationship management.[43]

The Commission also surveyed the work of international standard-setting bodies, notably the BCBS *Principles for Operational Resilience*.[44] The Commission also conferred with, and reviewed the standards published by the National Institute of Standards and Technology (NIST), a part of the U.S. Department of Commerce charged by Executive Order 13636 in 2013 with developing a framework to reduce cyber risks to critical infrastructure that incorporates voluntary consensus standards and industry best practices.[45] Standards developed in response to this charge and reviewed by the Commission include the *Framework for Improving Critical Infrastructure Cybersecurity* and the *Security and Privacy Controls for Information Systems and Organizations,* among others.[46] The Commission and other financial regulators have previously adapted NIST's standards in regulation and guidance related to operational resilience. The Commission's system safeguards requirements treat NIST's CSF as a source for well-established best practices for cybersecurity.[47] In Appendix A of the Interagency Sound Resilience Paper, the prudential regulators presented ''a collection of sound practices for cyber risk management, aligned to NIST and augmented to emphasize governance and third-party risk management.'' [48] The Commission also considered standards published by equivalent standard setting bodies like the International Standards Organization (ISO).[49]

Finally, in putting together the proposal, Commission staff engaged with staff at NFA and various federal agencies, including prudential regulators, and the SEC.[50] Based on these efforts, the Commission preliminarily believes that, if adopted, the proposed rule would strike an

[41] The White House, National Cybersecurity Strategy at 8–9 (Mar. 2023) (National Cyber Strategy) (''Our strategic environment requires modern and nimble regulatory frameworks for cybersecurity tailored for each sector's risk profile, harmonized to reduce duplication, complementary to public-private collaboration, and cognizant of the cost of implementation.''). *See also* FIA Taskforce Report, *supra* note 27, at 9 (''[T]he Taskforce encourages regulators and legislators to take a principles-based approach to cyber risk and operational resilience. That approach may not be sufficient in all areas, but such a flexible approach is well suited to a threat landscape that is likely to continue evolving at a rapid rate.'').

[42] *See* 17 CFR 37.1400 and 17 CFR 37.1401 (system safeguard requirements for swap execution facilities (SEFs)); 17 CFR 38.1050 and 17 CFR 38.1051 (designated contract markets (DCMs)); 17 CFR 39.18 (derivatives clearing organizations (DCOs)); 17 CFR 49.24 (swap data repositories (SDRs)). *See also* 17 CFR 1.3 (defining ''registered entity'' to include DCMs, DCOs, SEFs, and SDRs). For a summary of international regulatory efforts related to operational resilience, *see* FIA Taskforce Report, *supra* note 27, at 7–8.

[43] *See* NFA Interpretive Notice 9070, NFA Compliance Rules 2–9, 2–36 and 2–49: Information Systems Security (rev. Sept. 30, 2019) (NFA ISSP Notice); NFA Interpretive Notice 9079, NFA Compliance Rules 2–9 and 2–36: Members' Use of Third-Party Service Providers (NFA Third-Party Notice) (effective Sept. 30, 2021); NFA Rule 2–38: Business Continuity and Disaster Recovery Plan (rev. July 1, 2019); NFA Interpretive Notice 9052, NFA Compliance Rule 2–38: Business Continuity and Disaster Recovery Plan (NFA BCDR Notice) (April 7, 2003); Prudential Operational Resilience Paper, *supra* note 11; Interagency Guidance on Third-Party Relationships: Risk Management, 88 FR 37920 (Jun. 9, 2023) (Prudential Third-Party Guidance). *See also* Computer-Security Incident Notification Requirements for Banking Organizations and their Bank Service Providers, 86 FR 66424 (Nov. 23, 2021); 12 CFR part 30, app. A (Interagency Guidelines Establishing Standards for Safety and Soundness), 12 CFR part 30, app. B (Interagency Guidelines Establishing Information Security Standards).

[44] *See* BCBS Operational Resilience Principles, *supra* note 11. *See also* International Organization of Securities Commissions (IOSCO), *Cyber Task Force: Final Report* (2019) (identifying different but comparable core standards or frameworks, including both NIST and ISO standards); Financial Stability Board (FSB), *Final report on Enhancing Third-Party Risk Management and Oversight—a toolkit for financial institutions and financial authorities* (Dec. 4, 2023) (FSB Third-Party Report). Materials related to the FSB's work on cyber resilience are available at *https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/cyber-resilience/.*

[45] *See* The White House, Office of the Press Secretary, *Executive Order—Improving Critical Infrastructure Cybersecurity,* E.O. 13636 (Feb. 12, 2013).

[46] *See* NIST, Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1) at 2 (Apr. 16, 2018) (NIST CSF); NIST, SP 800–53, Security and Privacy Controls for Information Systems and Organizations (Sept. 2020, rev. Dec. 10, 2020) (NIST SP 800–53). *See also* Cybersecurity & Infrastructure Security Agency (CISA), Financial Services Sector-Specific Plan—2015 at 16 (rev. Dec. 17, 2020) (''While the [NIST cybersecurity framework] is designed to manage cybersecurity risks, its core functions of Identify, Protect, Detect, Respond, and Recover provide a model for considering physical risks as well. This methodology is increasingly central to the sector's thinking on security and resilience, and the concept aligns with existing [Federal Financial Institutions Examination Council (FFIEC)] guidance.'').

[47] System Safeguards Testing Requirements for Derivatives Clearing Organizations, 81 FR 64322, 64329 (Sept. 19, 2016).

[48] Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation, Sound Practices to Strengthen Operational Resilience (Nov. 2, 2020), *available at https://www.federalreserve.gov/supervisionreg/srletters/SR2024.html.*

[49] *See, e.g.,* ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection: Information security controls (Oct. 2022) (ISO/IEC 27001:2022).

[50] In accordance with section 712(a) of the Dodd-Frank Act (15 U.S.C. 8302), the Commission has consulted and coordinated, to the extent possible, with the SEC and the prudential regulators, including with the FRB, the OCC, and the FDIC, for purposes of assuring regulatory consistency and comparability. The Securities Exchange Act of 1934 and existing and proposed SEC regulations include requirements relating to risk management including cybersecurity, including requirements for SEC-regulated broker-dealers and security-based swap dealers. *See, e.g.* Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents, 88 FR 20212, sections IV.C.1.b.i and IV.C.1.b.iii (Apr. 5, 2023).

appropriate balance between supporting technological and market innovation and fair competition, ensuring covered entities devote the necessary thought, planning, and resources to their operational resilience so as to support the resilience of the U.S. derivatives markets and the financial sector as a whole.[51]

The Commission is proposing to codify the ORF rule for swap entities in existing Commission regulation 23.603, which currently contains the Commission's business continuity and disaster recovery requirements for swap entities.[52] As discussed in greater detail below, the Commission is proposing to retain the substance of the existing business continuity and disaster recovery requirements in current Commission regulation 23.603 as part of the ORF rule for swap entities, with certain modifications. Similar requirements would also be imposed on FCMs. The proposed ORF rule for FCMs would be codified in new Commission regulation 1.13. The proposed guidance on third-party relationships would be included in the appendices to parts 1 and 23 for FCMs and swap entities, respectively.

As proposed, the regulatory text of the ORF rule for swap entities is nearly identical in structure and substance to the ORF rule for FCMs. Accordingly, to promote readability, when referencing sections of the regulatory text, this notice generally refers to the relevant paragraph of the proposed regulations (*i.e.,* ''proposed paragraph (b)'' would refer to paragraph (b) of both proposed Commission regulations 1.13 and proposed Commission regulation 23.603).

The Commission invites comment on all aspects of the proposed rule, as further detailed below.

A. Generally—Proposed Paragraph (b)[53]

1. Purpose and Scope; Components—*Proposed Paragraphs (b)(1) and (b)(2)*

As previously mentioned, the proposed rule would require covered entities to establish, document, implement, and maintain an Operational Resilience Framework, or ORF.[54] The ORF would need to be reasonably designed to identify, monitor, manage, and assess risks relating to three key risk areas that challenge operational resilience: (i) information and technology security, as defined in the proposed rule and discussed further below; (ii) third-party relationships; and (iii) emergencies or other significant disruptions to the continuity of normal business operations as a covered entity.[55] Although these risk areas are often viewed distinctly, as the introduction to this notice illustrates, they are significantly interrelated, as the relative strength of information and technology security and third-party risk management can directly affect recovery activities and improve outcomes following an emergency or other significant disruption.[56] Together, the Commission believes they represent important sources of potential operational risk, the effective management of which is key to operational resilience.

The proposed rule would require covered entities to establish three written component programs or plans, each dedicated to addressing one of the three enumerated risks within the ORF. The three component programs or plans would be: (i) an information and technology security program, (ii) a third-party relationship program, and (iii) a business continuity and disaster recovery plan.[57] Each component program or plan would need to be supported by written policies and procedures and meet the requirements set forth in the rule, as discussed in subsequent sections of this notice.[58] The definitions and specific requirements for the information and technology security program, the third-party relationship program, and the business continuity and disaster recovery plan are discussed in detail in subsequent sections of this notice specifically dedicated to discussing each of the three components.[59]

Although they may go by different names, the Commission understands that written programs or plans of these types are generally recognized as common ways to address these risks and are even currently required of covered entities. NFA, for instance, currently requires members to adopt a written information systems security program (ISSP), a written supervisory framework to address outsourcing to third-party service providers, and a written business continuity and disaster recovery plan.[60] The Commission itself requires swap entities to have a written business continuity and disaster recovery plan.[61] Accordingly, to the extent that covered entities have existing programs or plans and policies and procedures that address the requirements of the ORF rule, by virtue of other regulatory requirements or otherwise, the Commission would not expect such covered entities to adopt entirely new component programs or plans. The Commission would only expect that covered entities review their existing programs and plans to ensure they meet the minimum requirements of the ORF rule and make any necessary amendments.

The Commission appreciates that covered entities may assign responsibility for the establishment, implementation, and maintenance of each ORF component program or plan to distinct functions within their organizations. By structuring the proposed rule to require a ''framework'' directed at operational resilience,

[51] *See* 7 U.S.C. 5.

[52] 17 CFR 23.603.

[53] Paragraph (a) of proposed Commission regulations 1.13 and 23.603 provides definitions for terms used within the ORF rule. Each proposed definition is discussed in the context of the relevant substantive regulatory requirement throughout the remainder of this notice.

[54] *See* paragraph (b)(1) of proposed Commission regulations 1.13 and 23.603.

[55] *See* paragraphs (b)(1)(i)–(iii) of proposed Commission regulations 1.13 and 23.603.

[56] *See, e.g.,* ISO/IEC 27031:2011, Information technology—Security techniques—Guidelines for information and communication technology readiness for business continuity (Mar. 2011) (''Failures of [information and communication technology (ICT)] services, including the occurrence of security issues such as systems intrusion and malware infections, will impact the continuity of business operations. Thus, managing ICT and related continuity and other security aspects form a key part of business continuity requirements. Furthermore, in the majority of cases, the critical business functions that require business continuity are usually dependent upon ICT. This dependence means that disruptions to ICT can constitute strategic risks to the reputation of the organization and its ability to operate . . . As a result, effective [business continuity management] is frequently dependent upon effective ICT readiness to ensure that the organization's objectives can continue to be met in times of disruptions.''). *See* Prudential Operational Resilience Paper, *supra* note 11, at 8 (''Secure and resilient information systems underpin the operational resilience of a firm's critical operations and core business lines.''); *see also* Prudential Third-Party Guidance, 88 FR 37920 (discussing the interplay of third-party risks and operational resilience).

[57] *See* paragraph (b)(2) of proposed Commission regulations 1.13 and 23.603; *see also* paragraph (a) of proposed Commission regulations 1.13 and 23.603 (defining ''information and technology security program,'' ''third-party relationship program,'' and ''business continuity and disaster recovery plan'').

[58] *See* paragraph (b)(2) of proposed Commission regulations 1.13 and 23.603. *See* paragraphs (d) (information and technology security program), (e) (third-party relationship program), and (f) (business continuity and disaster recovery plan) of proposed Commission regulations 1.13 and 23.603 (describing the requirements for each program, respectively).

[59] *See* sections II.C (information and technology security program), II.D (third-party relationship program), II.E (business continuity and disaster recovery plan) of this notice, *infra.*

[60] *See* NFA ISSP Notice, *supra* note 43; NFA Third-Party Notice, *supra* note 43; and NFA BCDR Notice, *supra* note 43. NFA's requirement to establish a business continuity and disaster recovery plan does not currently apply to swap entities, *see* NFA Rule 2–38, paragraph (a), *supra* note 43.

[61] *See* 17 CFR 23.603.

however, the Commission intends for executive leadership at covered entities to address the risk areas covered by the ORF as a cohesive and interrelated whole, breaking down any unnecessary internal silos, and to consider all aspects of operational resilience in determining their operational strategies, risk appetite, and risk tolerance limits.[62]

2. Standard—*Proposed Paragraph (b)(3)*

The Commission is proposing to require that each covered entity implement the requirements of the proposed ORF rule in a manner that is appropriate and proportionate to the nature, scope, complexity, and risk profile of its business activities as a covered entity, following generally accepted standards and best practices (the (b)(3) standard).[63] The proposed (b)(3) standard reflects the general principles-based approach underpinning the proposed rule, which the Commission believes would be appropriate given the increased reliance on and rapid evolution of technology within the financial industry and its attendant risks.[64] This standard incorporates two themes that have broad support from other governmental and international standard-setting bodies when addressing matters related to operational resilience: (i) proportionality; and (ii) reliance on established standards and best practices.[65]

Broadly speaking, the principle of proportionality recognizes that operational resilience, and information and technology security, in particular, cannot be addressed with a one-size-fits-all approach.[66] On the contrary, differences in operational structures and business strategies among covered entities necessitate a more flexible and adaptive approach that would allow individual covered entities to best address their specific risks and evolve to address emerging challenges as they arise. Covered entities vary widely in terms of their business structure and risk profiles, such that a covered entity operating within a large bank holding company group structure and involved in a broad array of asset classes would likely have a different risk profile and different resources than an entity that is solely registered with the CFTC or that has a narrower scope to its CFTC-regulated business. The Commission would therefore expect that covered entities facing different operational risks may take different approaches to managing and monitoring those risks. Designing an operational resilience framework that would apply uniformly across all covered entities would not only pose significant challenges, it would likely be ineffective, imposing operational costs where no risks demand it. Accordingly, the Commission preliminarily believes that a proportional, risk-based approach would help ensure that firms, customers, counterparties, and the financial system at large can appropriately respond to and recover from operational shocks in context.

Interpretive notices adopted by NFA reflect a comparable approach. Specifically, NFA's notices on ISSPs and the use of third-party service providers establish general, baseline requirements (*e.g.,* assess risks associated with the use of information technology systems or with reliance on third-party service providers) and then direct NFA members, including covered entities, to tailor the specifics to their businesses.[67] This approach is also consistent with the CFTC's own approach with respect to system safeguard requirements for registered entities,[68] as well as those of the prudential regulators.[69] Generally accepted standards and best practices themselves also generally support a proportional approach.[70]

The Commission emphasizes, however, that ''proportional'' does not mean ''permissive.'' The Commission's proposed standard for the ORF rule would not support a ''race to the bottom,'' where covered entities default to the minimum requirements of the proposed rule. On the contrary, covered entities would be required to implement an ORF that is reasonably designed to reflect and address their unique risk profile and activities, consistent with the proposed (b)(3) standard. Accordingly, the Commission would expect larger, more complex entities that operate more varied business lines, rely on more technological platforms, or

[62] The specific governance requirements of the proposed rule, which include the requirement to establish risk appetite and risk tolerance limits with respect to the ORF, further support this view. *See* paragraph (c) of proposed Commission regulations 1.13 and 23.603.

[63] *See* paragraph (b)(3) of proposed Commission regulations 1.13 and 23.603.

[64] *See* BCBS Operational Resilience Principles, *supra* note 11, at 1 (''Recognising that a range of potential hazards cannot be prevented, the Committee believes that a pragmatic, flexible approach to operational resilience can enhance the ability of banks to withstand, adapt to and recover from potential hazards and thereby mitigate potentially severe adverse impacts.''); *see also* Prudential Operational Resilience Paper, *supra* note 11, at 9 (providing as a sound practice of operational resilience that firms review information systems ''on a regular basis against common industry standards and best practices.'').

[65] *See, e.g.,* BCBS Operational Resilience Principles at 2–3 (''The principles for operational resilience set forth in this document are largely derived and adapted from existing guidance that has been issued by the Committee or national supervisors over a number of years. The Committee recognizes that many banks have well established risk management processes that are appropriate for their individual risk profile, operational structure, corporate governance and culture, and conform to the specific risk management requirements of their jurisdictions. By building upon existing guidance and current practices, the Committee is issuing a principles-based approach to operational resilience that will help to ensure proportional implementation across banks of various size, complexity and geographical location.''); FSB Third-Party Report, *supra* note 44, at 10–11; IOSCO, *Principles on Outsourcing: Final Report* at 10 (IOSCO Outsourcing Report) (Oct. 2021) (providing that ''[t]he application and implementation of these Principles should be proportional to the size, complexity and risk posed by the outsourcing'' of tasks, functions, processes, services, or activities to a service provider that would otherwise be undertaken by the regulated entity itself).

[66] *See e.g.,* FINRA, 2018 Report on Selected Cybersecurity Practices at 1 (Dec. 2018) (FINRA Cybersecurity Report) (''[T]here is no one-size-fits-all approach to cybersecurity.''); NIST CSF, *supra* note 46, at 2 (''The [NIST CSF] is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks—different threats, different vulnerabilities, different risk tolerances.'').

[67] *See* NFA ISSP Notice, *supra* note 43 (requiring each NFA member to adopt an ISSP appropriate to the its ''size, complexity of operations, type of customers and counterparties, the sensitivity of the data accessible within its systems, and its electronic interconnectivity with other entities''); NFA Third-Party Notice, *supra* note 43 (''NFA recognizes that a Member must have flexibility to adopt a written supervisory framework relating to outsourcing functions to a [third-party service provider] that is tailored to a Member's specific needs and business . . .'').

[68] *See, e.g.,* 17 CFR 37.1401(b) (SEFs); 17 CFR 38.1051(b) (DCMs); 17 CFR 39.18(b)(3) (DCOs); 17 CFR 49.24(c) (SDRs) (requiring registered entities to follow generally accepted standards and best practices with respect to the development, operation, reliability, security, and capacity of automated systems); *see also* System Safeguards Testing Requirements for Derivatives Clearing Organizations, 81 FR 64322, 64329 (Sept. 19, 2016) (DCO System Safeguards Testing Requirements) (describing the CFTC's approach to system safeguards for DCOs as providing DCOs with ''flexibility to design systems and testing procedures based on the best practices that are most appropriate for that DCO's risks'').

[69] 12 CFR part 30, app. B (Interagency Guidelines Establishing Information Security Standards); *id.* at II.A. (Information Security Program) (''Each [financial institution] shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the [financial institution] and the nature and scope of its activities.''); FFIEC Information Technology Examination Handbook, Information Security at 2 (Sept. 2016) (FFIEC Information Security Booklet) (''Institutions should maintain effective information security programs commensurate with their operational complexities.'').

[70] The NIST CSF, for example, identifies activities designed to achieve specific cybersecurity outcomes and tiers practices by increasing degree of rigor and sophistication. In selecting a tier, NIST directs entities to consider their ''current risk management practices, threat environment, legal and regulatory requirements, information sharing practices, business/mission objectives, supply chain cybersecurity requirements, and organizational constraints.'' *See* NIST CSF, *supra* note 46, at 8.

have more complicated agreements with third-party service providers to arrive at an ORF that is appropriate to their likely increased level of operational risk.[71]

The requirement for covered entities to follow generally accepted standards and best practices serves to ground covered entities' approaches to operational resilience in practices that are widely recognized as effective in aiding financial institutions to mitigate and recover from operational shocks. In adopting system safeguard requirements for registered entities, which require registered entities to follow generally accepted standards and best practices, the Commission identified several sources of standards and best practices.[72] NFA and other bodies have compiled similar lists.[73] Among perhaps the most commonly relied on by financial institutions are the NIST CSF, ISO, the Center for internet Security (CIS), and FFIEC, whose examination booklets and Cyber Assessment Tool (CAT) are specifically designed to guide financial institutions.[74] The Commission would expect covered entities to use generally accepted standards and industry best practices that are appropriate and proportionate to the nature, size, scope, complexities, and risk profile of their business activities, in designing or updating an ORF that would comply with the proposed rule. For instance, in conducting the risk assessment required under proposed paragraph (c)(1), a covered entity would need to identify risks to its information and technology security with reference to risks discussed in an appropriate standard or based on industry best practices, and then assess and prioritize those risks using frameworks and metrics recommended by those standards or practices. Requiring covered entities to follow generally accepted standards and industry best practices in developing and implementing the ORF would help ensure that covered entities establish, document, implement, and maintain ORFs reasonably designed to address their particular operational resilience-related risks.

The proposed rule leverages these standards not only by directing covered entities to consider them in developing their approaches but by incorporating common themes contained within them into the substance of the proposed rule. In the Commission's view, reliance on such standards supports the use of a common lexicon, facilitating the development of understandable and transposable practices on a cross-border basis. The Commission further recognizes that generally accepted standards and best practices are likely to evolve over time, and the applicability of any particular standard may vary based on the unique circumstances and risk profile of each covered entity. Accordingly, the Commission preliminarily believes requiring covered entities to follow generally accepted standards and best practices supports the goal of an adaptive approach that can respond nimbly to rapid changes in emerging threats.[75]

3. Request for Comment

The Commission invites comment on all aspects of proposed paragraph (b), including the following questions:

1. *Applicability to FCMs.* In adopting the RMP rule for FCMs in 2013, the Commission determined to limit the rule's applicability to FCMs that hold or accept customer funds.[76] The CEA and Commission regulations define a ''futures commission merchant'' as an entity that solicits or accepts orders to buy or sell futures contracts, options on futures, retail off-exchange forex contracts or swaps, *and* accepts money or other assets from customers to support such orders.[77] Although some entities are, for various reasons, currently registered as FCMs despite not accepting customer funds, as the Commission explained in the adopting release for the FCM RMP rule, FCMs that do not accept or hold customer funds to margin, guarantee, or security commodity interests are generally not operating as FCMs.[78] With respect to the proposed ORF rule, the Commission has preliminarily determined to apply the proposed requirements to all registered FCMs. Although the customer protection concerns may be mitigated for FCMs that do not handle customer assets, the Commission preliminarily believes that the potential systemic risk that can result from failures to manage information and technology risk, third-party relationships, emergencies, or other significant disruptions persist for all FCMs, given their access to customer information and their potential relationships with and/or connectivity to other regulated entities, including exchanges and clearinghouses.[79]

a. Are the risks associated with information and technology security, third-party relationships, and emergencies or other significant disruptions substantially different or reduced for FCMs that do not hold customer funds? If yes, please explain.

b. Should the Commission consider limiting the ORF rule to FCMs that do not hold customer funds, consistent with the FCM RMP rule? Why or why not? Please explain.

2. *Standard.* The proposed rule would require covered entities to follow ''generally accepted standards and best practices'' in establishing, implementing, and maintaining their ORFs. Although this notice identifies various sources of such standards and practices, including NIST, ISO, CIS, and FFIEC, the proposed rule does not further define or otherwise limit the scope of ''generally accepted standards and best practices,'' acknowledging that there are several sources of recognized standards currently relied on by covered entities and that standards and practices

[71] *See* National Cyber Strategy, *supra* note 41, at 4 (''The most capable and best-positioned actors in cyberspace must be better stewards of the digital ecosystem.''); *see also* IOSCO Outsourcing Report, *supra* note 65, at 10.

[72] *See, e.g.,* DCO System Safeguards Testing Requirements, 81 FR 64322–23; 17 CFR 39.18(b)(3) (requiring DCOs to follow generally accepted standards and best practices with respect to the development, operation, reliability, security, and capacity of automated systems)*; see also* 17 CFR 37.1401(b) (SEFs) (requiring the same); 17 CFR 38.1051(b) (DCMs) (same); 17 CFR 49.24(c) (SDRs) (same).

[73] *See, e.g.,* NFA, Cybersecurity FAQs, ''Does NFA recommend any particular consultants that can help a Member draft an ISSP or perform penetration testing?''; *see also* FFIEC, Cybersecurity Resource Guide for Financial Institutions (Sept. 2022) (rev. Nov. 2022).

[74] The Financial Services Sector Coordinating Council (FSSC) has also developed a NIST CSF profile specifically designed for financial institutions. The profile is now maintained, updated, and managed by the Cyber Risk Institute (CRI) and was last updated in January 2023. *See* CRI Profile v1.2 (Dec. 14, 2021), *available at https://cyberriskinstitute.org/the-profile/.*

[75] *See* National Cyber Strategy, *supra* note 41, at 9 (''By leveraging existing international standards in a manner consistent with current policy and law, regulatory agencies can minimize the burden of unique requirements and reduce the need for regulatory harmonization.'').

[76] *See* 17 CFR 1.11(a) (Nothing in this section shall apply to a futures commission merchant that does not accept any money, securities, or property (or extend credit in lieu thereof) to margin, guarantee, or secure any trades or contracts that result from soliciting or accepting orders for the purchase or sale of any commodity interest.).

[77] *See* 7 U.S.C. 1a(28)(A); 17 CFR 1.3 (defining ''futures commission merchant'') (emphasis added).

[78] As of July 31, 2023, twelve (12) entities were registered as FCMs but were not required to segregate any funds on behalf of customers. *See* CFTC, Financial Data for FCMs (July 31, 2023), *available at https://www.cftc.gov/MarketReports/financialfcmdata/index.htm.* The Commission made clear in the adopting notice for the FCM RMP rule that it would expect that, prior to changing their business model to begin accepting customer funds, any registered FCM that does not currently accept customer funds would need to establish a risk management program that complies with Commission regulation 1.11 and file such program with the Commission and with the FCM's designated self-regulatory organization (DSRO). *See* Final FCM RMP Rule, 78 FR 68517.

[79] The Final FCM RMP rule, by contrast, could be viewed as more directly targeting the management of specific risks associated with operating as an FCM.

are likely to evolve over time in response to changes in technology or emerging threats. Nevertheless, the Commission understands that, particularly in the United States, NIST and ISO standards are heavily relied on by covered entities and referenced by other regulators, making them widely recognized as the leading industry standards for cybersecurity and operational risk management.

a. Should the Commission further define or otherwise limit what constitutes ''generally accepted standards and best practices''? Specifically, should the Commission require covered entities to follow NIST or ISO standards, as some commenters on the RMP ANPRM recommended? [80] Why or why not? Please explain.

b. Are there any other standards or practices commonly relied on by covered entities that the Commission did not identify, directly or indirectly, in this notice? If so, please identify them and specify how they are currently relied on by covered entities.

B. Governance—Proposed Paragraph (c)

The topic of governance has gained increased attention within the context of operational resilience, particularly with respect to the area of information and technology security. As of the date of this notice, NIST is undergoing a process to update the NIST CSF, and new governance outcomes are expected to feature prominently.[81] Prudential regulators have also emphasized the role of effective governance to operational resilience.[82] In the Commission's view, the overall objective of an effective governance regime for an ORF should be the integration of operational resilience topics into existing reporting lines and operational structures, including the entity's overall operational strategy, to ensure active executive engagement and oversight in the management of operational risk that could challenge a covered entity's operational resilience.[83]

1. Approval of Components—*Proposed Paragraph (c)(1)*

Accordingly, to ensure that a covered entity's senior leadership is involved in key decision-making around operational resilience, and is ultimately held accountable for implementation of the ORF, the proposed rule would require covered entities to have their senior leadership annually approve the ORF.[84] In recognition of the wide variety of corporate structures represented among covered entities, however, the proposed rule would give covered entities broad flexibility and discretion to identify the appropriate senior-level individual or body to provide such approval.

Specifically, paragraph (c)(1) of the proposed rule would require that each ORF component program or plan required by paragraph (b)(2) of the proposed rule is approved in writing, on at least an annual basis, by either the senior officer, an oversight body, or a senior-level official of the covered entity.[85] The term ''oversight body'' itself would be broadly defined to encompass any board, body, or committee of a board or body of the covered entity specifically granted the authority and responsibility for making strategic decisions, setting objectives and overall direction, implementing policies and procedures, or overseeing the management of operations for the covered entity.[86] Consistent with Commission regulation 3.1(j), ''senior officer'' would mean the chief executive officer or other equivalent officer of the covered entity.[87] As an example, under the proposed rule, a covered entity could elect to have its information and technology security program annually approved by its chief executive officer, its chief information security officer, or a committee with oversight authority over information and technology security.[88] Again, the intention behind offering this flexibility is to ensure that covered entities would be able to rely on and incorporate operational resilience into their existing governance structures when complying with the proposed ORF rule, while ensuring that each component program or plan would be approved by an individual or group of individuals with senior-level responsibilities and authority.

2. Risk Appetite and Risk Tolerance Limits—*Proposed Paragraph (c)(2)*

The proposed rule would further require covered entities to establish and implement appropriate risk appetite and risk tolerance limits with respect to the three risk areas enumerated in paragraph (b)(1) (information and technology security, third-party relationships, and emergencies or other significant disruptions to the continuity of normal business operations).[89] Although the terms ''risk appetite'' and ''risk tolerance'' are sometimes used interchangeably, the Commission intends the terms to have distinct meanings within the context of the proposed rule. Specifically, in the context of the proposed rule, ''risk appetite'' would mean the aggregate amount of risk a covered entity is willing to assume to achieve its strategic objectives.[90] Risk appetite is typically documented through a risk appetite statement, which establishes qualitative and quantitative measures designed to help identify when risk appetite has been exceeded and what appropriate mitigating strategies that can be taken.[91]

[80] *See, e.g.,* R.J. O'Brien Letter, *supra* note 13, at 6 (''The Commission should also seek to implement the [NIST CSF] as a part of its standard for managing and mitigating this area of risk. The NIST CSF is widely accepted throughout many different industries and would set a universal standard and best practices for registrants to follow.'').

[81] *See* NIST, *NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework* at 10–11 (Jan. 19, 2023) (discussing how the update ''will emphasize the importance of cybersecurity governance'' by adding a new govern function); *see also* CRI, *The Profile Workbook: Guidance for Implementing the CRI Profile v1.2.1 and Responding to its Diagnostic Statements* at 16 (rev. Jan. 2023) (CRI Profile Workbook) (providing guidance on governance outcomes that have already been incorporated into the NIST CSF financial services sector profile).

[82] *See* Prudential Operational Resilience Paper, *supra* note 11, at 3.

[83] *See* BCBS Operational Resilience Principles, *supra* note 11, at 4 (''Principle 1: Banks should utilise their existing governance structure to establish, oversee and implement an effective operational resilience approach that enables them to respond and adapt to, as well as recover and learn from, disruptive events in order to minimise their impact on delivering critical operations through disruption.'') (internal citation omitted).

[84] *See* paragraph (c)(1) of proposed Commission regulations 1.13 and 23.603.

[85] *Id.*

[86] *See* paragraph (a) of proposed Commission regulations 1.13 and 23.603 (defining ''oversight body'').

[87] *See* paragraph (a) of proposed Commission regulations 1.13 and 23.603 (defining ''senior officer''). *See also* 17 CFR 3.1(j) (defining ''senior officer'').

[88] Other possible senior-level officials could be the covered entity's chief risk officer or chief operating officer, as appropriate.

[89] *See* paragraph (c)(2)(i) of proposed Commission regulations 1.13 and 23.603. *See also* paragraph (b)(1) of proposed Commission regulations 1.11 and 23.603 (identifying the risk areas proposed to be covered by the ORF).

[90] *See* paragraph (a) of proposed Commission regulations 1.13 and 23.603 (defining ''risk appetite''). *See also* 12 CFR part 30, app. D, I.E.10 (Definitions) (defining ''risk appetite'' as the aggregate level and types of risk the board of directors and management are willing to assume to achieve a covered bank's strategic objectives and business program, consistent with applicable capital, liquidity, and other regulatory requirements); Prudential Operational Resilience Paper, *supra* note 11, at 14 (defining ''risk appetite'' as ''[t]he aggregate level and types of risk the board and senior management are willing to assume to achieve a firm's strategic business objectives, consistent with applicable capital, liquidity, and other requirements and constraints''); BCBS Operational Resilience Principles, *supra* note 11, at 3, n.7 (defining ''risk appetite'' as ''the aggregate level and types of risk a bank is willing to assume, decided in advance and within its risk capacity, to achieve its strategic objectives and business program'').

[91] *See* 12 CFR part 30, app. D (requiring covered financial institutions to have a comprehensive written risk appetite statement). *See also* CRI Profile

With its proposed definition of ''risk tolerance limit,'' the Commission intends to capture a more focused measure of acceptable risk. Specifically, ''risk tolerance limit'' would mean the amount of risk, beyond its risk appetite, that a covered entity is prepared to tolerate through mitigating actions.[92] Thus, risk tolerance limits assume a particular type of risk has materialized (*e.g.,* an operational disruption has occurred) and identify the amount of disruption a firm is prepared to tolerate beyond its risk appetite.[93] Risk tolerance limits are also more likely to be measured in quantitative terms (*e.g.,* number of hours a particular system or application is down).[94]

As with each component ORF program or plan, the proposed rule would require that a covered entity's risk appetite and risk tolerance limits be reviewed and approved in writing on at least an annual basis by either the senior officer, an oversight body, or a senior-level official of the covered entity.[95] This proposed requirement is intended to ensure that the risk appetite and risk tolerance limits are consistent with the covered entity's operational strategy and objectives, as established by senior leadership, and that senior leadership is involved in, and ultimately held accountable for, how operational risks faced by the covered entity are internalized by the covered entity.

The setting and approval of risk appetite and risk tolerance limits for operational risk is a well-recognized key component of effective governance and oversight.[96] The Commission therefore preliminarily believes the setting and approval of risk appetite and risk tolerance limits for operational risks captured by the ORF would be helpful to ensuring effective governance and oversight of the ORF. Specifically, the Commission believes that the process of identifying appropriate risk appetite and risk tolerance limits would have a disciplining effect, encouraging covered entities to think critically about the risks they face and their ability to comfortably manage them without incurring intolerable harm to themselves or their customers or counterparties. The Commission further believes that operating within set risk appetite and risk tolerance limits would help support a culture where senior leaders at covered entities can make more informed decisions about the risks they are willing to take and the mitigation measures they would need to employ to manage these risks, which would further support operational resilience.

3. Internal Escalations—*Proposed Paragraph (c)(3)*

To further ensure that senior leadership remains involved in and accountable for the ORF as it is implemented, the proposed rule would require either the senior officer, an oversight body, or a senior-level official of the covered entity to be notified of: (i) circumstances that exceed the risk tolerance limits established pursuant to paragraph (c)(2)(i) of the proposed rule; and (ii) incidents that require notification to the Commission, customers, or counterparties under the proposed rule, as further discussed in subsequent sections of this notice.[97]

The Commission believes that circumstances that would push a covered entity outside of its risk tolerance limits or trigger a Commission notification requirement would be extraordinary, non-business-as-usual events, and would likely require the involvement of senior leadership to direct responsive actions to preserve or mitigate damage to operational resilience and prevent situations of intolerable harm. Ensuring that appropriate senior leadership, as determined by the covered entity, is apprised of instances where expected risk tolerance limits have been exceeded would further help senior leadership determine whether the risk appetite and risk tolerance limits are appropriately calibrated and whether identified mitigation strategies are working, creating opportunities to update either as necessary.

4. Consolidated Program or *Plan*—*Proposed Paragraph (c)(4)*

The Commission is aware that many covered entities function as a division or affiliate of a larger entity or holding company structure; and that, in such instances, operational risks stemming from information and technology security, third-party relationships, and emergencies or other significant disruptions are generally monitored and managed at the enterprise level to address the risks holistically and to achieve economies of scale.[98] The proposed rule recognizes the benefits of such a consolidated approach and is not intended to interfere with covered entities' operational structures. Accordingly, the proposed rule would allow covered entities to satisfy the component program or plan requirement in paragraph (b)(2) through its participation in a consolidated program or plan, provided the consolidated program or plan meets the

Workbook, *supra* note 78, at 16 (''Risk appetite statements define certain risk tolerance metrics that help describe systems and services that the organization may consider high-risk.'').

[92] *See* paragraph (a) of proposed Commission regulations 1.13 and 23.603 (defining ''risk tolerance limit''). *See also* Prudential Operational Resilience Paper, at 3, n. 11; 14 (defining ''tolerance for disruption'' as ''determined by a firm's risk appetite for weathering disruption from operational risks considering its risk profile and the capabilities of its supporting operational environment'' and ''informed by existing regulations and guidance and by the analysis of a range of severe but plausible scenarios that would affect its critical operations and core business lines.''); CRI Profile Workbook at 291 (stating that ''risk tolerance'' ''reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve''). ISACA, *Risk IT Framework,* 2nd Ed. (July 27, 2020) (defining ''risk tolerance'' as ''the acceptable deviation from the level set by the risk appetite and business objectives'').

[93] The Commission recognizes that Commission regulations 1.11 and 23.600 incorporate the term ''risk tolerance limits.'' *See* 17 CFR 1.11(e)(1), 17 CFR 23.600(c)(1). As proposed to be defined in the ORF rule, however, ''risk tolerance limits'' would be limited to the context of the risks identified in paragraph (b)(1) of the proposed rule and associated disruptions. Accordingly, if adopted, the defined use of the term ''risk tolerance limit'' in the proposed rule would not be intended to affect how covered entities use or interpret the term in the context of the Commission's RMP rules.

[94] The Commission believes its proposed definitions are in line with proposed definitions of ''risk appetite'' and ''risk tolerance'' used by NIST. For example, in NIST Interagency or Internal Report 8286 (NIST IR 8286), NIST explains that a statement of risk appetite might be that ''[e]mail shall be available during the large majority of a 24-hour period,'' while the associated risk tolerance would be narrower, stating something like ''[e]mail services shall not be interrupted more than five minutes during core hours.'' *See* NIST IR 8286 at 5–6 (Oct. 2020). Accordingly, any existing risk appetite and risk tolerance limits established by covered entities pursuant to NIST or prudential regulator standards would be considered consistent with the proposed rule.

[95] *See* paragraph (c)(2)(ii) of proposed Commission regulations 1.13 and 23.603.

[96] *See, e.g.,* BCBS Operational Resilience Principles, *supra* note 11, at 4 (''The board of directors should review and approve the bank's operational resilience approach considering the bank's risk appetite and tolerance for disruption to its critical operations. In formulating the bank's tolerance for disruption, the board of directors should consider the bank's operational capabilities given a broad range of severe but plausible scenarios that would affect its critical operations. The board of directors should ensure that the bank's policies effectively address instances where the bank's capabilities are insufficient to meet its stated tolerance for disruption.''); CRI Profile v1.2, *supra* note 74.

[97] *See* paragraph (c)(3) of proposed Commission regulations 1.13 and 23.603. *See also* paragraphs (i) and (j) of proposed Commission regulations 1.13 and 23.603, discussed in section II.G of this notice, *infra.*

[98] In responding to the RMP ANPRM, several commenters noted how cybersecurity risk is generally managed at the enterprise level and should not be managed at the level of the entity regulated by the Commission. *See* FIA Letter at 11 (Sept. 18, 2023); International Swaps and Derivatives Association, Inc. (''ISDA'') and the Securities Industry and Financial Markets Association (''SIFMA'') Letter at 9 (Sept. 18, 2023).

requirements of the proposed rule.[99] As defined in the proposed rule, a ''consolidated program or plan'' would mean any information and technology security program, third-party relationship program, or business continuity and disaster recovery plan in which a covered entity participates with one or more affiliates and is managed and approved at the enterprise level.[100]

Nevertheless, the Commission does have a strong regulatory interest in ensuring that operational shocks, such as cyber incidents or technological failures, having an impact on the discrete interests and operations of the covered entity are appropriately considered through the unique lens of the covered entity, which is regulated by the Commission. Accordingly, for a covered entity to satisfy the component program or plan requirement through its participation in a consolidated program or plan, the consolidated program or plan would need to meet the requirements of the proposed rule, as discussed in this notice. Those requirements include the establishment of appropriate risk appetite and risk tolerance limits that address the covered entity, as well as testing and other requirements, as discussed further below.

With respect to the requirements in proposed paragraphs (c)(1) and (c)(2)(i) that senior leadership of the covered entity approve, respectively, the component program or plan and the risk appetite and risk tolerance limits at least annually, the Commission recognizes that such a requirement might be challenging in the context of a consolidated program or plan, which is likely to address matters related to affiliates that are not within the scope of knowledge or responsibility of the covered entity. Accordingly, the proposed rule would allow covered entities relying on a consolidated program or plan to satisfy the approval requirements in paragraphs (c)(1) and (c)(2)(i) of the proposed rule, provided that either the senior officer, an oversight body, or a senior-level official of the covered entity attests in writing, on at least an annual basis, that the consolidated program or plan meets the requirements of this section and reflects the risk appetite and risk tolerance limits appropriate to the covered entity.[101] Notably, the senior officer, an oversight body, or a senior-level official at the covered entity would still need to be notified when the risk appetite and risk tolerance limits related to the covered entity are exceeded.[102] The Commission believes that such an attestation requirement would promote efficiency by allowing covered entities to continue to rely on an enterprise-level ORF and governance structures that have acknowledged benefits while also ensuring that such enterprise-level ORF appropriately addresses the risks specific to the covered entity, and would ensure that the requirements of the Commission's proposed rule are addressed for those covered entities in the same way as they would for a covered entity that is not a part of a larger enterprise.[103]

5. Request for Comment

The Commission invites comment on all aspects of the proposed governance requirements for the ORF, including the following questions:

1. *Governance structures.* The proposed rule is intended to provide covered entities sufficient flexibility to integrate the proposed operational resilience requirements into existing reporting lines and operational structures, as well as to select the individual or body with senior-level responsibilities and authority to approve the component programs or plans of the ORF. Does the proposed rule accomplish this goal? If not, what other governance structure(s) should the Commission consider? Alternatively, should the Commission consider a more prescriptive, bright-line approach where only the senior officer or board of directors of the covered entity may provide any approvals required under the proposed rule? Please explain.

2. *Internal escalations.* The proposed rule would require that the senior officer, an oversight body, or other senior-level official(s) of the covered entity be notified of circumstances that exceed risk tolerance limits or that require reporting to the Commission or counterparties or customers under the proposed rule. Should the Commission require internal escalation to any other specific personnel or under any other circumstances? Please identify and explain why.

3. *Consolidated program or plan.* The proposed rule would allow covered entities relying on a consolidated program or plan to satisfy certain governance requirements by requiring the senior officer, an oversight body, or another senior-level official of the covered entity to attest in writing, on at least an annual basis, that the consolidated program or plan meets the requirements of the rule and reflects a risk appetite and risk tolerance limits appropriate to the covered entity. Is this standard workable for covered entities that function as a division or affiliate of a larger entity or holding company? Why or why not? Do such covered entities typically set their own risk appetite and risk tolerance limits, or are setting such limits conducted at the enterprise level? If they are set at the enterprise level, how is senior leadership of the covered entity typically involved in setting risk appetite and risk tolerance limits?

C. Information and Technology Security Program—Proposed Paragraph (d)

As mentioned above, the proposed rule would require each covered entity's ORF to include an information and technology security program, defined as a written program reasonably designed to identify, monitor, manage, and assess risks relating to information and technology security and that meets the minimum requirements for the program, as set forth in the proposed rule and discussed below.[104] The proposed rule would define ''information and technology security'' as the preservation of (a) the confidentiality, integrity, and availability of covered information and (b) the reliability, security, capacity, and resilience of covered technology.[105] ''Covered information'' would be defined to mean any sensitive or confidential data or information maintained by a covered entity in connection with its business activities as a covered entity.[106] ''Covered technology'' would be defined to mean any application, device, information technology asset, network service,

[99] *See* paragraph (c)(4)(i) of proposed Commission regulations 1.13 and 23.603.

[100] *See* paragraph (a) of proposed Commission regulations 1.13 and 23.603 (defining ''consolidated program''). Again, the specific definitions and minimum requirements of each program are discussed in sections II.C, II.D, and II.E of this notice, *infra*.

[101] *See* paragraph (c)(4)(ii) of proposed Commission regulations 1.13 and 23.603.

[102] *See* paragraph (c)(3)(i) of proposed Commission regulations 1.13 and 23.603.

[103] The Commission also believes this approach would be consistent with NFA's current interpretive notice on ISSPs. *See* NFA ISSP Notice, *supra* note 43 (''[T]o the extent a Member firm is part of a holding company that has adopted and implemented privacy and security safeguards organization-wide, then the Member firm can meet its supervisory responsibilities imposed by Compliance Rules 2–9, 2–36 and 2–49 to address the risks associated with information systems through its participation in a consolidated entity ISSP.'').

[104] *See* paragraph (d) of proposed Commission regulations 1.13 and 23.603. *See also* paragraph (a) of proposed Commission regulations 1.13 and 23.603 (defining ''information and technology security program'').

[105] *See* paragraph (a) of proposed Commission regulations 1.13 and 23.603 (defining ''information and technology security'').

[106] *See* paragraph (a) of proposed Commission regulations 1.13 and 23.603 (defining ''covered information'').

system, and other information-handling component, including the operating environment, that is used by a covered entity to conduct its business activities, or to meet its regulatory obligations, as a covered entity.[107]

The proposed definition of ''covered information'' is intended to focus the requirements of the ORF on protecting data and information that are sensitive or otherwise intended to be kept confidential, whether by law or for business purposes. Notably, such data and information would include position, order, and account information, all of which covered entities have an obligation to keep confidential and which if made public could result in harm to customers, counterparties, or the markets more broadly. Often referred to as the ''CIA triad,'' confidentiality, integrity, and availability represent the three pillars of information security: preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information; guarding against the improper modification or destruction of data and information, ensuring its authenticity; and ensuring the timely and reliable access to and use of information.[108] The Commission therefore believes that compromising any aspect of the CIA triad with respect to covered information would have meaningful consequences for customers, counterparties, the covered entity, or even the market.

The proposed definition of ''information and technology security'' is likewise intended to ensure that the ORF is designed to address risks to two key facets of a covered entities' business for which they are registered with the Commission: the technology they use to conduct their regulated business activities and the sensitive information stored or transmitted therein. The proposed definition of ''covered technology'' is sufficiently broad to capture all types of technology (and related components) but is tailored to focus on the technology that is used by covered entities in the context of their regulated business activities, such that its disruption would have an impact on regulated business activities. The Commission preliminarily believes that reliability, security, capacity, and resilience are all key attributes of covered technology that must be preserved for it to function as intended without posing a disruption to operations. Accordingly, the Commission believes that having a program designed to preserve the confidentiality, integrity, and availability of covered information and the reliability, security, capacity, and resilience of covered technology is key to ensuring operational resilience.

Under the proposed rule, each covered entity's information and technology security program would need to meet the (b)(3) standard, *i.e.,* be appropriate and proportionate to the nature, size, scope, complexities and risk profiles of the covered entity's business activities, following generally accepted standards and best practices.[109] The proposed rule would nevertheless establish certain minimum requirements for the information and technology security program, including a periodic risk assessment, effective controls, and an incident response plan. Each proposed minimum requirement is discussed in turn below.

1. Risk Assessment—*Proposed Paragraph (d)(1)*

As part of the information and technology security program, covered entities would be required to conduct and document the results of a periodic and comprehensive risk assessment reasonably designed to identify, assess, and prioritize risks to information and technology security.[110] Risk assessments are widely recognized as a necessary and effective first step to monitoring and managing risks to information and technology security.[111] According to NIST, the purpose of a risk assessment is to inform decision makers and support risk responses by identifying: (i) relevant threats to organizations or threats directed through organizations against other organizations; (ii) vulnerabilities both internal and external to organizations; (iii) impact (*i.e.,* harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) the likelihood that harm will occur.[112] Given this broad and important purpose, the Commission believes conducting a comprehensive risk assessment would be reasonably necessary for covered entities to have a thorough understanding of their information and technology security risks, including the types of threats the covered entities face, internal and external vulnerabilities, the impact of such risks, and their relative priorities, to guide mitigation efforts.

As stated, the risk assessment would need to identify, assess, and prioritize risks to information and technology security.[113] In broad terms, the Commission anticipates that conducting the assessment could first involve taking an inventory of covered technology and then identifying and assessing the likelihood and potential impact of reasonably foreseeable threats and vulnerabilities to information and technology security (*i.e.,* to the confidentiality, integrity, and availability of covered information, or to the reliability, security, capacity or resilience of covered technology) in light of the existing operational environment. Identified threats and vulnerabilities could derive from a wide array of sources, including both external cyber threats and internal gaps in existing systems or controls.

The Commission would then expect the risks to be prioritized in light of the covered entity's stated risk appetite and risk tolerance limits to help direct resources and other activities in order to best support information and technology security. If the proposal is adopted as final, the Commission would expect covered entities to use the results of each risk assessment as a basis for designing, implementing, and refining other elements of its information and technology security program, including

[107] *See* paragraph (a) of proposed Commission regulations 1.13 and 23.603 (defining ''covered technology'').

[108] *See* NIST, SP 1800–26, Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events (Dec. 2020) (discussing the CIA triad).

[109] *See* paragraph (b)(3) of proposed Commission regulations 1.13 and 23.603.

[110] *See* paragraph (d)(1)(i) proposed Commission regulations 1.13 and 23.603.

[111] *See, e.g.,* ISO/IEC 27001:2022, *supra* note 48 (requiring a risk assessment to help organizations identify, analyze, and evaluate weaknesses in their information systems); ISO/IEC 31010:2019, *Risk management: Risk assessment techniques* (July 2, 2019); NIST, SP 800–39, *Managing Information Security Risk: Organization, Mission, and Information System View* at 37 (Mar. 2011) (NIST SP 800–39) (''Risk assessment identifies, prioritizes, and estimates risk to organizational operations (*i.e.,* mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems. Risk assessments use the results of threat and vulnerability assessments to identify and evaluate risk in terms of likelihood of occurrence and potential adverse impact (*i.e.,* magnitude of harm) to organizations, assets, and individuals.''); NIST, SP 800–30, *Guide for Conducting Risk Assessments,* Rev. 1, at ix (Sept. 2012) (NIST SP 800–30) (''Risk assessments are a key part of effective risk management and facilitate decision making . . .''). *See also* 12 CFR part 30, app. B (establishing a requirement to assess risk by identifying reasonably foreseeable threats, assessing the likelihood and potential damage of the threats, and assessing the sufficiency of arrangements to control risks); Prudential Operational Resilience Paper, *supra* note 11, at 4 (''The firm's operational risk management function implements and maintains risk identification and assessment approaches that adequately capture business processes and their associated operational risks, including technology and third-party risks.'').

[112] *See* NIST SP 800–30 at 1.

[113] *See* paragraph (d)(1)(i) proposed Commission regulations 1.13 and 23.603.

but not limited to, the development of controls, testing protocols, and the incident response plan, as discussed further below.[114] In this way, a well-conducted risk assessment should support the development of a more rational, effective, and valuable information and technology security framework, especially as the assessment is repeated and built upon over time.

The proposed rule would not prescribe a specific process or methodology for the risk assessment, but the risk assessment would need to be consistent with the proposed (b)(3) standard.[115] Following generally accepted standards and best practices, covered entities would need to implement processes and methodologies that ensure the risk assessment reflects the nature, size, scope, complexities, and risk profile of its business activities as a covered entity. Any such processes or methodologies should also be sufficient to identify, assess, and prioritize risks to information and technology security and to evaluate their potential impact on covered technology and covered information.[116]

To ensure that the risk assessment is conducted objectively, the proposal would require that the personnel involved in conducting the assessment are not responsible for the development or implementation of the covered technology or related controls.[117] Such personnel could be employees of the covered entity, an affiliated entity, or a third-party service provider. To ensure that senior leadership is aware of risks to information security, and can appropriately prioritize them within the covered entity's broader strategy and risk management framework, the proposed rule would expressly require that the results of the risk assessment be provided to the senior officer, oversight body, or other senior-level official who approves the information and technology security program upon the risk assessment's completion.[118] The Commission believes the results of the risk assessment would be key information for senior leadership in determining whether to approve an information and technology security program.

The proposed rule would require that the covered entity conduct the risk assessment at a frequency consistent with the (b)(3) standard (*i.e.,* a frequency appropriate and proportionate to the nature, scope, and complexities of its business activities as a covered entity, following generally accepted standards and best practices) but, in any case, no less frequently than annually.[119] Given the rapidly evolving nature of technological developments and related threats, the Commission preliminarily believes that a uniform requirement to conduct a risk assessment on at least an annual basis would support the development of a strong, foundational level of information and technology security across the industry, thereby mitigating the overall threat of systemic risk. However, the Commission understands that generally accepted standards and best practices may encourage more frequent risk assessments for covered entities that engage in broader or more complex business activities and would expect covered entities to conduct risk assessments more frequently if the circumstances so require.

As mentioned above, the proposed rule would allow covered entities to satisfy the requirement to have an information and technology security program through its participation in a consolidated information and technology security program.[120] Accordingly, such covered entities would be allowed to rely on a risk assessment that is conducted at an enterprise level. In such cases, the Commission would expect that the covered entities review the program and supporting policies and procedures for conducting the risk assessment to ensure it captures and assesses the risks to the covered entity consistent with the proposed rule so as to support the related attestation requirement.[121]

2. Effective Controls—*Proposed Paragraph (d)(2)*

The proposed rule would require that the information and technology security program establish, document, implement, and maintain controls reasonably designed to prevent, detect, and mitigate identified risks to information and technology security.[122] An essential component of any information and technology security program, and a critical component of a covered entity's overall ORF, controls (also referred to as ''countermeasures'' or ''safeguards'') include any measures (actions, devices, procedures, techniques) designed to promote information and technology security.[123] The selection, design, and implementation of controls can therefore have significant implications for a covered entity's information and technology security and overall operational resilience.[124] Accordingly, the Commission believes effective controls would be a critical component of a covered entity's overall ORF.

Although the proposed rule would not mandate that covered entities implement specific controls, it would require covered entities to consider, at a minimum, certain categories of controls, discussed below, and adopt those consistent with the (b)(3) standard.[125] If the proposal is adopted as final, the Commission would further expect that a particular covered entity's determination of which controls to implement would be guided by the results of its risk assessment, considering the covered entity's risk appetite and risk tolerance limits.[126]

---

[114] *See* NIST SP 800–39 at 34 (''Information generated during the risk assessment may influence the original assumptions, change the constraints regarding appropriate risk responses, identify additional tradeoffs, or shift priorities.'').

[115] *See* paragraph (b)(3) of proposed Commission regulations 1.13 and 23.603, discussed *supra.* The Commission is aware of several sources for industry standards and best practices regarding information security risk assessments. *See, e.g.,* NIST SP 800–39; *see also* FFIEC Information Security Booklet, *supra* note 69.

[116] *See* paragraph (d)(1)(i) of proposed Commission regulations 1.13 and 23.603.

[117] *See* paragraph (d)(1)(ii) of proposed Commission regulations 1.13 and 23.603.

[118] *See* paragraph (d)(1)(iii) of proposed Commission regulations 1.13 and 23.603. *See also* NIST SP 800–30, *supra* note 111, at 1 (''The purpose of risk assessments is to inform decision makers and support risk responses . . .'').

[119] *See* paragraph (d)(1)(ii) of proposed Commission regulations 1.13 and 23.603.

[120] *See* paragraph (c)(4)(i) of proposed Commission regulations 1.13 and 23.603.

[121] *See* paragraph (c)(4)(ii) of proposed Commission regulations 1.13 and 23.603.

[122] *See* paragraph (d)(2) of proposed Commission regulations 1.13 and 23.603.

[123] *See* Committee on Payments and Market Infrastructures (CPMI), IOSCO, *Guidance on cyber resilience for financial market infrastructures* at 7 (Jun. 2016) (CPMI IOSCO Cyber Resilience Guidance) (noting that a strong information and communications technologies control environment is a fundamental and critical component of overall cyber resilience). *See also* NIST SP 800–53, *supra* note 46, at 8 (''Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and reflecting the protection needs of organizational stakeholders. Controls are selected and implemented by the organization in order to satisfy the system requirements. Controls can include administrative, technical, and physical aspects.''); ISO/IEC 27001:2022, *supra* note 48, Annex A (*Information security management systems*) (providing guidelines for 93 objectives and controls).

[124] *See* Prudential Operational Resilience Paper, *supra* note 11, at 8 (identifying as a sound practice for operational resilience routinely applying and evaluating the effectiveness of processes and controls to protect confidentiality, integrity, availability, and overall security of data and information systems).

[125] *See* paragraphs (d)(2)(i)–(xii) of proposed Commission regulations 1.13 and 23.603 (identifying categories of controls for covered entities to consider). *See also* paragraph (b)(3) of proposed Commission regulations 1.13 and 23.603.

[126] *See* paragraph (c)(2) of proposed Commission regulations 1.13 and 23.603 (requiring covered

Adopted controls would also need to address risks to information and technology security identified through other means, including outcomes of continuous monitoring of threats and vulnerabilities, actual and attempted cyber-attacks, threat intelligence, scenario analysis, and the likelihood and realistic impact of such attacks. In other words, the controls would need to be linked to and address the identified and prioritized risks to information and technology security. The Commission would advise covered entities to document their consideration of controls within each of the enumerated categories and their reasoning for adopting specific controls within any given category, or for declining to adopt any controls within a particular category. Further, the Commission would expect those controls to be reviewed and revised as needed to reflect the results of the covered entity's most recent risk assessment.

The specific categories of controls the Commission would require covered entities to consider under the proposed rule include: access controls; access restrictions; encryption; dual control procedures,[127] segregation of duties, and background checks; change management practices; system development and configuration management practices; flaw remediation; measures to protect against destruction, loss, or damage to covered information; monitoring systems and procedures to detect attacks or intrusions; response programs; and measures to promptly recover and secure any compromised covered information.[128]

The Commission preliminarily believes that these categories of controls collectively represent a comprehensive array of controls for ensuring the information and technology security. Access controls, access restrictions, encryption, and background checks would limit access to covered technology and covered information to individuals with a legitimate business need in both physical and digital environments. Dual control procedures, segregation of duties, procedures relating to modifications to covered technology, and measures to protect against destruction, loss, or damage to covered information, would support the integrity and availability of covered information from accidental or intentional damage or disclosure to unauthorized recipients. Change management practices would ensure that the information and technology security program, and associated controls, continue to operate as intended over time as systems and processes are updated. Systems development, configuration management, and flaw remediation practices would operate to ensure the integrity and availability of covered technology throughout any updates to covered technology or following a vulnerability analysis.[129] Measures to protect against destruction of covered information due to environmental hazards would further ensure that covered information remains available even following a physical disruption. Monitoring systems and procedures, response programs, and measures to promptly recover and secure any compromised covered information would serve to detect unauthorized access to covered information and to recover it if the covered entity's access to the covered information were impaired (*e.g.,* through a ransomware attack).

The proposed rule is modeled after an approach adopted by prudential regulators. Since the early 2000s, prudential regulators have required financial institutions to consider a similar list of categories of controls when designing their information security programs.[130] In adopting their list of categories, prudential regulators described them as designed to control identified risks and to achieve the overall objective of ensuring the security and confidentiality of customer information.[131] Prudential regulators further emphasized that the categories were broad enough to be adapted by institutions of varying sizes, scope of operations, and risk management structures, such that the manner of implementing the guidelines would vary from institution to institution.[132] Given that the list of control categories developed by prudential regulators, many of which are included in the Commission's proposed rule, has a longstanding history of being effective and adaptable to the financial industry at large, the Commission preliminarily believes that incorporating a similar approach with respect to covered entities would also further the Commission's intent to adopt a flexible rule that can be tailored to each individual covered entity and adapted over time to respond to changing threat environments and risk profiles.[133]

3. Incident Response Plan—Proposed Paragraph (d)(3)

The proposed rule would require that the 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.[134] A hallmark of operational resilience is the recognition that although meaningful steps can be taken to prevent and deter risks to information and technology security, such risks may never be entirely eliminated.[135] As the ION incident illustrated, quick and complete recovery of covered technology and operations may be key to mitigating the potential systemic impact to the financial markets. Accordingly, a crucial aspect of any information and technology security program, and therefore any ORF, is having a plan to respond to and recover from events that may create risks to information and technology security.[136]

entities to establish and implement risk appetite and risk tolerance limits).

[127] Dual control procedures refer to a technique that requires two or more separate persons, operating together, to protect sensitive data and information. Both persons are equally responsible for protecting the information and neither can access the information alone. *See* Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 FR 8616, 8622 (Feb. 1, 2001) (Interagency Guidelines Safeguarding Customer Information).

[128] *See* paragraphs (d)(2)(i)–(xi) of proposed Commission regulations 1.13 and 23.600.

[129] Based on its experience, the Commission further believes that that failures in change management, systems development, and vulnerability patching practices are common sources of disruption among financial institutions and are often neglected control areas.

[130] *See* Interagency Guidelines Safeguarding Customer Information, 66 FR 8616; *see also* 12 CFR part 30, app. B. The guidelines were expanded and retitled, ''Interagency Guidelines Establishing Information Security Standards'' in 2004, *see* Proper Disposal of Consumer Information Under the Fair and Accurate Credit Transactions Act of 2003, 69 FR 77610 (Dec. 28, 2004).

[131] *See* Interagency Guidelines Safeguarding Customer Information, 66 FR 8621.

[132] Commenters further supported the level of detail, *see id.* at 8622.

[133] NIST has compiled a comprehensive catalog of security and privacy controls for all types of computing platforms, including general purpose computing systems, cyber-physical systems, cloud systems, mobile systems, and Internet of Things (IoT) devices. *See* NIST SP 800–53, *supra* note 123.

[134] *See* paragraph (d)(3) of proposed Commission regulations 1.13 and 23.603. The Commission is aware that some covered entities may have established an incident response plan as a separate document or as an attachment to another plan, such as a BCDR plan. If the proposed rule is adopted, the Commission would be agnostic as to where a covered entity elects to house its incident response plan provided it otherwise meets the requirements of the proposed rule, including recordkeeping, furnishing it to the Commission upon request, and distributing it to personnel.

[135] *See* BCBS Operational Resilience Principles, *supra* note 12, at 1 (stating that, in recognition that ''the range of potential hazards cannot be prevented,'' the focus should be on ''the ability of banks to withstand, adapt to and recover from potential hazards and thereby mitigate potentially severe adverse impacts'').

[136] *See, e.g.,* BCBS Operational Resilience Principles at 7, n.18 (''The goal of incident

Continued

The Commission believes, therefore, that an effective incident response plan would help covered entities minimize the potential impact to their operations and customers or counterparties when negative events occur, facilitating their recovery as swiftly and successfully as possible.[137] It can also assist in securing against the destruction or theft of sensitive and important confidential customer or counterparty information, which could have a very real impact on their business and assets.

For purposes of the proposed rule, ''incident'' would be defined as any event, occurrence, or circumstance that could jeopardize information and technology security, including if it occurs at a third-party service provider.[138] The purpose of the incident response plan is to identify and classify foreseeable types of incidents and to establish steps to detect, assess, contain, mitigate the impact of, and recover from incidents. The Commission's proposed definition of ''incident'' is intentionally broad to ensure that the incident response plan would address any event that could reasonably jeopardize (*i.e.,* endanger or put at risk) information and technology security, even if that danger never materializes or the incident response plan is otherwise successful at preventing or reversing the danger. As defined in the proposed rule, ''incident'' is broad enough to cover various types of risks to covered technology (*e.g.,* disruption or modification) or covered information (*e.g.,* disclosure or destruction), regardless of the source (*e.g.,* external threat actor or internal staff, physical or electronic) or whether the event was accidental or malicious in nature, since intent may not be readily determined at the outset of an incident. Common examples of incidents would include unauthorized access to a system or data; unauthorized changes to system hardware, software, or data; or a failure of controls that could, if not addressed, endanger information and technology security.

Consistent with the general framework for the ORF as a whole, the proposal would require the incident response plan to meet certain minimum requirements.[139] In broad terms, these requirements focus on identifying persons relevant to an incident response (*i.e.,* personnel involved in responding to the incident and persons who should be notified of such incidents) and how and when they should be involved; documenting the nature of the covered entity's response; and remediating any weaknesses that lead to the incident.[140] The Commission believes that clearly identifying parties who would be involved in incident response, including external parties like third-party service providers and law enforcement, and establishing associated roles and responsibilities would help ensure that incidents are: (1) resolved in a timely manner and by appropriate personnel; (2) adequately resourced financially, operationally, and staffing-wise; and (3) disclosed to appropriate persons either within senior leadership of the covered entity or externally, where required.[141] The process of documenting incidents and management's response, as well as any subsequent remediation efforts, would assist with any related reporting obligations and required information sharing, as well as with subsequent testing of the incident response plan or post-mortem analysis, which would potentially lead to adjustments in subsequent risk assessments and provide lessons learned that could serve to help prevent the occurrence of incidents in the future.[142]

Among these minimum requirements for the incident response plan is the need for it to include escalation protocols, *i.e.,* a process of identifying when to involve or alert specific personnel, including senior leadership, of an incident.[143] Specifically, the proposed rule would require that the senior officer, oversight body, or other senior-level official that has primary responsibility for overseeing the information and technology security program; the Chief Compliance Officer (CCO); [144] and any other relevant personnel be timely informed of incidents that may significantly impact the covered entity's regulatory obligations or require notification to the Commission.[145] This provision is designed to ensure that every individual who has a role in responding to an incident at a covered entity would be appropriately notified. CCOs of covered entities in particular have a duty to take reasonable steps to ensure compliance with Commission regulations relating to the covered entities' business as a covered entity.[146] Timely disclosure of incidents to the CCO that could impact a covered entity's regulatory obligations or require disclosure to the Commission would therefore be crucial for a covered entity CCO to fulfill the duty to take reasonable steps to ensure compliance. As previously discussed above in the section addressing governance, the Commission believes that involving senior leadership in incident response would be particularly important to ensure that they are apprised of and held accountable for the ultimate effectiveness of the ORF, and that incidents receive proper attention and are swiftly addressed.

4. Request for Comment

The Commission invites comment on all aspects of the proposed information and technology security program requirement, including the following questions:

1. *Risk Assessment.*

a. The proposed rule would require that the risk assessment be provided to relevant senior leadership of the covered entity upon its completion but would not require that such senior leadership certify in writing that they have received the results of the risk assessment or approve the results of the risk assessment. Such approvals and certifications may be required in other contexts to ensure that senior leadership

management is to limit the disruption and restore critical operations in line with the bank's risk tolerance for disruption.''). *See also* FFIEC Information Security Booklet, *supra* note 69, 50–51 (''containing the incident, coordinating with law enforcement and third parties, restoring systems, preserving data and evidence, providing assistance to customers, and otherwise facilitating operational resilience''); NIST, SP 800–184, *Guide for Cybersecurity Event Recovery* (Dec. 2016) (NIST SP 800–184) (''evaluate the potential impact, planned response activities, and resulting recovery processes long before an actual cyber event takes place''); CIS, *Incident Response Policy Template: Critical Security Controls* (Mar. 8, 2023) at 4 (''The primary goal of incident response is to identify threats on the enterprise, respond to them before they can spread, and remediate them before they can cause harm.'') (CIS Incident Response Template).

[137] *See* FFIEC, CAT at 52 (May 2017) (''The incident response plan is designed to ensure recovery from disruption of services, assurance of data integrity, and recovery of lost or corrupted data following a cybersecurity incident''); CPMI IOSCO Cyber Resilience Guidance, *supra* note 123, at 16 (recognizing the incident response plan enables the business ''to resume critical operations rapidly, safely and with accurate data'').

[138] *See* paragraph (a) of proposed Commission regulations 1.13 and 23.603 (defining ''incident'').

[139] *See* paragraphs (d)(3)(i)–(vi) of proposed Commission regulations 1.13 and 23.603.

[140] See id.

[141] *See also* NIST SP 800–61 (''It is important to identify other groups within the organization that may need to participate in incident handling so that their cooperation can be solicited before it is needed. Every incident response team relies on the expertise, judgment, and abilities of others . . .'').

[142] *See* NIST SP 800–184, *supra* note 132; CIS Incident Response Template, *supra* note 136, at 4 (''Without understanding the full scope of an incident, how it happened, and what can be done to prevent it from happening again, defenders will just be in a perpetual 'whack-a-mole' pattern.'').

[143] *See* paragraph (d)(3)(ii) of proposed Commission regulations 1.13 and 23.603.

[144] *See* 17 CFR 3.3 (establishing the qualifications and duties of covered entity CCOs).

[145] *See* paragraph (d)(3)(ii) of proposed Commission regulations 1.13 and 23.603. *See also* paragraph (i) of proposed Commission regulations 1.13 and 23.603 (requiring notification of certain incidents to the Commission), discussed in section II.H of this release, *infra.*

[146] *See* 17 CFR 3.3(d)(3).

is aware of risk assessments and consider them in establishing strategic goals, risk appetite, and risk tolerance limits. Should the Commission require such a certification or approval? Why or why not? Please explain.

b. Given the rapidly evolving technological and threat landscape, the proposed rule would require risk assessments to be performed on at least an annual basis to support the mitigation of systemic risk and develop a strong baseline standard across covered entities. The Commission is aware of standards imposing risk assessments as frequently as every six months and as infrequently as every two years. Should the Commission consider a shorter or longer baseline frequency for risk assessments? Why or why not? Please explain.

2. *Effective controls.* The proposed rule would require covered entities to consider broad categories of controls and determine which to adopt consistent with the proposed (b)(3) standard. The Commission is also aware that certain controls, including firewalls, antivirus, and multifactor authentication (MFA) are commonly recommended within the industry. With respect to MFA, which requires users to present two or more authentication factors at login to verify their identity before they are granted access, CISA advises that implementing MFA is important because it makes it more difficult for threat actors to gain access to information systems, even if passwords or PINs are compromised through phishing attacks or other means.[147] In 2021, FFIEC issued guidance advising financial institutions that MFA or controls of equivalent strength, including for those employees, could help more effectively mitigate risks when a financial institution's risk assessment indicates that single-factor authentication with layered security is inadequate.[148] The guidance added that MFA factors, which may include memorized secrets, look-up secrets, out-of-band devices, one-time-password devices, biometrics identifiers, and cryptographic keys, can vary in terms of usability, convenience, and strength and their ability to be exploited.[149] That same year, the Federal Trade Commission updated its rule for safeguarding customer information to mandate financial institutions to adopt MFA for all users.[150] The Commission preliminarily believes that requiring covered entities to implement such widely recommended controls, such as and including MFA, would help reduce cyber security risks and clarify expectations. Should the Commission mandate the use of any specific controls, including firewalls, antivirus, and/or MFA? Why or why not? Please explain.

3. *Incident response plan.* As proposed, covered entities would be required to notify their CCOs of incidents that they have determined may significantly impact regulatory obligations or require notification to the Commission. Commission staff are aware of instances where covered entity CCOs have not been notified of incidents sufficiently early to play a meaningful role in determining whether the incident implicates any CFTC requirements and in developing an appropriate remediation plan. Should covered entities be required to notify their CCOs of all incidents, only incidents that may require notification under the proposed rule, or incidents that may require notification under the proposed rule to other financial regulatory authorities? Why or why not?

D. Third-Party Relationship Program—Proposed Paragraph (e)

The second program required to be included as part of the proposed ORF would be a third-party relationship program, defined as a written program reasonably designed to identify, monitor, manage, and assess risks relating to third-party relationships that meets the requirements of the proposed rule.[151] The Commission understands that covered entities currently routinely rely upon third parties for a wide variety of products, services, and activities, including, for example, information technology, counterparty or customer relationship management, accounting, compliance, human resources, margin processing, trading, and risk management. Reliance on third-party service providers carries many potential benefits, including a reduction in operating costs and access to technological advancements that can improve operations and regulatory compliance.[152]

But that reliance is not riskless.[153] As the ION incident illustrated, operational disruptions of third-party services, particularly of those important to a firm's operations or regulatory obligations, can present challenges for individual firms and even the financial system as a whole.[154] The risks may vary from minor to significant, depending on the nature of the provider or the service being rendered, but they are inherent in the nature of a third-party service provider relationship, in which a firm relies on the performance of another entity and the quality and reliability of that performance is not in the direct control of the firm.[155] The Commission accordingly believes that, in order to support their operational resilience, covered entities should have a plan in place to identify, monitor, manage, and assess the risks associated with third-party relationships.[156]

---

[147] CISA, Multi-Factor Authentication Fact Sheet (Jan. 2022), *available at https://www.cisa.gov/sites/default/files/publications/MFA-Fact-Sheet-Jan22-508.pdf.* NIST defines MFA as ''[a]n authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are *something you know, something you have, and something you are.*'' NIST, SP 800–63–3, *Digital Identity Guidelines* at 49 (June 2017).

[148] FFIEC, Authentication and Access to Financial Institution Services and Systems at 7 (rev. Jan. 5, 2022).

[149] *Id.*

[150] *See* Standards for Safeguarding Customer Information, 86 FR 70272 (Dec. 9, 2021); *see also* 16 CFR 314.4(c)(5) (requiring financial intuitions to ''[i]mplement multi-factor authentication for any individual accessing any information system unless [a qualified individual, as defined in the rule] has approved in writing the use of reasonably equivalent or more secure access controls.'').

[151] *See* paragraph (e) of proposed Commission regulations 1.13 and 23.603. *See also* paragraph (a) of proposed regulations 1.13 and 23.603 (defining ''third-party relationship program'').

[152] *See* Prudential Third-Party Guidance, 88 FR 37927 (''The use of third parties can offer banking organizations significant benefits, such as access to new technologies, human capital, delivery channels, products, services, and markets.''); IOSCO Outsourcing Report, *supra* note 65, at 4 (''The benefits of outsourcing include lowering costs, increasing automation to speed up tasks and reduce the need for manual intervention, and providing flexibility to allow regulated entities to rapidly adjust both to the scope and scale of their activities.''); FFIEC, *Information Technology Examination Handbook, Outsourcing Technology Services Booklet* at 1 (June 2004) (''The ability to contract for technology services typically enables an institution to offer its customers enhanced services without the various expenses involved in owning the required technology or maintaining the human capital required to deploy and operate it.'').

[153] *See* Prudential Third-Party Guidance, 88 FR 37927 (''[T]he use of third parties can reduce a banking organization's direct control over activities and may introduce new risks or increase existing risks, such as operational, compliance, and strategic risks.'').

[154] *See supra* note 20 and accompanying text.

[155] *See* Prudential Third-Party Guidance, 88 FR 37927 (''Increased risk often arises from greater operational or technological complexity, newer or different types of relationships, or potential inferior performance by the third party. A banking organization can be exposed to adverse impacts, including substantial financial loss and operational disruption, if it fails to appropriately manage the risks associated with third-party relationships.'').

[156] For purposes of the proposed rule, the Commission would construe ''third-party service provider'' broadly and consistently with the terms ''third-party'' and ''business arrangement'' as used in the Prudential Third-Party Relationship Guidance. *See id.* (''Third-party relationships can include, but are not limited to, outsourced services, use of independent consultants, referral arrangements, merchant payment processing

Continued

As mentioned above, the Commission appreciates that the risks presented by individual third-party relationships may vary depending on the firm, the provider, or service. For instance, risks may be more elevated if the service provider is a new entrant to the marketplace or the service relates to a new, untested technology, and covered entities with more numerous or intricate third-party relationships may experience greater overall risk from third parties by virtue of the number and complexity of their relationships. Accordingly, the proposed rule would not require third-party relationship programs to apply an identical degree of scrutiny and oversight to all third-party relationships. Instead, consistent with the principles-based focus of the proposed rule, and the proposed (b)(3) standard, the Commission would expect covered entities to adopt a third-party relationship program that helps them identify and assess the risks of their existing and future third-party relationships and adapt their risk management practices consistent with those risks, their risk appetite and risk tolerance limits, and the nature, size, scope, complexity, and risk profile of their business activities, following generally accepted standards and best practices.[157]

1. Third-Party Relationship Lifecyle Stages—Proposed Paragraph (e)(1)

To guide covered entities in developing their third-party relationship programs, and to ensure that the programs address the full scope of risks that third-party relationships can present, the proposed rule would require the third-party relationship program to describe how the covered entity would address the risks attendant to each stage of the third-party relationship lifecycle.[158] Specifically, the proposed rule would require the program to address: (i) pre-selection risk assessment; (ii) the due diligence process for prospective third-party relationships; [159] (iii) contractual negotiations; (iv) ongoing monitoring during the course of the relationship; and (v) termination of the relationship, including preparations for planned and unplanned terminations.[160]

Each of these stages offers covered entities opportunities to assess and take steps to mitigate the potential risks associated with reliance on third-party service providers. At the outset, covered entities should determine whether it is appropriate for a third-party service provider to perform a particular service and evaluate the associated risks.[161] For instance, the determination to secure a third-party service provider may carry greater risks where the service directly impacts a regulatory requirement, where the third-party service provider would be given direct access to covered information, or where a disruption of services could impact regulatory compliance or have a negative impact on customers or counterparties. Due diligence provides covered entities with information to assess whether a prospective third-party service provider is equipped, operationally and otherwise, to perform as expected.[162] Contractual negotiations offer a possibility to mitigate potential risks by including provisions to assign specific responsibilities or liabilities, but may also contribute to risks, especially where a covered entity may have more limited negotiating power.[163] Ongoing monitoring of a third-party service provider's performance likewise aids covered entities in identifying whether selected third-party service providers remain able to perform as expected throughout the duration of the relationship.[164] Finally, the manner in which the relationship ends can have a major impact on the covered entity, particularly if it ends due to a breach of performance. Plans to address the termination, through contingencies or otherwise, could therefore prove important to ensuring the covered entity's ongoing operations.[165] The Commission therefore preliminarily believes that effective management of third-party risks would require covered entities to have a program that establishes methodologies and practices to assess and manage the risks of third-party relationships throughout each of these five stages of the third-party relationship lifecycle.[166]

2. Heightened Requirements for Critical Third-Party Service Providers—Proposed Paragraph (e)(2)

Although the Commission appreciates that third-party risks are not uniform, it nevertheless believes that certain circumstances warrant enhanced risk management practices across all covered entities. Specifically, the proposed rule would require that the third-party relationship program establish heightened due diligence and ongoing

services, services provided by affiliates and subsidiaries, and joint ventures. Some banking organizations may form third-party relationships with new or novel structures and features—such as those observed in relationships with some financial technology (fintech) companies.'').

[157] *See* paragraph (b)(3) of proposed Commission regulations 1.13 and 23.603. *See also* NFA Third-Party Notice, *supra* note 43 (''NFA recognizes that a Member must have flexibility to adopt a written supervisory framework relating to outsourcing functions to a Third-Party Service Provider that is tailored to a Member's specific needs and business . . .''); Prudential Third-Party Guidance, 88 FR 37924 (''[I]t is the responsibility of the banking organization to identify and evaluate the risks associated with each third-party relationship and to tailor its risk management practices, commensurate with the banking organization's size, complexity, and risk profile, as well as with the nature of its third-party relationships.'').

[158] *See* paragraph (e)(1) of proposed Commission regulations 1.13 and 23.603.

[159] The proposed rule is not intended to interfere with the obligation in Commission regulation 1.11(e) for FCMs to conduct onboarding and ongoing due diligence on depositories carrying customer funds. *See* 17 CFR 1.11(e)(3)(i)(A)–(B).

[160] *See* paragraphs (e)(1)(i)–(v) of proposed Commission regulations 1.13 and 23.603. *See also* NFA Third-Party Notice (requiring NFA members to establish a written supervisory framework that includes an initial risk assessment, onboarding due diligence, ongoing monitoring, termination, and recordkeeping); 12 CFR part 30, app. B, III.D. (Oversee Service Provider Arrangements) (requiring financial institutions to exercise appropriate due diligence in selecting service providers, contract with service providers to implement ''appropriate measures designed to meet the objectives of'' prudential guidelines for information security; and, where indicated by its risk assessment, monitor service providers to confirm they have satisfied their obligations).

[161] *See* NFA Third-Party Notice (''At the outset, a Member should determine whether a particular regulatory function is appropriate to outsource and evaluate the risks associated with outsourcing the function.''); Prudential Third-Party Guidance, 88 FR 37928 (''As part of sound risk management, effective planning allows a banking organization to evaluate and consider how to manage risks before entering into a third-party relationship.'').

[162] *See* IOSCO Outsourcing Report, *supra* note 65, at 18 (''It is important that regulated entities exercise due care, skill, and diligence in the selection of service providers. The regulated entity should be satisfied that the service provider has the ability and capacity to undertake the provision of the outsourced task effectively at all times.''); Prudential Third-Party Guidance, 88 FR 37929 (''Conducting due diligence on third parties before selecting and entering into third-party relationships is an important part of sound risk management. It provides management with the information needed about potential third parties to determine if a relationship would help achieve a banking organization's strategic and financial goals. The due diligence process also provides a banking organization with the information needed to evaluate whether it can appropriately identify, monitor, and control risks associated with the particular third-party relationship.'').

[163] *See* IOSCO Outsourcing Report at 21 (''Contractual provisions can reduce the risks of non-performance or aid the resolution of disagreements about the scope, nature, and quality of the service to be provided.'').

[164] *See id.* at 18 (''The regulated entity should also establish appropriate processes and procedures for monitoring the performance of the service provider on an ongoing basis to ensure that it retains the ability and capacity to continue to provide the outsourced task.'').

[165] *See id.* at 33 (''Where a task is outsourced, there is an increased risk that the continuity of the particular task in terms of daily management and control of that task, related information and data, staff training, and knowledge management, is dependent on the service provider continuing in that role and performing that task.'').

[166] *See* Prudential Third-Party Guidance, 88 FR 37928 (''Effective third-party risk management generally follows a continuous life cycle for third-party relationships.'').

monitoring practices with respect to third-party service providers deemed critical third-party service providers.[167] The proposed rule would define ''critical third-party service provider'' to mean a third-party service provider, the disruption of whose performance would be reasonably likely to either (a) significantly disrupt a covered entity's businesses operations or (b) significantly and adversely impact the covered entity's counterparties or customers.[168] The Commission understands that it is common practice for financial institutions, whether by regulatory mandate or otherwise, to identify a subset of services or providers more central to their operations and apply greater scrutiny and oversight to them to ensure the services are provided without disruption. The proposed rule's definition of ''critical third-party service provider'' focuses on the potential impact a disruption to performance would have on the covered entity's regulated business operations, customers, or counterparties. Where such an impact would be significant, as assessed in light of the covered entity's business activities, risk appetite, and risk tolerance limits, the Commission believes heightened due diligence for potential critical third-party service providers and ongoing monitoring for onboarded critical third-party service providers are warranted to both mitigate the potential for such an occurrence and to promote the ability for covered entities to take early and effective action if a critical third-party service provider's performance is disrupted to mitigate the impact and effectively recover.[169]

3. Third-Party Service Provider Inventory—Proposed Paragraph (e)(3)

To help ensure that covered entities implement a comprehensive and consistent approach to identifying their critical third-party service providers, covered entities would be required to create, maintain, and regularly update an inventory of third-party service providers they have engaged to support their activities as a covered entity, identifying whether each third-party service provider in the inventory is a critical third-party service provider.[170] The Commission preliminarily believes that the process of creating an inventory of service providers, particularly the deliberative process involved in designating certain providers as critical third-party service providers, would help covered entities assess and evaluate the risks they face from their third-party service providers, and determine when to apply heightened monitoring. Maintaining such an inventory would also reflect that not all third-party service providers present the same level and types of risks to a covered entity, and would help covered entities assess and evaluate who is providing services and the attendant risk that any disruption of those services would have on a covered entity's business. The inventory would also provide covered entities a holistic view of their third-party service providers, which would help them better understand how risks identified during due diligence and ongoing monitoring may interact or require additional management. Having a clear understanding of who is providing services, particularly those services identified as critical, would further assist covered entities in identifying potential interconnections that may not be readily apparent if the entities are not assembled and reviewed collectively.[171]

Covered entities relying on a consolidated third-party relationship program would be able to rely on an enterprise-wide third-party service provider inventory provided that the inventory meets the requirements of the proposed rule, including identifying critical third-party service providers specific to the covered entity.[172]

4. Retention of Responsibility—Proposed Paragraph (e)(3)

For the avoidance of doubt, the proposed rule would make clear that, notwithstanding their determination to rely on a third-party service provider, covered entities remain responsible for meeting their obligations under the CEA and Commission regulations.[173] This provision reflects the principle, widely recognized among financial regulatory authorities, including the Commission, that while financial institutions may be able to delegate functions to third-party service providers, they cannot delegate their responsibility to comply with applicable laws and regulations.[174] This provision is intended to ensure that covered entities are aware that they remain responsible for the performance of all applicable regulatory functions, whether performed by the covered entity or by a third-party service provider, and are accordingly fully subject to the Commission's jurisdiction, including its examination and enforcement authorities.

5. Application to Existing Third-Party Relationships

Should the proposed rule be adopted as final, the Commission would expect covered entities to apply their third-party relationship programs across all stages of the relationship lifecycle on a going-forward basis. Although the Commission would not require covered entities to renegotiate or terminate existing agreements, it would expect covered entities to conduct ongoing monitoring of existing third-party service providers consistent with the program and this regulation and, to the extent possible, to rely on its program with respect to termination. For any third-party service providers contemplated or onboarded after the effective date of the proposed rule, or for any contracts renegotiated or renewed after the effective date of the rule, however, the Commission would expect covered entities to apply the entirety of the third-party relationship program from pre-selection through termination.

[167] *See* paragraph (e)(2) of proposed Commission regulations 1.13 and 23.603.

[168] *See* paragraph (a) of proposed Commission regulations 1.13 and 23.603 (defining ''critical third-party service provider'').

[169] *See* NFA Third-Party Notice, *supra* note 43 (''Additionally, a Member's onboarding due diligence process should be heightened for Third-Party Service Providers that obtain or have access to a Member's critical and/or confidential data and those that support a Member's critical regulatory-related systems (*e.g.,* handling customer segregated funds, keeping required records, filing financial reports, etc.).'').

[170] *See* paragraph (e)(3) of proposed Commission regulations 1.13 and 23.603.

[171] Prudential Third-Party Guidance, 88 FR 37927 (''Maintaining a complete inventory of its third-party relationships and periodically conducting risk assessments for each third-party relationship supports a banking organization's determination of whether risks have changed over time and to update risk management practices accordingly.'').

[172] *See* paragraph (c)(4)(i) of proposed Commission regulations 1.13 and 23.603 (allowing covered entities to rely on consolidated programs).

[173] *See* paragraph (e)(3) of proposed Commission regulations 1.13 and 23.603.

[174] *See* NFA Third-Party Notice, *supra* note 43 (''If a Member outsources a regulatory function, however, it remains responsible for complying with NFA and/or CFTC Requirements and may be subject to discipline if a Third-Party Service Provider's performance causes the Member to fail to comply with those Requirements.''); Prudential Third-Party Guidance, 88 FR 37927 (''A banking organization's use of third parties does not diminish its responsibility to meet these requirements to the same extent as if its activities were performed by the banking organization in-house.''); IOSCO Outsourcing Report, *supra* note 65, at 12 (''The regulated entity retains full responsibility, legal liability, and accountability to the regulator for all tasks that it may outsource to a service provider to the same extent as if the service were provided in-house.''). *See also* 17 CFR 37.204 (SEFs); 17 CFR 38.154 (DCMs); 17 CFR 39.18(d) (DCOs) (providing that such registered entities retain responsibility for meeting relevant regulatory requirements when entering into contractual outsourcing arrangements).

6. Guidance on Third-Party Relationship Programs—Proposed Paragraph (e)(4); Appendix A to Part 1; Appendix A to Subpart J of Part 23

To assist covered entities in developing third-party relationship programs that adequately address risks from third-party relationships, the Commission is proposing guidance outlining potential risks, considerations, and strategies for covered entities to consider.[175] The proposed guidance addresses all five stages of the relationship lifecycle and, if adopted, would be codified as appendices to parts 1 and 23 of the Commission's regulations for FCMs and swap entities, respectively.[176] Designed to be broadly applicable to all covered entities, the proposed guidance identifies actions and factors for covered entities to consider. The factors and actions identified are not exhaustive, nor should they be viewed as a required checklist. The nonbinding guidance would merely be intended to aid covered entities as they design third-party relationship programs tailored to their own unique circumstances, consistent with the general ORF ''appropriate and proportionate standard'' discussed above.

In developing the proposed guidance, the Commission considered the recommendations of international standard-setting bodies, including IOSCO and FSB, in light of observations and lessons derived from its own oversight activities.[177] In an effort to incorporate as much consensus as possible, the Commission also gave special consideration to existing guidance from NFA and the guidance on third-party relationships recently adopted by prudential regulators, both of which currently apply to at least some covered entities.[178]

The full text of the guidance is included at the end of this notice as proposed appendix A to part 1 for FCMs and proposed appendix A to subpart J of part 23. The guidance is identical in substance for FCMs and swap entities.

7. Request for Comment

The Commission invites comment on all aspects of the proposed third-party relationship program requirement and associated guidance, including the following questions:

1. *Scope of Application.* NFA's interpretive notice on third-party relationships is limited in scope to ''outsourcing,'' which NFA defines as third-party relationships in which an NFA member has a third-party service provider or vendor perform certain functions that would otherwise by undertaken by the member itself to comply with NFA and CFTC requirements.[179] The proposed rule would follow the approach taken by prudential regulators in their third-party guidance, which more broadly addresses any circumstances where banking organizations rely on third parties for products, services, or activities to ''capture[ ] the full range of third-party relationships that may pose risk to banking organizations.'' [180] Should the Commission consider limiting the scope of its guidance to outsourcing of CFTC regulatory obligations? Why or why not? Please explain.

2. *Critical third-party service provider.* The proposed rule includes a definition of ''critical third-party service provider.'' The Commission understands it is common practice for financial institutions to identify and apply heightened oversight of third-party service providers they deem critical. NFA's interpretive notice related to third-party relationships, for instance, advises members to tailor the frequency and scope of ongoing monitoring reviews to the criticality of and risk associated with the outsourced function but does not define ''criticality'' for covered entities. Is the Commission's proposed definition consistent with existing standards or definitions of ''criticality'' applied by covered entities? If not, how is it different? Should the Commission consider allowing covered entities to generate and apply their own definition of ''critical third-party service provider''? Why or why not? Please explain.

3. *Guidance—Affiliated Third-Party Service Providers.* The proposed third-party relationship program requirement would apply to all third-party relationships, including where the third-party is an affiliate of the covered entity. This position is consistent with both NFA and prudential guidance related to third-party relationships.[181] Nevertheless, the Commission recognizes that arrangements with affiliates may present different or lower risks than with unaffiliated third parties. Should the Commission consider including any additional guidance with respect to the management of third-party service providers that are affiliated entities? If so, what factors should covered entities consider when evaluating relationships with affiliated third-party service providers?

4. *Guidance—Due Diligence.* The proposed guidance recommends that covered entities perform due diligence on prospective third-party service providers to assess their ability to deliver contracted services to an acceptable standard (*i.e.,* consistent with risk appetite and risk tolerance limits) and provides examples of information that covered entities should review and sources for obtaining that information.

a. Are there any additional due diligence tasks that should be conducted by the covered entity beyond reviewing information about the potential third-party service provider? Are there additional risks that should be included in the guidance for the covered entity to inquire into? If yes, please identify and explain.

b. Are there additional sources of due diligence information beyond those listed in the guidance (see section B of the guidance) that should be included in the guidance? If yes, please identify and explain.

c. Should covered entities be advised to periodically refresh their due diligence, or upon the occurrence of specific triggers (*e.g.,* a material change to the service outsourced)? Why or why not? Would such a recommendation be duplicative of the covered entity's ongoing monitoring activities, or would the subsequent due diligence provide additional valuable information to the covered entity beyond that provided by ongoing monitoring? Why or why not? Please explain.

d. The proposed guidance does not recommend that covered entities perform due diligence directly on any subcontractors secured by third-party service providers. Rather, the Commission's guidance suggests that covered entities review the operational risk management practices of the potential third-party service provider with respect to their subcontractors. Should the Commission recommend more enhanced due diligence of subcontractors? Why or why not? What

[175] *See* paragraph (e)(4) of proposed Commission regulations 1.13 and 23.603.

[176] *See* proposed Appendix A to part 1 and proposed Appendix A to Subpart J of part 23.

[177] *See* IOSCO Outsourcing Report, *supra* note 65; FSB Third-Party Report, *supra* note 44.

[178] *See* NFA Third-Party Notice; Prudential Third-Party Guidance, 88 FR 37920.

[179] *See* NFA Third-Party Notice, *supra* note 43.

[180] *See* Prudential Third-Party Guidance, 88 FR 37921–22.

[181] *See* NFA Third-Party Notice at n.1 (''Further, even if a Member outsources a regulatory obligation to an affiliate, . . . a Member should comply with this Notice's requirements.''); Prudential Third-Party Guidance, 88 FR 37927 (''Third-party relationships can include, but are not limited to, . . . services provided by affiliates and subsidiaries. . .'').

means are practicable for covered entities to conduct due diligence on subcontractors to their third-party service providers? Please identify and explain.

E. Business Continuity and Disaster Recovery Plan—Proposed Paragraph (f)

The third component of the ORF would be a business continuity and disaster recovery (BCDR) plan, defined as a written plan outlining the procedures to be followed in the event of an emergency or other significant disruption to the continuity of a covered entity's normal business operations and that meets the requirements of the proposed rule.[182] Similar to the incident response plan (and, in extreme cases, possibly triggered by an incident covered by the incident response plan), the proposed BCDR plan requirement recognizes the operational reality that not all operational disruptions can be prevented or immediately mitigated and asks covered entities to strategize and implement plans for how to minimize the impact to operations, customers, and counterparties when such adverse events occur.

Although NFA requires FCMs to establish and maintain a BCDR plan, if adopted, the proposed rule would create a new CFTC BCDR plan requirement for FCMs.[183] Current Commission regulation 23.603 contains an active BCDR plan requirement for swap entities.[184] In essence, the proposal would make certain amendments to the CFTC BCDR plan requirement for swap entities and expand the requirement to include FCMs. The proposed amendments to the swap entity BCDR plan requirement have two general purposes. For the most part, the proposal would streamline and simplify some of the language to help it further conform to the proposed ORF rule more broadly, in ways the Commission intends to be non-substantive. The proposal would also make a few substantive changes, informed either by the Commission's review of NFA's and CME's current BCDR requirements for their members or by its decade of experience applying current Commission regulation 23.603 to swap entities.[185] The proposed substantive changes, each subsequently discussed in this notice, relate to either the defined scope of and recovery objective for the BCDR plan or the testing and audit requirements for the plan.

Current Commission regulation 23.603 includes requirements that the proposed rule would apply to the entirety of the proposed ORF more broadly. Those requirements include requirements to: distribute the BCDR plan to relevant employees (current Commission regulation 23.603(c)); notify the Commission of emergencies or disruptions (current Commission regulation 23.603(d)); identify emergency contacts (current Commission regulation 23.603(e)); review, test, and update the BCDR plan (current Commission regulation 23.603(f) and (g)); and recordkeeping (current Commission regulation 23.603(i)). Each of these requirements is discussed in the relevant sections of this notice that follow.[186] Accordingly, the Commission's proposed amendment to the current BCDR audit requirement is discussed in the context of the ORF's broader proposed review and testing requirements.[187]

1. Definition of ''Business Continuity and Disaster Recovery Plan''

The proposed definition of ''business continuity and disaster recovery plan'' is slightly modified from the language in the current BCDR plan requirement for swap entities. Current Commission regulation 23.603 requires swap entities to establish and maintain a BCDR plan that ''outlines the procedures to be followed in the event of an emergency or other disruption of its normal business activities.'' [188] As stated above, the proposed rule would specify that the BCDR plan would need to address ''significant'' disruptions to the continuity of a covered entity's normal business operations, which the Commission preliminarily believes is more in line with what would constitute an ''emergency'' that would result in activation of a BCDR plan and how Commission regulation 23.603 has operated in practice.[189]

2. Purpose—Proposed Paragraph (f)(1)

Under the proposed rule, the BCDR plan would need to be reasonably designed to enable covered entities to: (i) continue or resume normal business operations with minimal disruption to customers or counterparties and the markets and (ii) recover and make use of all covered information, as well as any other data, information, or documentation required to be maintained by law and regulation.[190] The Commission preliminarily believes that this standard, which emphasizes the need to quickly resume regulated activities and to recover all information kept and required to be kept in connection with those activities, supports the overall regulatory objectives of the ORF rule of enhancing the operational resilience of covered entities to promote the protection of customers and the mitigation of system risk.

Current Commission regulation 23.603 requires swap entities' BCDR plans to ''be designed to enable the [swap entity] to continue or to resume any operations by the next business day with minimal disturbance to its counterparties and the market.'' The proposed rule would modify this language by requiring that the BCDR plan be ''reasonably'' designed to continue or resume operations with minimal disruption and by removing the requirement that such operations be resumed ''by the next business day.'' [191] The Commission views the qualification that the BCDR plan be ''reasonably'' designed as simply a more concrete expression of the Commission's current expectations, in recognition that what might be necessary to achieve recovery is not an absolute fact and may vary depending on the circumstances, including the nature, size, scope, complexity, and risk profile of a covered entity's business activities.[192] The

[182] *See* paragraph (f) proposed Commission regulations 1.13 and 23.603. *See* also paragraph (a) of proposed Commission regulations 1.13 and 23.603 (defining ''business continuity and disaster recovery plan'').

[183] *See* NFA Rule 2–38, *supra* note 43.

[184] *See* 17 CFR 23.603.

[185] *See* NFA Rule 2–38; CME Rule 983 (Disaster Recovery and Business Continuity).

[186] *See* sections II.F (Training), G (Review and Testing), H (Required Notifications), and I (Emergency Contacts, Recordkeeping) of this notice, *infra.* The proposed rule would not retain Commission regulation 23.603(h), which merely articulates the fact that swap entities are required to comply with Commission's BCDR requirements in addition to any other applicable BCDR requirements from other regulatory bodies. *See* 17 CFR 23.603(h). The Commission accordingly views this amendment as non-substantive.

[187] *See* paragraph (h) of proposed Commission regulations 1.13 and 23.603 and section II.G, *infra.*

[188] *See* 17 CFR 23.603(a).

[189] *See also* NFA Rule 2–38, *supra* note 43 (requiring certain members, including FCMs, to establish a BCDR plan to be followed in the event of a ''significant business disruption''). The proposed language change from ''normal business activities'' to ''the continuity of normal business operations'' is intended only to bring the language more in line with the focus of the proposed ORF rule on the resiliency of operations and is not intended to have substantive effect. *See* paragraph (a) of proposed Commission regulations 1.13 and 23.603 (defining ''business continuity and disaster recovery plan''); 17 CFR 23.603(a).

[190] *See* paragraphs (f)(1)(i)–(ii) of proposed Commission regulations 1.13 and 23.603. *See also* 17 CFR 23.603(a).

[191] The Commission views the use of the phrase ''minimal disturbance'' in current Commission regulation 23.603 as equivalent to the phrase ''minimal disruption'' in the proposed rule and therefore views this change in language with respect to swap entities to be non-substantive. *Compare* 17 CFR 23.603(a) *with* paragraph (f)(1) of proposed Commission regulations 1.13 and 23.603.

[192] *See also* NFA Rule 2–38 (requiring BCDR plans be ''*reasonably* designed'') (emphasis added).

reasonableness of the plan would thus be viewed in light of the proposed (b)(3) standard (*i.e.,* what is appropriate and proportional to the covered entity, following generally accepted standards and best practices).

The proposal not to include a next business day recovery time objective is based in the Commission's preliminary view that, depending on the circumstances, a next business day recovery standard could be either too short or too long, to the point where it may be misdirecting the focus of the rule. The Commission understands that the ''next business day'' standard has been common for businesses to employ for BCDR purposes in the context of purely physical disasters, such as power outages or natural disasters. Based on its experience in recent years, however, the Commission believes a next-day standard may in some cases be impractical in an era where rapid innovation has deepened and expanded reliance on technology among financial institutions, and pandemics and cyberattacks have become more prevalent or alarming forms of disruption. With the ION incident, for instance, it took weeks before back office operations were back to normal. Nevertheless, the impact to customers and the markets during that time was manageable. Were even one business day to stretch between FCMs paying and collecting margin, for example, the Commission does not believe the impact to customers or the markets could be characterized as minimal.

Accordingly, the Commission preliminarily believes that by not including a precise recovery time objective, such as next business day, the emphasis of the proposed BCDR plan standard appropriately lies on ensuring that any disruption to customers, counterparties, and the markets is ''minimal.'' [193] For that standard to be met, however, the Commission would still expect covered entities to plan for a recovery that is expeditious. The longer a covered entity is not operating as usual, the more likely it is that customers and counterparties may be affected and that a crisis in confidence could develop, potentially affecting the industry more broadly.

Current Commission regulation 23.603 requires swap entities' BCDR plans to be designed ''to recover all documentation and data required to be maintained by applicable law and regulation.'' The proposal to require covered entities to reasonably design their BCDR plans to ''recover and *make use of* all *covered information,* as well as any other data, information, or documentation required to be maintained by law and regulation'' is intended to both incorporate the proposed defined term ''covered information,'' and make clear the need to also preserve the availability of the recovered data and information (*i.e.,* reliable access to and use of information), which the Commission believes is an integral component of information and technology security.[194] The Commission believes that making plans to ensure covered information—sensitive or confidential information and data the proposed ORF rule is designed, at its core, to ensure covered entities protect—as well as any other information covered entities are legally required to maintain, is recovered and accessible following an emergency is key to ensuring the protection of customers and counterparties and the ongoing orderly functioning of the commodity interest markets, as this information is vital to a covered entity's ability to assess its ongoing compliance with the Commission's regulations governing the requirements for covered entities.[195]

3. Minimum Contents—Proposed Paragraph (f)(2)

Consistent with the proposed (b)(3) standard for the ORF as a whole, the BCDR plan would need to be appropriate and proportionate to the covered entity, following generally accepted standards and best practices.[196] Accordingly, should the proposal be adopted as final, the Commission would expect each BCDR plan to be highly tailored to each specific covered entity. However, the proposed rule would also require the BCDR plan to include certain minimum contents, which are generally comparable to the current requirements in Commission regulation 23.603.[197]

First, the proposed rule would require the BCDR plan to identify its covered information, as well as any other data or information required to be maintained by law or regulation, and to establish and implement procedures to backup or copy it with sufficient frequency and to store it offsite in either hard-copy or electronic format.[198] The BCDR plan would also need to identify any resources, including covered technology, facilities, infrastructure, personnel, and competencies, essential to the operations of the swap entity or to fulfill the regulatory obligations of the swap entity, and establish and maintain procedures and arrangements to provide for their backup in a manner that is sufficient to meet the requirements of the rule (*i.e.,* to continue or resume operations with minimal disruption, to recover and make use of information).[199] These minimum requirements are intended to ensure that the BCDR plan meets the proposed recovery standard by ensuring covered entities have gone through the process of cataloging everything they need (information, technology, infrastructure, human capital, *etc.*) to operate as a covered entity, and have established ways to recover them and to continue or resume operations with minimal disruption to customers, counterparties, or the markets. Furthermore, in establishing arrangements for backup resources, the Commission would want covered entities to consider diversification to the greatest extent possible to reduce the likelihood that an emergency that affects a primary operating resource affects any planned backups. Accordingly, the proposed rule would require covered entities to establish backup arrangements for resources that are in one or more areas geographically separate from the covered entity's primary resources (*e.g.,* a different power grid than the primary facility).[200] The proposed rule would make clear those resources could be

[193] The Commission notes that neither NFA nor CME includes a specific recovery time objective in its BCDR plan requirements. *See* NFA Rule 2–38; CME Rule 938.

[194] *See supra* note 108 and accompanying text (discussing the ''CIA triad'' of confidentiality, integrity, and availability).

[195] In designing a BCDR plan that would meet this recovery standard, the Commission would advise covered entities to identify a broad range of events that could constitute emergencies or pose significant disruptions, including natural events (*e.g.,* hurricanes, wildfires), technical events (*e.g.,* power failures, system failures), malicious activity (*e.g.,* fraud, cyberattacks), failures of controls, and low likelihood but high impact events (*e.g.,* terrorist attacks, pandemics), and consider potential impact on business operations and data and information.

[196] *See* paragraph (b)(3) of proposed Commission regulations 1.13 and 23.603.

[197] *See* paragraph (f)(2) of proposed Commission regulations 1.13 and 23.603. *See also* 17 CFR 23.603(b). Although the exact language of the proposed minimum contents in paragraph (f)(2) may diverge somewhat from that of current Commission regulation 23.603(b), the modifications were intended to streamline language and incorporate the proposed terms ''covered information'' and ''covered technology.'' The Commission does not intend any of the changes to have a substantive impact on compliance with the Commission's BCDR plan requirement for swap entities.

[198] *See* paragraph (f)(2)(i) of proposed Commission regulations 1.13 and 23.603. *See also* 17 CFR 23.603(b)(1), (b)(6).

[199] *See* paragraph (f)(2)(ii) of proposed Commission regulations 1.13 and 23.603. *See also* 17 CFR 23.603(b)(2), (b)(4), (b)(5).

[200] *See* paragraph (f)(2)(ii) of proposed Commission regulations 1.13 and 23.603. *See also* 17 CFR 23.603(b)(5).

provided by third-party service providers.[201]

To ensure that critical third-party service providers are given particular consideration when planning for disruptions, the proposed rule would specifically require the BCDR plan to identify potential disruptions to critical third-party service providers and establish a plan to minimize the impact of such potential disruptions.[202] Additionally, given the importance of internal and external communication in times of crisis, and for duties and responsibilities to be well established, the proposed rule would require the BCDR plan to identify supervisory personnel responsible for implementing the BCDR plan, along with the covered entity's required ORF emergency contacts, and establish a procedure for communicating with relevant persons in the event of an emergency or significant disruption.[203]

The minimum contents of the proposed BCDR plan requirement were designed to align with the substance of the ''essential components'' of a BCDR plan identified in current Commission regulation 23.603(b), with certain modifications.[204] The changes are intended to streamline language, incorporate the proposed BCDR plan standard and defined terms (*e.g.,* covered information, covered technology, critical third-party service provider), and reorder and combine elements to improve readability and application. Key changes include:

- Replacing the identification or backup of documents and information essential to the continued operations of the swap entity and/or to fulfill the regulatory obligations of the swap dealer or major swap participant with covered information, as well as any other data or information required to be maintained by law and regulation.[205] This change is intended to align the information required to be identified in the proposed BCDR plan with its purpose (recover and make use of all covered information, as well as any other data, information, or documentation required to be maintained by law and regulation).
- Specifying that data and information must be backed up or copied with sufficient frequency ''to meet the requirements of this section,'' to make clear that the backup frequency should be linked to the broader purpose of the BCDR plan (*i.e.,* to continue or resume operations with minimal disruption and to recover and make use of in-scope information).[206]
- Removing the qualification that resource backups be designed to achieve the timely recovery of data and documentation and to resume operations as soon as reasonably possible and generally within the next business day.[207] This language could be viewed as in contradiction with the overall proposed purpose of the BCDR plan, which would not include a ''next business day'' recovery time objective.
- Replacing third parties that are necessary to the continued operations of the swap dealer or major swap participant with critical third-party service provider, as defined in the proposed rule, as the Commission believes these terms are intended to capture similar concepts.[208]

4. Accessibility—Proposed Paragraph (f)(3)

Finally, to ensure that the BCDR plan is available in the event of an emergency or other significant disruption that prevents a covered entity from accessing its primary office location, the proposed rule would require each covered entity to maintain copies of its BCDR plan at one or more accessible off-site locations.[209]

5. Request for Comment

The Commission invites comment on all aspects of the proposed business continuity and disaster recovery plan requirement, including the following question:

1. *Recovery time objective.* Under current Commission regulation 23.603, the Commission requires swap entities to establish and maintain a BCDR plan that is designed to enable the swap entity to continue or resume any operations ''by the next business day'' with minimal disturbance to is counterparties.[210] Noting that such a standard may pose some challenges, the Commission has proposed to not include a recovery time objective, relying on covered entities to establish a BCDR plan that allows for sufficiently exigent recovery so as to impose ''minimal disruption'' to customers, counterparties, or the markets.

a. Has a next business day standard posed challenges for swap entities to implement? Would such a standard be achievable for FCMs? Why or why not? Please explain.

b. Should the Commission consider including additional language to ensure covered entities design BCDR plans that enable quick recovery (*e.g.,* ''as soon as possible'' or ''as soon as practicable'')? Why or why not? Please explain.

2. *Transfer of business to another entity.* NFA and CME rules allow for BCDR plans to include the possibility of transferring their business to another regulated entity in the event of an emergency or disruption. NFA Rule 2–38 provides that a BCDR plan ''shall be reasonably designed to . . . transfer its business to another Member with minimal disruption to its customers, other members, and the commodity futures markets.'' [211] CME Rule 983 provides that clearing members must have procedures in place to allow them to continue to operate during periods of stress ''or to transfer accounts to another fully operational clearing member with minimal disruption to either [CME] or their customers.'' [212] Do any covered entities currently have arrangements with other covered entities to transfer business or accounts in the event of an emergency or disruption? Should the Commission consider adding the option to transfer business to another regulated entity into its proposed BCDR rule? Why or why not? How would such a transfer function in practice? Please explain.

F. Training and Plan Distribution—Proposed Paragraph (g)

To support the effectiveness of the ORF by ensuring personnel are aware of relevant policies, procedures, and

[201] *See id.*

[202] *See* paragraph (f)(2)(iii) of proposed Commission regulations 1.13 and 23.603. *See also* 17 CFR 23.603(b)(7) (identify ''potential business interruptions encountered by third parties that are necessary to the continued operations of the swap dealer or major swap participant and a plan to minimize the impact of such disruptions'').

[203] *See* paragraphs (f)(2)(iv)–(v) of proposed Commission regulations 1.13 and 23.603. *See also* paragraph (k) of proposed Commission regulations 1.13 and 23.603 (requiring emergency contacts), discussed in section II.I.1 of this notice, *infra;* 17 CFR 23.603(b)(3).

[204] *See* 17 CFR 23.603(b).

[205] *See* proposed paragraph (f)(2)(i) of Commission regulations 1.13 and 23.603; 17 CFR 23.603(b)(1) (Identification of the documents and data essential to the continued operations of the swap entity and to fulfill the obligations of the swap entity); (b)(6) (Back-up or copying of documents and data essential to the operations of the swap entity or to fulfill the regulatory obligations of the swap entity'').

[206] *Cf.* 17 CFR 23.603(b)(6) (Back-up or copying, with sufficient frequency, of documents and data).

[207] *See* 17 CFR 23.603(b)(4) (Procedures for, and the maintenance of, back-up facilities, systems, infrastructure, alternative staffing and other resources to achieve the timely recovery of data and documentation and to resume operations as soon as reasonably possible and generally within the next business day.).

[208] *See* 17 CFR 23.603(b)(7) (Identification of potential business interruptions encountered by third parties that are necessary to the continued operations of the swap dealer or major swap participant and a plan to minimize the impact of such disruptions.).

[209] *See* paragraph (e)(3) of proposed Commission regulations 1.13 and 23.603. *See also* 17 CFR 23.603(c).

[210] *See* 17 CFR 23.603(a).

[211] *See* NFA Rule 2–38, *supra* note 43.

[212] *See* CME Rule 983, *supra* note 185.

practices, the proposed rule would require that each covered entity establish, implement, and maintain training with respect to all aspects of the ORF.[213] Relevant training is important to ensuring the ORF operates as intended, and to supporting a firm culture that promotes and prioritizes operational resilience.[214] The training would therefore need to include, at a minimum, (i) cybersecurity awareness training for all personnel and (ii) role-specific training for personnel involved in establishing, documenting, implementing, and maintaining the ORF.[215] The importance of cybersecurity training is widely recognized, as incidents commonly occur because well-intentioned employees or other users make preventable mistakes.[216] The Commission would further expect that role-specific training would include not only training on relevant policies and procedures but additional relevant threat and vulnerability response training for personnel involved in the development and maintenance of the information and technology security program (*e.g.,* system administration courses for IT professionals, secure coding training for web developers).[217]

As with all aspects of the ORF, if the proposal is adopted as final, the Commission would expect each covered entity's ORF training to meet the (b)(3) standard (*i.e.,* be appropriate and proportionate to the nature, scope, and complexities of its business activities as a covered entity, following generally accepted standards and best practices).[218] To ensure the training remains relevant overtime and that personnel are adequately informed with respect to the ORF, covered entities would also be required to provide and update their ORF training as necessary, but no less frequently than annually.[219] Requiring that the training occur annually would be a new CFTC requirement with respect to the BCDR plan training requirement for swap entities.[220] The Commission nevertheless believes an annual training requirement is necessary for staff involved in BCDR planning to ensure they remain up-to-date on changes to the BCDR plan following the annual reviews and testing of the plan.[221]

To further support the proposed training requirement and ensure relevant personnel have access to and are aware of the current information and technology security, third-party relationships, and BCDR plans that form the ORF, the proposed rule would require that covered entities distribute copies of those plans to relevant personnel and promptly provide any significant revisions thereto.[222] This proposed plan distribution requirement is consistent with the current BCDR plan distribution requirement for swap entities in current Commission regulation 23.603.[223]

Request for Comment

The Commission invites comment on all aspects of the proposed training requirement.

G. Reviews and Testing—Proposed Paragraph (h)

To ensure the ORF remains viable and effective over time, the proposed rule would require covered entities to establish, implement, and maintain a plan reasonably designed to assess its adherence to, and the effectiveness of, the ORF through regular reviews and risk-based testing.[224] As discussed above, the purpose of the proposed ORF would be to identify, monitor, manage, assess, and report on risks relating to information and technology security, third-party relationships, and emergencies or other significant business disruptions.[225] Monitoring and managing these risks is a dynamic, ever-evolving process, especially given the increased reliance on and rapid evolution of technological advancements and related cyber risks.[226] The Commission believes regular reviews and testing are an important tool needed to confirm that systems and information remain protected, controls are working as expected, and policies and procedures are being followed.[227] Accordingly, the Commission preliminarily believes that regular reviews and testing would provide covered entities with essential information about the actual quality, performance, and reliability of the ORF in relation to its objectives and regulatory requirements. The Commission further expects that reviews and testing would be key to revealing unknown gaps or weaknesses in systems or controls that could then be analyzed to identify corrective actions designed to improve overall operational resilience over time.[228] The results of the reviews and testing should be used to support sound decision-making at the covered entity regarding prioritization and funding of resources in a manner

[213] *See* paragraph (g) of proposed Commission regulations 1.13 and 23.603.

[214] *See* FFIEC Information Security Booklet, *supra* note 69, at 17 (''Training ensures personnel have the necessary knowledge and skills to perform their job functions.''); CIS Critical Security Controls v.8., Control no. 14 (Security Awareness and Skills Training) at 43 (May 2021) (CIS Control 14) (training helps ''influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise'').

[215] *See* paragraphs (g)(1)(i)–(ii) of proposed Commission regulations 1.13 and 23.603. Proposed paragraph (g)(1)(ii) would supplant the current requirement in Commission regulation 23.603 for swap entities to train relevant employees on applicable components of the BCDR plan. *See* 17 CFR 23.603(c). The Commission does not intend any substantive difference in the BCDR plan training for swap entities.

[216] The FSB found that most successful cyberattacks involved human error, which is why training is important for all personnel. *See* FSB, *Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices* at 7 (Oct. 13, 2017), *available at https://www.fsb.org/wp-content/uploads/P131017-1.pdf. See also* CIS Control 14 (''Users themselves, both intentionally and unintentionally, can cause incidents as a result of mishandling sensitive data, sending an email with sensitive data to the wrong recipient, losing a portable end-user device, using weak passwords, or using the same password they use on public site . . .); Prudential Operational Resilience Paper, *supra* note 11, at 11 (''The firm provides cybersecurity awareness education especially to personnel engaged in the operations of critical operations and core business lines, . . . and adequately trains them to perform their information security-related duties and responsibilities consistent with related processes and agreements.'').

[217] *See* CISA, Incident Response Plan (IRP) Basics (advising that all staff need to understand their role in maintaining and improving the security of the organization), *available at https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf.*

[218] *See* paragraph (b)(3) of proposed Commission regulations 1.13 and 23.603; *supra* note 63 and accompanying text.

[219] *See* paragraph (g)(2) of proposed Commission regulations 1.13 and 23.603.

[220] *See* 17 CFR 23.603(c).

[221] *See* paragraph (h) of proposed Commission regulations 1.13 and 23.603, discussed in section II.G, *infra.*

[222] *See* paragraph (g)(3) of proposed Commission regulations 1.13 and 23.603.

[223] *See* 17 CFR 23.603(c) (Each swap entity shall distribute a copy of its business continuity and disaster recovery plan to relevant employees and promptly provide any significant revision thereto.).

[224] *See* paragraph (h) of proposed Commission regulations 1.13 and 23.603.

[225] *See* paragraph (b)(1) of proposed Commission regulations 1.13 and 23.603, *supra* note 55 and accompanying text.

[226] *See* Prudential Operational Resilience Paper, *supra* note 11, at 9 (''The firm also regularly reviews and updates its systems and controls for security against evolving threats including cyber threats and emerging or new technologies.'').

[227] *See, e.g.,* 17 CFR 37.1401 (SEFs); 17 CFR 38.1051 (DCMs); 17 CFR 39.18 (DCOs); 17 CFR 49.24 (SDRs) (requiring system safeguard testing). *See also* FFIEC Information Security Booklet, *supra* note 69 (providing that entities should have a documented testing and evaluation plan).

[228] *See also* CPMI IOSCO Cyber Resilience Guidance, *supra* note 123, at 18 (''Sound testing regimes produce findings that are used to identify gaps in stated resilience objectives and provide credible and meaningful inputs to the [entity's] cyber risk management process. Analysis of testing results provides direction on how to correct weaknesses or deficiencies in the cyber resilience posture and reduce or eliminate identified gaps.'').

that furthers operational resilience.[229] Without such regular reviews and testing, the Commission is concerned that the ORF would quickly grow stale and ineffective, allowing unseen vulnerabilities to go unaddressed and potentially weaken the stability of the covered entity or the financial system at large.

1. Reviews—Proposed Paragraph (h)(1)

Under the proposed rule, reviews would need to include an analysis of the adherence to, and the effectiveness of, the ORF, as well as any recommendations for modifications or improvements that address root causes of issues identified by the review.[230] Again, the Commission believes that the process of reviewing the ORF to evaluate both its current effectiveness and make recommendations for prospective improvements that relate to deficiencies found through the review would help ensure that the ORF remains effective at managing operational resilience as circumstances change over time.

The proposed rule would require covered entities to conduct such reviews at least annually and in connection with any material change to the activities or operations of the covered entity that is reasonably likely to affect the risks addressed by the ORF.[231] An annual review standard is consistent with the Commission's existing review requirement for the RMP for covered entities, the BCDR plan for swap entities, and NFA's ISSP Interpretive Notice.[232] Although the Commission would expect the ORF to be reviewed at least annually in its entirety, including not only the required plans but training and governance, the reviews could be broken into phases, staged over the course of the year. The Commission preliminarily believes that requiring the ORF to be reviewed on at least an annual basis and in connection with any relevant, material business change is sufficiently frequent to help ensure that the ORF remains effective and continues to meet its objectives over time.

The proposed review requirement for the ORF would replace the similar annual review requirement for swap entities' BCDR plans contained in current Commission regulation 23.603. Current Commission regulation 23.603(f) requires that a member of senior management for a swap entity review the BCDR plan annually or upon any material change to the business and to document any deficiencies found or corrective action taken.[233] The Commission preliminarily believes that the proposed annual review of the ORF, which would encompass a review of the BCDR plan, is sufficient to ensure the ORF's effectiveness and that it would no longer be necessary for a separate review of the BCDR plan to be conducted by senior management.

2. Testing—Proposed Paragraph (h)(2)

With respect to risk-based testing of the ORF, the proposed rule would generally provide that covered entities determine the frequency, nature, and scope of the testing consistent with the proposed (b)(3) standard.[234] Covered entities have available to them a wide range of testing tools, techniques, and methodologies, particularly with respect to information and technology security. Those tools and techniques include open source analysis, network security assessments, physical security reviews, source code reviews, compatibility testing, performance testing, and end-to-end testing, just to name a few.[235] Such testing methods can vary significantly in terms of what they test and how, and in the degree of sophistication and sensitivity they need to run them correctly and reliably.[236] Covered technology among covered entities varies, both in terms of the sensitivity of the data and information it contains and transmits, as well as its operational importance and risk profile.

The Commission therefore preliminarily believes that leaving the specifics of the design and implementation of ORF testing to the reasonable judgment of each covered entity would help ensure that such testing protocols remain nimble as operations and recommended testing techniques change progressively over time.[237] Covered entities would, however, need to ensure that the testing is reasonably designed to test the effectiveness of the function or system being tested.[238] Covered entities should determine which particular tests to incorporate, consistent with the (b)(3) standard and their risk assessments, to ensure the testing effectively targets their particular business lines, activities, operations, and risk profile. Covered entities would accordingly be encouraged to document the decision-making regarding how it determined the nature, scope, and frequency of testing.

Although the proposed rule would generally not mandate the use of any specific techniques, it would establish certain minimum testing frequencies with respect to a few testing categories that have broad consensus. With respect to testing of the information and technology security program, the proposed rule would require testing of key controls and the incident response plan at least annually.[239] Consistent with the definition in the Commission's system safeguard rules for registered entities, the proposal would define ''key controls'' as those controls that an appropriate risk analysis determines are either critically important for effective information and technology security, or are intended to address risks that evolve or change more frequently and therefore require more frequent review to ensure their continuing effectiveness in addressing such risks.[240] Given their importance to preserving information and technology security and recovering from incidents, the Commission believes that regular testing of the incident response plan and key controls on at least an annual basis is an important baseline requirement to ensure the continued effectiveness of

[229] *See id.* at 18 (''The results of the testing programme should be used by the [entity] to support the ongoing improvement of its cyber resilience.'').

[230] *See* paragraph (h)(1) of proposed Commission regulations 1.13 and 23.603.

[231] *Id.*

[232] *See* 17 CFR 1.11(f)(1); 17 CFR 23.600(e)(1) (requiring covered entities to review their RMPs on an annual basis or upon any material change in the business reasonably likely to alter their risk profile); 17 CFR 23.603(f) (requiring an annual review of swap entities' BCDR plan); NFA ISSP Notice, *supra* note 43 (providing that members should perform a regular review of their information systems security program at least once every twelve months).

[233] *See* 17 CFR 23.603(f).

[234] *See* paragraph (h)(2) of proposed Commission regulations 1.13 and 23.603. *See also* paragraph (b)(3) of proposed Commission regulations 1.13 and 23.603; *supra* note 63 and accompanying text.

[235] *See* NIST, SP 800–115, Technical Guide to Information Security Testing and Assessment (Sept. 2008).

[236] *Id.*

[237] *See also* Interagency Guidelines Safeguarding Customer Information, 66 FR 8623 (''The Agencies believe that a variety of tests may be used to ensure the controls, systems, and procedures of the information security program work properly and also recognize that such tests will progressively change over time''); FINRA Cybersecurity Report, *supra* note 66, at 13 (''Many firms determined the systems to be tested and the frequency with which they should be tested based on a risk assessment where higher risk systems were tested more frequently.'').

[238] *See* paragraph (h) of proposed Commission regulations 1.13 and 23.603 (requiring that the testing plan be reasonably designed to assess the adherence to, and the effectiveness of, the ORF).

[239] *See* paragraph (h)(2)(i)(A) of proposed Commission regulations 1.13 and 23.603.

[240] *See* paragraph (a) of proposed Commission regulations 1.13 and 23.603 (defining ''key controls''). *See also* 17 CFR 37.1401(h)(1) (SEFs); 17 CFR 38.1051(h)(1) (DCMs); 17 CFR 39.18(a) (DCOs); 17 CFR 49.24(j)(1) (SDRs) (defining ''key controls'' for purposes of system safeguard requirements).

the information and technology security program.[241]

The proposed rule would also require that testing of the information and technology security program include vulnerability assessments and penetration testing.[242] Vulnerability assessments include methods and techniques to identify, diagnose, and prioritize vulnerabilities in the security of covered technology.[243] Technical vulnerabilities can be identified through scanner tools, which can be run continuously or periodically, often daily, and may include checking servers for security patches to ensure they are current.[244] Penetration testing (or ''pen testing''), meanwhile, attempts to identify ways to exploit vulnerabilities and circumvent or defeat security features, mimicking potential real-world attacks. Experts have developed a wide variety of penetration tests (*e.g.,* wireless, network, web application, cloud, client side, social engineering, physical, threat-led) and approaches to or modes of completing them (*e.g.,* black box, white box, gray box).[245] Some tests go further by using cyber-threat intelligence in designing these simulated attacks, a testing referred to as threat-led penetration testing or ''red teaming.'' [246]

With respect to vulnerability assessments, the proposed rule would require covered entities to test their information and technology security programs using vulnerability assessments, including daily or continuous automated vulnerability scans.[247] The Commission preliminarily believes that some degree of vulnerability assessment is considered standard cybersecurity hygiene in order to monitor systems and controls for vulnerabilities, and that the availability of automated vulnerability scanning tools help provide a base level of monitoring that is easily accessible to all covered entities.[248]

With respect to penetration testing, the proposed rule would not require covered entities to undertake specific types of testing. Given the diverse nature of entities registered as FCMs and swap entities, the Commission believes that determination of the type and method of penetration testing would be best left to the reasoned judgement of each covered entity after conducting its own assessment. The Commission would, however, require that covered entities conduct some penetration testing at least annually.[249] The Commission preliminarily believes that annual penetration testing of some type, determined consistent with the proposed (b)(3) standard, would be important for covered entities to have knowledge and awareness of the actual vulnerability of their covered technology to internal or external threats. According to FINRA's 2018 cyber risk report, firms with strong cybersecurity programs conducted penetration tests at least annually and more frequently for mission critical, high risk systems such as for an online trading system.[250] Covered entities would also be encouraged to consider additional risk-based penetration testing after key events, such as any time a significant change is made to important elements of the firm's applications and systems infrastructure, in addition to any other regular compliance testing.

Current Commission regulation 23.603 includes a testing requirement for the BCDR plan for swap entities.[251] The proposed ORF testing provision would replace that requirement in current Commission regulation 23.603 and specify that, as part of the testing, covered entities would need to conduct a walk-through or tabletop exercise designed to test the effectiveness of backup facilities and capabilities at least annually.[252] The Commission preliminarily believes that swap entities currently test their BCDR plans through such exercises and that they are an important way to test the effectiveness of a BCDR plan in practice. Unlike current Commission regulation 23.603, however, the proposed rule would not require that covered entities' BCDR plans be audited every three years by a qualified third-party service provider.[253] Based on the Commission's experience, this audit requirement has proven redundant and unnecessary in light of the requirements to review and test the plan annually.

3. Independence—Proposed Paragraph (h)(3)

To support the reliability and objectivity of the review and testing results, the proposed rule would require the reviews and testing to be conducted by qualified personnel who are independent of the aspect of the ORF being reviewed or tested.[254] The personnel conducting the testing could be employees of the covered entity itself, an affiliate, or of a third-party service provider, provided that such personnel are sufficiently trained and not responsible for the development, installation, operation, or maintenance of the ''object'' of the testing (*e.g.,* covered technology, key controls, training, *etc.*). For example, a covered entity's internal audit department may be sufficiently trained and independent to test certain key controls but may need to secure a third-party to test certain systems or program installations if it does not have sufficient capabilities in-house. Covered entities would therefore be permitted under the proposal to determine whether a particular test should be conducted in-house or by a third-party service provider, provided that the qualification and independence requirements are met.[255]

This proposed independence requirement is consistent with the testing requirement for swap entity

---

[241] *See* 17 CFR 37.1401(h)(5) (SEFs); 17 CFR 38.1051(h)(5) (DCMs); 17 CFR 39.18(e)(5) (DCOs); 17 CFR 49.24(j)(5) (SDRs) (annual testing of incident response plans and key controls); *see also* FFIEC, Information Technology Handbook, Audit Booklet at A–15 (Apr. 2012) (including testing of key controls at least annually as an examination point

[242] *See* paragraphs (h)(2)(i)(B)–(C) of proposed Commission regulations 1.13 and 23.603.

[243] *See* FFIEC Information Security Booklet, *supra* note 69, at 8.

[244] *Id.*

[245] *See* FINRA Cybersecurity Report, *supra* note 66, at 13.

[246] *See* FSI, FSI Insights on policy implementation No. 21, Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions (Nov. 2019).

[247] *See* paragraph (h)(2)(i)(B) of proposed Commission regulations 1.13 and 23.603. *See also* 17 CFR 37.1401(h)(2) (SEFs); 17 CFR 38.1051(h)(2) (DCMs); 17 CFR 39.18(e)(2) (DCOs); 17 CFR 49.24(j)(2) (SDRs) (requiring automated vulnerability scanning).

[248] For instance, CISA makes available a free vulnerability scanner. *See* CISA, Cyber Hygiene Services, *available at https://www.cisa.gov/cyber-hygiene-services.*

[249] *See* paragraph (h)(2)(i)(C) of proposed Commission regulations 1.13 and 23.603.

[250] FINRA Cybersecurity Report, *supra* note 66, at 13–14. FFIEC's exam book also appears to contemplate at least some degree of penetration testing among financial institutions. *See* FFIEC Information Security Booklet, *supra* note 69, at 55 (noting that independent testing, including penetration testing and vulnerability scanning, is conducted according to the risk assessment for external-facing systems and the internal network).

[251] *See* 17 CFR 23.603(g) (requiring the BCDR plan to tested annually by qualified, independent internal personnel or a qualified third-party service).

[252] Current Commission regulation 23.603 does not specify the nature of the BCDR testing, *see id.*

[253] *See id.* (''Each business continuity and disaster recovery plan shall be audited at least once every three years by a qualified third party service. The date the audit was performed shall be documented, together with the nature and scope of the audit, any deficiencies found, any corrective action taken, and the date that corrective action was taken.'').

[254] *See* paragraph (h)(3) of proposed Commission regulations 1.13 and 23.603.

[255] If a covered entity determines to use a third-party service provider, the proposed requirements and guidance with respect to the management of third-party relationships would apply. *See supra* note 153 and accompanying text.

BCDR plans in current Commission regulation 23.603.[256]

4. Documentation—Proposed Paragraph (h)(4)

The proposed rule would require covered entities to document all reviews and testing of the ORF. The documentation would need to include, at a minimum: (i) the date the review or testing was conducted; (ii) the nature and scope of the review or testing, including methodologies employed; (iii) the results of the review or testing, including any assessment of effectiveness; (iv) any identified deficiencies and recommendations for remediation; and (v) any corrective action(s) taken, including the date(s) such actions were taken.[257] The Commission primarily believes documenting these key aspects of the testing and related results would not only assist in ensuring accountability for the testing, but would help covered entities take full advantage of any insights the testing may provide and to build upon their resiliency from lessons learned. Such documentation would also assist the Commission in performing its oversight duties with respect to covered entities and their implementation of their ORF.

This proposed documentation requirement is consistent with the requirement for swap entity BCDR plans in current Commission regulation 23.603.[258]

5. Internal Reporting—Proposed Paragraph (h)(5)

To support covered entities' compliance with the ORF rule and ensure that senior leadership is apprised of and held accountable for the effectiveness of the ORF, the proposed rule would expressly require covered entities to report on the results of their reviews and testing to the CCO and any other relevant senior-level official(s) and oversight body(ies).[259] The proposed rule would not mandate the form, method, or frequency of such reporting, but the Commission would encourage the reporting to be provided in a sufficiently timely manner so as to allow the CCO and senior leadership to act upon the information to take steps to improve compliance and the overall effectiveness of the ORF.

This requirement does not exist with respect to the swap entity BCDR plan requirement in current Commission regulation 23.603 and would therefore be a new requirement.

6. Request for Comment

The Commission invites comment on all aspects of the proposed review and testing requirements, including the following question:

1. *Key Controls.* The proposed rule would require covered entities to test key controls on at least an annual basis and includes a definition of ''key controls'' that is comparable to how the term is defined for purposes of the Commission's system safeguard requirements for registered entities.[260] Are covered entities currently testing key controls? How are they determining what controls should be regularly tested? Should the Commission consider allowing covered entities to define ''key controls'' for themselves consistent with the proposed (b)(3) standard?

H. Required Notifications—Proposed Paragraphs (i) and (j)

The proposed rule would require covered entities to notify the Commission, customers, or counterparties of certain events within the scope of the ORF. Notifications to the Commission would relate to incidents that have an adverse impact, or a covered entity's decision to activate its BCDR plan.[261] Notifications to customers or counterparties would relate to incidents that adversely impact their interests.[262] These notification provisions are discussed in turn below.

1. Commission Notification of Incidents—Proposed Paragraph (i)(1)

The proposed rule would require covered entities 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 covered entity to continue its business activities as a covered entity, or (C) the assets or positions of a customer or counterparty.[263] The notification would need to include any information available to the covered entity at the time of the notification that could assist the Commission in assessing and responding to the incident, including the date the incident was detected, possible cause(s) of the incident, its apparent or likely impacts, and any actions the covered entity has taken or is taking to mitigate or recover from the incident, including measures to protect customers or counterparties.[264] Covered entities would need to provide the notification as soon as possible, but no later than 24 hours after such incident has been detected.[265]

The purpose of this proposed notification provision is multifold. At a fundamental level, the proposed rule would allow the Commission to exercise its oversight function with respect to the ORF, offering the Commission a real-world, real-time insight into the effectiveness of a particular covered entity's ORF and whether it is operating as intended. Early warning of impactful incidents would also enable the Commission to be more responsive, providing guidance or appropriate relief to help the covered entity withstand and recover from the incident. The Commission would also expect such early warnings to aid it in identifying and reacting to events that could pose a more 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 (*e.g.,* a ransomware attack against multiple covered entities or a third-party service provider engaged by more than one covered entity). In such potentially systemic circumstances, early awareness of the incident is expected to facilitate the Commission's role in coordinating industry efforts and information sharing, allowing it to help forestall the impact of potential broad-scale threats by sharing information with other regulators through its involvement in Financial and Banking Information Infrastructure Committee (FBIIC), issue timely statements to stabilize public confidence, and potentially take emergency regulatory action. Over time, the Commission preliminarily believes that the knowledge and experience gained from these incident reports could provide the Commission a vantage point from which to identify trends and lessons learned that could improve its supervisory guidance supporting industry efforts to

[256] *See* 17 CFR 23.603(g) (requiring the BCDR plan to tested annually by qualified, independent internal personnel or a qualified third-party service).

[257] *See* paragraph (h)(4)(i)–(v) of proposed Commission regulations 1.13 and 23.603.

[258] *See* 17 CFR 23.603(g) (''The date the testing was performed shall be documented, together with the nature and scope of the testing, any deficiencies found, any corrective action taken, and the date that corrective action was taken.'').

[259] *See* paragraph (h)(5) of proposed Commission regulations 1.13 and 23.603.

[260] *See, e.g.,* 17 CFR 37.1401(h)(1) (SEFs); 17 CFR 38.1051(h)(1) (DCMs); 17 CFR 39.18(a) (DCOs); 17 CFR 49.24(j)(1) (SDRs) (defining ''key controls'' for purposes of system safeguard requirements).

[261] *See* paragraph (i) of proposed Commission regulations 1.13 and 23.603.

[262] *See* paragraph (j) of proposed Commission regulations 1.13 and 23.603.

[263] *See* paragraph (i)(1)(A)–(C) of proposed Commission regulations 1.13 and 23.603.

[264] *See* paragraph (i)(1)(ii) of proposed Commission regulations 1.13 and 23.603.

[265] *See* paragraph (i)(1)(iii) of proposed Commission regulations 1.13 and 23.603.

enhance their ORF practices, or lead to other regulatory improvements.

As discussed above, the proposed rule would define ''incident'' as any event, occurrence or circumstance that could jeopardize (*i.e.,* put into danger) information and technology security.[266] This standard would include events that have the potential to harm information and technology security regardless of whether a harm actually materializes. The proposed notification standard, by contrast, would limit the scope of incidents required to be reported to the Commission to those where there is an observable negative impact or harm, or such negative impact or harm is reasonably likely. Covered entities would not, for instance, need to notify the Commission of unsuccessful attempts at unauthorized access, as the detection and deterrence of such an attempt would not require Commission action and would appear to be suggestive of an ORF that is operating as expected. If, however, a covered entity determines that an unauthorized person did access covered information, the Commission would need to be notified, regardless of how much information was accessed or whether the covered entity believes it has been used. The Commission would similarly want to know of any successful distributed denial-of-service attack that disrupts business operations, regardless of the length of time of that disruption.[267]

The Commission appreciates that, at the outset, information regarding an incident is likely to be incomplete and in flux, and the full impact and root cause of an incident may take some time to reveal itself. Covered entities may also not be able to detect incidents immediately after their occurrence, and with sophisticated malicious attacks, culprits often take steps to hide their intrusions. Nevertheless, the Commission preliminarily believes that delays in reporting an incident to the Commission could impede its ability to make timely assessments and take appropriate action. The Commission is concerned that such delays could have broad implications, especially when there are potential sector-wide ramifications or spill-over effects to other regulated entities that the Commission could assist in managing.

Accordingly, the proposed rule would not prescribe a specific form or content for the notification or include a materiality limiter. The proposed rule would only require that covered entities provide whatever information they have on hand at the time that could assist the Commission in its assessment and response activities.[268] If the proposed rule is adopted, the Commission would simply expect that as an incident progresses, covered entities would continue to engage with the Commission and provide updates as needed.[269]

The proposed rule would not prescribe a particular form for the notification but would require notification via email.[270]

2. Commission Notification of BCDR Plan Activation—Proposed Paragraph (i)(2)

For similar reasons, the proposed rule would also require covered entities to notify the Commission of any determination to activate its BCDR plan.[271] Consistent with the proposed incident notification, covered entities would need to notify the Commission of its determination to activate their BCDR plan within 24 hours of making that determination.[272] Current Commission regulation 23.603 requires swap entities to notify the Commission ''promptly'' of any emergency or other disruption that may affect the ability of a swap entity to fulfill its regulatory obligations or would have a significant adverse effect on the swap entity, its counterparties, or the market.[273] Based on the Commission's experience with this provision, which became particularly relevant during the onset of the COVID–19 pandemic, the Commission believes this standard has been open to wide interpretation among swap entities, leading to broad variations in the timeliness of the notifications to the Commission regarding their decisions to implement their BCDR plans and employ a remote work posture. The Commission therefore preliminarily believes that a more bright-line test that centers on the decision to activate the BCDR plan, an action that presumably would not occur absent an emergency or significant disruption impacting the covered entity, would be easier to apply. The Commission also believes such a standard would facilitate the prompt delivery of information to the Commission so that it may consider whether any action to support the continued integrity of the markets during the course of the emergency is necessary to continue to fulfill its oversight obligations. For that purpose, the Commission believes that 24 hours from activation of the BCDR plan would both encourage covered entities to inform the Commission with sufficient time for it to take any needed action and encourage covered entities to focus initial efforts on resuming or continuing operations.

Under the proposed rule, the notification would need to include all information available to the covered entity at that time, including the date of the emergency or disruption, a brief description thereof, its apparent impact, and any actions the covered entity has taken or is taking to mitigate or recover from the incident, including measures to protect customers and counterparties, as the Commission believes this information would be necessary for it to perform its oversight obligations and take responsive action if needed.[274] The proposed rule would not prescribe a particular form for the notification but would require notification via email.[275]

3. Notifications to Customers or Counterparties—Proposed Paragraph (j)

Finally, the proposed rule would require covered entities to notify customers or counterparties as soon as possible of any incident that could have adversely affected the confidentiality or integrity of such customer or counterparty's covered information or their assets or positions.[276] Such incidents could include the identification of a longstanding vulnerability that left exposed covered information, regardless of whether the covered entity has determined that a

[266] *See* paragraph (a) of proposed Commission regulations 1.13 and 23.603 (defining ''incident'').

[267] Covered entities would not need to notify the Commission of routine testing or planned maintenance.

[268] *See* paragraph (i)(1)(ii) of proposed Commission regulations 1.13 and 23.603.

[269] For avoidance of doubt, the proposed rule would not have any impact on covered entities' obligations to notify criminal authorities as appropriate or required by other law or regulation.

[270] *See* paragraph (i)(2)(iii) of proposed Commission regulations 1.13 and 23.603.

[271] *See* paragraph (i)(2)(i) of proposed Commission regulations 1.13 and 23.603.

[272] *See* paragraph (i)(2)(iii) of proposed Commission regulations 1.13 and 23.603.

[273] *See* 17 CFR 23.603(d) (''Each swap dealer and major swap participant shall promptly notify the Commission of any emergency or other disruption that may affect the ability of the swap dealer or major swap participant to fulfill its regulatory obligations or would have a significant adverse effect on the swap dealer or major swap participant, its counterparties, or the market.'').

[274] *See* paragraph (i)(2)(ii) of proposed Commission regulations 1.13 and 23.603.

[275] *See* paragraph (i)(2)(iii) of proposed Commission regulations 1.13 and 23.603. Current Commission regulation 23.603 does not prescribe the contents of the notification or the method of notification, so these would be new requirements for swap entities. *See* 17 CFR 23.603(d) (''Each swap dealer and major swap participant shall promptly notify the Commission of any emergency or other disruption that may affect the ability of the swap dealer or major swap participant to fulfill its regulatory obligations or would have a significant adverse effect on the swap dealer or major swap participant, its counterparties, or the market.'').

[276] *See* paragraph (j)(1) of proposed Commission regulations 1.13 and 23.603.

bad actor has obtained access to that information. The Commission preliminarily believes that covered entities owe an enhanced duty to protect the covered information provided to them by their customers and counterparties in order to ensure market integrity and support customer protections. The proposed notification standard therefore encompasses incidents where an impact on customers or counterparties may not be definite so that they may have an opportunity to take whatever actions they deem necessary to protect their interests.

Unlike with the proposed notifications to the Commission, however, the Commission preliminarily believes that the accuracy of information provided to customers and counterparties should be prioritized over early delivery to avoid causing unnecessary panic that could have potentially negative and irreversible spill-over effects. Accordingly, the proposed customer/counterparty notification provision does not include a specific minimum timing requirement for the notification other than to require the notification to be provided to customers and counterparties as soon as possible.[277] The proposed rule would further require covered entities to disclose to customers and counterparties information necessary for them to understand and assess the potential impact of the incident on their information, assets, or positions and take any necessary actions (*e.g.,* closing accounts, changing passwords).[278] Such information would include, at a minimum, a description of the incident, the particular way in which the customer or counterparty may have been adversely impacted, measures taken by the covered entity to protect against further harm, and contact information for the covered entity where the customer or counterparty may learn more or ask questions.[279]

4. Request for Comment

The Commission invites comment on all aspects of its proposed ORF notification provisions, including the following questions:

1. *Incident notification to Commission.* The proposed rule would require covered entities to notify the Commission of any incident that ''adversely impacts, or is reasonably likely to adversely impact,'' information and technology security, the ability of the covered entity to continue its business activities as a covered entity, or the assets or positions of a customer or counterparty. As discussed above, the Commission believes this standard would give the Commission an early warning of incidents that do result in an observable negative impact or harm, or such negative impact or harm is reasonably likely, *i.e.,* where information and technology security, business operations, or customers/counterparties is harmed or compromised. Given the purpose of the proposed rule as providing the Commission an early warning so that it may act to help mitigate the potential impacts of the event, the proposed rule does not include a materiality limiter. Should the Commission consider including changing the requirement to further limit the incident notice to the incidents with a ''material'' or ''significant'' adverse impact, or where such a material or significant adverse impact would be reasonably likely? If yes, how would including such a materiality limiter change the scope of incidents that would be reported to the Commission? In other words, what types of incidents would not be reported to the Commission under a standard that includes a materiality limiter, and why should the Commission not receive an early warning of those types of incidents? Please explain and provide examples.

2. *BCDR notification to Commission.* The Commission is proposing to change the notification requirement in Commission regulation 23.603 to trigger upon a covered entity's determination to activate its BCDR plan, rather than ''promptly'' after an emergency or other disruption. Do covered entities typically make a specific determination before activating the BCDR plan? What is the process for making that determination and who makes it? Are there aspects of the BCDR plan that may become active before any formal determination is made? Should the Commission instead require notification ''when'' or ''as soon as'' a BCDR plan is activated? Why or why not? Please explain.

3. *Notifications to customers or counterparties.* The proposed rule would require covered entities to provide affected customers and counterparties information necessary for the affected customer/counterparty to understand and assess the potential impact of the incident on its information, assets, or positions and to take any necessary action. Does the proposed rule provide sufficient information for covered entities to assess and comply with that standard?

I. Amendment and Expansion of Other Provisions in Current Commission Regulation 23.603

As mentioned in previous sections of this notice, the proposed rule would expand and apply the substance of existing provisions in current Commission regulation 23.603 to all covered entities and the ORF in its entirety. Such provisions not yet addressed include (1) the establishment of emergency contacts for the Commission and (2) recordkeeping obligations.[280]

1. Emergency Contacts—Proposed Paragraph (k)

To assist the Commission in responding to a reported incident, or an emergency or other significant disruption causing a covered entity to activate its BCDR plan, the proposed rule would require each covered entity to provide the Commission the name and contact information for two employees with knowledge of the covered entity's incident response plan and two employees with knowledge of the covered entity's BCDR plan.[281] Each identified employee would need to be authorized to make key decisions on behalf of the covered entity in the event of either an incident or the BCDR plan activation, as applicable, as the Commission would want to be sure to be contacting personnel with appropriate knowledge and authority.[282] Any updates to the ORF contacts would need to be made to the Commission as necessary to ensure the Commission's contact information remains accurate and up to date.[283]

This provision is consistent with the existing emergency contacts requirement in the swap entity BCDR plan requirement in current Commission regulation 23.603.[284]

[277] *See id.*

[278] *See* paragraphs (j)(2)(i)–(iv) of proposed Commission regulations 1.13 and 23.603.

[279] *See id.*

[280] *See* 17 CFR 23.603(e) and (i). The Commission would not retain Commission regulation 23.603(h) (business continuity and disaster recovery plans required by other regulatory authorities) as superfluous, *see supra* note 198.

[281] *See* paragraph (k)(1) of proposed Commission regulations 1.13 and 23.603. *See also* 17 CFR 23.603(e) (requiring the designation of two emergency contacts with respect to the BCDR plan for swap entities).

[282] *See* paragraph (k)(2) of proposed Commission regulations 1.13 and 23.603. The two employee contacts identified with respect to the information and technology security program could be the same as the employee contacts for the BCDR plan, provided that they have the requisite authority. *See id.*

[283] *See* paragraph (k)(3) of proposed Commission regulations 1.13 and 23.603.

[284] *See* 17 CFR 23.603(e) (''Each swap dealer and major swap participant shall provide to the Commission the name and contact information of two employees who the Commission can contact in the event of an emergency or other disruption. The

Continued

2. Recordkeeping—Proposed Paragraph (l)

To aid the Commission in fulfilling its oversight responsibilities, the proposed rule would require each covered entity to maintain all records required pursuant to the proposed ORF rule, including the information and technology security program, the third-party relationship program, and the BCDR plan, in accordance with Commission regulation 1.31 and to make them available promptly upon request to representatives of the Commission and to representations of applicable prudential regulators as defined in section 1a(39) of the CEA.[285] This provision is consistent with the existing recordkeeping requirement in the swap entity BCDR plan requirement in current Commission regulation 23.603.[286]

3. Request for Comment

The Commission invites comment on all aspects of the proposed emergency contacts and recordkeeping requirements.

J. Cross-Border Application for Swap Entities

In September 2020, the Commission published a final rule addressing the cross-border application of certain provisions of the CEA applicable to swap entities.[287] The rule addresses the application of the registration thresholds and certain requirements applicable to swap entities and establishes a formal process for requesting comparability determinations for such requirements from the Commission.[288] Therein, the Commission classified current Commission regulation 23.603 (BCDR requirements for swap entities) as a group A requirement.[289] The Commission described the group A requirements as helping swap entities ''implement and maintain a comprehensive and robust system of internal controls to ensure the financial integrity of the firm, and, in turn, the protection of the financial system'' and as ''constitut[ing] an important line of defense against financial, operational, and compliance risks that could lead to a firm's default.'' [290] Pursuant to Commission regulation 23.23(f)(1), a non-U.S. swap entity may satisfy any applicable group A requirement on an entity-wide basis by complying with the applicable standards of a foreign jurisdiction to the extent permitted by, and subject to any conditions specified in, a comparability determination issued by the Commission.[291] In determining to offer substituted compliance for group A requirements broadly to all non-U.S. swap entities, the Commission explained its belief that group A requirements cannot be effectively applied on a fragmented jurisdictional basis, such that it would not be practical to limit substituted compliance for group A requirements to transactions involving only non-U.S. persons.[292]

As discussed above, the proposed rule would amend current Commission regulation 23.603 to contain the entirety of the ORF requirements applicable to swap entities, which would include requirements not only relating to BCDR but also those relating to information and technology security and third-party relationships. The Commission preliminarily believes that the same rationale for classifying BCDR requirements as a group A requirement would apply to the ORF rule more broadly. As discussed in detail above, the Commission preliminarily believes that the proposed information and technology security and third-party risk relationship requirements would also serve to help swap entities implement and maintain a comprehensive and robust system of internal controls, serving as an important line of defense against the threat of failure at the firm level and of the financial system more broadly. Accordingly, should the ORF rule be adopted, the Commission would continue to classify Commission regulation 23.603 in its entirety as a group A requirement, for which substituted compliance would broadly be available pursuant to the requirements of Commission regulation 23.23(f)(1).

As mentioned above, Commission regulation 23.23(f)(1) only allows substituted compliance ''to the extent permitted by, and subject to any conditions specified in, a comparability determination issued by the Commission under [Commission regulation 23.23(g)].'' [293] Current Commission comparability determinations do not address the entirety of the proposed ORF rule, as it has yet to be adopted. Rather, they only address the requirements in current Commission regulation 23.603, which are limited to the BCDR plan requirement.

The Commission appreciates that non-U.S. swap entities have come to rely on existing comparability determinations with respect to the current BCDR requirements in Commission regulation 23.603. Accordingly, in the interest of comity and good governance, should the proposed rule be adopted, the Commission has preliminarily determined to permit non-U.S. swap entities to continue to rely on current comparability determinations with respect to the Commission's BCDR requirements, even as amended. However, for substituted compliance to be available for the ORF rule in its entirety, an eligible swap entity or foreign regulatory authority would need to submit a request for a comparability determination pursuant to Commission regulation 23.23(g). The submission would need to address the full complement of the provisions of the ORF rule, however codified in amended Commission regulation 23.603, including the BCDR requirements. The Commission would then evaluate the request, considering amended Commission regulation 23.603 in its entirety, and, if the Commission were to conclude it appropriate to do so, issue updated comparability determinations that would supersede any pre-existing comparability determinations with respect to BCDR requirements for swap entities.

Request for Comment

The Commission invites comment on all aspects of the cross-border implications of the proposed rule.

---

individuals identified shall be authorized to make key decisions on behalf of the swap dealer or major swap participant and have knowledge of the firm's business continuity and disaster recovery plan. The swap dealer or major swap participant shall provide the Commission with any updates to this information promptly.'').

[285] *See* paragraph (l) of proposed Commission regulations 1.13 and 23.603. *See* 7 U.S.C. 1(a)(39).

[286] *See* 17 CFR 23.603(i) (''The business continuity and disaster recovery plan of the swap dealer and major swap participant and all other records required to be maintained pursuant to this section shall be maintained in accordance with Commission Regulation § 1.31 and shall be made available promptly upon request to representatives of the Commission and to representatives of applicable prudential regulators.'').

[287] *See* Cross-Border Application of the Registration Thresholds and Certain Requirements Applicable to Swap Dealers and Major Swap Participants, 85 FR 56924 (Sept. 14, 2020) (Final Cross Border Rule); 17 CFR 23.23.

[288] *Id.*

[289] *Id.* at 56964–65; 17 CFR 23.23(a)(6) (defining ''group A requirements'').

[290] Final Cross-Border Rule, 85 FR 56964 (providing that ''requiring swap entities to rigorously monitor and address the risks they incur as part of their day-to-day businesses lowers the registrants' risk of default—and ultimately protects the public and the financial system.'').

[291] *See* 17 CFR 23.23(f)(1). *See also* 17 CFR 23.23(a)(11) (defining ''non-U.S. swap entity''); 17 CFR 23.23(g) (describing the process for the issuance of comparability determinations).

[292] *See* Final Cross-Border Rule, 85 FR 56977.

[293] *See* 17 CFR 23.23(f)(1).

K. Implementation Period

Should the proposed rule be adopted, the Commission recognizes that covered entities may need time to establish an ORF or review and update existing plans and procedures for compliance with the proposed ORF rule. The Commission preliminarily believes that, given existing and applicable NFA, prudential, and foreign requirements, six months from the rule's adoption would be a sufficient amount of time for covered entities to achieve compliance with the ORF rule.

The Commission invites comment on the Commission's proposed implementation period for the proposed ORF rule, including the following questions:

1. Would six months be as sufficient amount of time for covered entities to develop compliant ORFs? If not, why not? Please explain.

2. If covered entities would need more than six months to implement the ORF as proposed, how much more time would they estimate to need, and what would they be doing with that time? Please be as detailed as possible.

III. Related Matters

A. Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA) requires Federal agencies, in promulgating regulations, to consider the impact of those regulations on small entities—whether the rules will have a significant economic impact on a substantial number of small entities—and if so, to provide a regulatory flexibility analysis reflecting the impact.[294] The Commission has established certain definitions of ''small entities'' to be used by the Commission in evaluating the impact of its rules on small entities in accordance with the RFA.[295] The proposed regulations would affect FCMs, SDs, and MSPs. The Commission has previously determined that FCMs, SDs, and MSPs are not small entities for purposes of the RFA.[296] Accordingly, the Chairman, on behalf of the Commission, hereby certifies pursuant to 5 U.S.C. 506(b) that the proposed rule and rule amendments would not have a significant economic impact on a substantial number of small entities.

B. Paperwork Reduction Act

The Paperwork Reduction Act (PRA) imposes certain requirements on federal agencies, including the Commission, in connection with conducting or sponsoring any ''collection of information,'' as defined by the PRA.[297] The PRA is intended, in part, to minimize the paperwork burden created for individuals, businesses, and other persons as a result of the collection of information by federal agencies, and to ensure the greatest possible benefit and utility of information created, collected, maintained, used, shared, and disseminated by or for the Federal Government.[298] The PRA applies to all information, regardless of form or format, whenever the Federal Government is obtaining, causing to be obtained, or soliciting information, and includes required disclosure to third parties or the public, of facts or opinions, when the information collection calls for answers to identical questions posed to, or identical reporting or recordkeeping requirements imposed on, ten or more persons.[299]

This proposed rulemaking would result in new collection of information requirements within the meaning of the PRA. The Commission is therefore submitting this proposal to the Office of Management and Budget (OMB) for review.[300] The title for this collection of information is ''Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants.'' The OMB has not yet assigned this collection a control number. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid control number.[301]

If the proposed regulations are adopted, responses to this collection of information would be mandatory. The Commission will protect proprietary information according to the Freedom of Information Act and part 145 of the Commission's regulations, ''Commission Records and Information.'' [302] In addition, section 8(a)(1) of the CEA strictly prohibits the Commission, unless specifically authorized by the CEA, from making public ''data and information that would separately disclose the business transactions or market positions of any person and trade secrets or names of customers.'' [303] The Commission is also required to protect certain information contained in a government system of records according to the Privacy Act of 1974.[304]

1. Information Provided by Reporting Entities/Persons

The proposed regulations would require each covered entity to establish, document, implement, and maintain an ORF that includes an information and technology security program, a third-party relationship program, and a BCDR plan, each of which would need to be supported by written policies and procedures. In addition, the proposed regulations would impose the following reporting, recordkeeping, and disclosure obligations on each covered entity: (1) on an annual basis, written approval of each component program or plan of the ORF and of risk appetite and risk tolerance limits, or in the case of covered entities relying on a consolidated program or plan, written attestation; (2) on an annual basis, documenting review and testing of the ORF; (3) as applicable, notifying the Commission of certain ''incidents,'' as defined in the proposed rule; (4) as applicable, notifying the Commission upon activation of the BCDR plan; (5) as applicable, notifying customers or counterparties of certain ''incidents,'' as defined in the proposed rule; and (6) providing emergency contact information to the Commission in connection with the information and technology security program and the BCDR plan. These requirements will result in new PRA burdens for covered entities.

For purposes of the PRA, the term ''burden'' means the ''time, effort, or financial resources expended by persons to generate, maintain, or provide information to or for a Federal Agency.'' [305] This total includes the anticipated burden associated with the development of the required written policies and procedures, satisfaction of various reporting, recordkeeping, and disclosure obligations, the documentation of required ORF testing and review, and the documentation of risk appetite and risk tolerance limits approval.

As of October 31, 2023, there are 160 covered entities that would become subject to the proposed rule (100 registered swaps dealers, 54 registered futures commission merchants, and 6 dually-registered swap dealers/futures commission merchants). The estimated burden associated with the proposed

[294] 5 U.S.C. 601 *et seq.*

[295] *See* Policy Statement and Establishment of Definitions of ''Small Entities'' for Purposes of the Regulatory Flexibility Act, 47 FR 18618 (Apr. 30, 1982) (RFA Definitions of ''Small Entities'').

[296] *See* RFA Definitions of ''Small Entities,'' 47 FR 18619 (FCMs); Final Swap Entities RMP Rule, 77 FR 20193–94 (SDs and MSPs).

[297] 44 U.S.C. 3501 *et seq.*

[298] *Id.*

[299] *See* 44 U.S.C. 3502(3).

[300] *See* 44 U.S.C. 3507(d); 5 CFR 1320.11.

[301] *See* 44 U.S.C. 3507(a)(3); 5 CFR 1320.5(a)(3).

[302] *See* 5 U.S.C. 552. *See also* 17 CFR part 145.

[303] 7 U.S.C. 12(a)(1).

[304] *See* 5 U.S.C. 552a.

[305] 44 U.S.C. 3502(2).

information collections is calculated as follows:

a. Recordkeeping Requirements

The proposed regulation contains recordkeeping requirements that would result in a collection of information from ten or more persons over a 12-month period.

Establishing, documenting, implementing, and maintaining information and technology security program: As part of an overall ORF, proposed Commission regulations 1.13(d) and 23.603(d) would require covered entities to establish an information and technology security program reasonably designed to identify, monitor, manage, and assess risks relating to information and technology security, including through conducting and documenting risk assessments at least annually. Upon the risk assessment's completion, the results would need to be provided to the oversight body, senior officer, or other senior-level official who approves the information and technology security program. As part of the information and technology security program, the proposed rule would require the covered entity to establish, document, implement, and maintain controls to prevent, detect, and mitigate identified risks to information and technology security. In addition, the proposed rule would require that the information and technology security program include a written incident response plan reasonably designed to detect, assess, contain, mitigate the impact of, and recover from an incident.

The Commission anticipates that a covered entity would require an estimated 200 hours to develop their information and technology security program, including conducting and documenting an annual risk assessment and developing an incident response plan. This yields a total annual burden of 32,000 burden hours (160 respondents × 200 hours = 32,000 hours).

Accordingly, the aggregate annual estimate for the recordkeeping burden associated with this proposal would be as follows:[306]

Number of registrants: 160.

Estimated number of responses: 1.

Estimated total annual burden per registrant: 200 hours.

Frequency of collection: Annually.

Total annual burden: 32,000 burden hours [160 registrants × 200 hours].

Establishing, documenting, implementing, and maintaining third-party relationship program: Proposed Commission regulations 1.13(e) and 23.603(e) would require covered entities to develop a program reasonably designed to identify, monitor, manage, and assess risks relating to third-party relationships. The program would be required to address the risks attendant to each stage of the third-party relationship lifecycle and would be required to include an inventory of third-party service providers the covered entity has engaged to support its activities as a covered entity.

The Commission anticipates that a covered entity would require an estimated 160 hours annually to develop their third-party relationship program, including creating and maintaining a third-party service provider inventory. This yields a total annual burden of 25,600 hours (160 respondents × 160 hours = 25,600 burden hours). The aggregate annual estimate for the recordkeeping burden associated with this proposal would be as follows: [307]

Number of registrants: 160.

Estimated number of responses: 1.

Estimated total annual burden per registrant: 160 hours.

Frequency of collection: Annually.

Total annual burden: 25,600 burden hours [160 registrants × 160 hours].

Establishing, documenting, implementing, and maintaining BCDR plan: Proposed Commission regulations 1.13(f) and 23.603(f) would require covered entities to establish a written BCDR plan reasonably designed to identify, monitor, manage, and assess risks relating to emergencies or other significant disruptions to the continuity of normal business operations as a covered entity.[308] The proposed rule would require the BCDR plan be reasonably designed to enable the covered entity to: (1) continue or resume any activities as a covered entity with minimal disruption to customers, counterparties, and markets; and (2) recover and make use of covered information, in addition to any other data, information, or documentation required to be maintained by law and regulation. These plans would be required to, among other things, establish procedures for data backup and establish and maintain arrangements to provide for redundancies or their backup for covered technology, facilities, infrastructure, personnel, and competencies.

The Commission anticipates that a covered entity would require an estimated 50 hours annually to develop or to update their existing written BCDR plan. This yields a total annual burden of 8,000 burden hours (160 respondents × 50 hours = 8,000 hours).

Accordingly, the aggregate annual estimate for the recordkeeping burden associated with this proposal would be as follows:[309]

Number of registrants: 160.

Estimated number of responses: 1.

Estimated total annual burden per registrant: 50 hours.

Frequency of collection: Annually.

Total annual burden: 8,000 burden hours [160 registrants × 50 hours].

Documentation of ORF review: Proposed Commission regulations 1.13(h) and 23.603(h) would require covered entities to establish, implement, and maintain plans reasonably designed to assess their adherence to, and the effectiveness of, their ORF through regular reviews and risk-based testing.

The proposed rule would require that reviews be conducted at least annually and when any material change to covered entities' activities or operations occurs that is reasonably likely to affect

[306] This estimate reflects the aggregate information collection burden estimate associated with the proposed recordkeeping requirement for the first annual period following implementation of the proposed regulations. Because proposed Commission regulations 1.13(d) and 23.603(d) would require the one-time recordkeeping requirement as to developing the information and technology security program, Commission staff estimates that for each subsequent annual period, the number of burden hours would be reduced accordingly.

[307] This estimate reflects the aggregate information collection burden estimate associated with the proposed recordkeeping requirement for the first annual period following implementation of the proposed regulations. Because proposed Commission regulations 1.13(e) and 23.603(e) would require the one-time recordkeeping requirement as to developing the third-party relationship program, Commission staff estimates that for each subsequent annual period, the number of burden hours would be reduced accordingly.

[308] As discussed in section II.E (Continuity and Disaster Recovery Plan) of this notice, swap entities are already required to establish a written BCDR plan pursuant to current Commission regulation 23.603. The existing burdens for current Commission regulation 23.603 are found in the following information collection, Regulations Establishing and Governing the Duties of Swap Dealers and Major Swap Participants (OMB Control No. 3038–0084). The burden of swap entities updating their BCDR plan is included in the new collection of information established by the proposed rule, but the Commission is retaining its existing burden estimates under Control No. 3038–0084 at this time to avoid undercounting. The Commission will adjust its burden estimates associated with OMB Control No. 3038–0084 at a later date, as necessary.

[309] This estimate reflects the aggregate information collection burden estimate associated with the proposed recordkeeping requirement for the first annual period following implementation of the proposed regulations. Because proposed Commission regulations 1.13(f) and 23.603(f) would require the one-time recordkeeping requirement, as to developing the BCDR plan, Commission staff estimates that for each subsequent annual period, the number of burden hours would be reduced accordingly.

the risks identified in the ORF. With regard to testing, the proposed rule would require that the testing of information and technology security program include, at a minimum, the testing of key controls and the incident response plan at least annually; daily or continuous automated vulnerability scans; and penetration testing at least annually. Additionally, the proposed rule would require that testing of the BCDR plan must include, at a minimum, a walk-through or tabletop exercise designed to test the effectiveness of backup facilities and capabilities at least annually.

The proposed rule would also require covered entities to document all reviews and testing of their ORFs. The proposed rule would require that documentation to include, at a minimum, (i) the date the review or testing was conducted; (ii) the nature and scope of the review or testing, including methodologies employed; (iii) the results of the review or testing, including any assessment of effectiveness; (iv) any identified deficiencies and recommendations for remediation; and (v) any corrective action(s) taken or initiated, including the date(s) of such action(s).

The Commission anticipates that covered entities would require an estimated 80 hours annually to establish a plan to assess adherence to, and the effectiveness of, its ORF, as well as documenting all reviews and testing of the ORF. This yields a total annual burden of 12,800 hours (160 respondents × 80 hours = 12,800 burden hours).

The aggregate annual estimate for the recordkeeping burden associated with this proposal would be as follows: [310]

Number of registrants: 160.

Estimated number of responses: 1.

Estimated total annual burden per registrant: 80 hours.

Frequency of collection: Annually.

Total annual burden: 12,800 burden hours [160 registrants × 80 hours].

Documentation of approval of the component programs or plan, risk appetite, and risk tolerance limits: Proposed Commission regulations 1.13(c)(1) and 23.603(c)(1) would require covered entities to ensure that the information and technology security program, third-party relationship program, and BCDR plan are approved in writing on at least an annual basis by either the senior officer, an oversight body, or a senior-level official with primary responsibility for the component programs or plan. Proposed Commission regulations 1.13(c)(2) and 23.603(c)(2) would require the risk appetite and risk tolerance limits established by covered entities be approved in writing at least annually by either the senior officer, an oversight body, or a senior-level official. Proposed Commission regulations 1.13(c)(4)(ii) and 23.603(c)(4)(ii) would allow covered entities that rely on a consolidated program or plan for its ORF to meet the annual approval requirement for the component programs or plan of the ORF, risk appetite, and risk tolerance limits through an annual written attestation by either the senior officer, an oversight body, or a senior-level official.

The Commission anticipates that covered entities would require an estimated 20 hours annually to document approval of the ORF, risk appetite, and risk tolerance limits or to prepare the written attestation. This yields a total annual burden of 3,200 hours (160 respondents × 20 hours = 3,200 burden hours).

The aggregate annual estimate for the recordkeeping burden associated with this proposal would be as follows:

Number of registrants: 160.

Estimated number of responses: 1.

Estimated total annual burden per registrant: 20 hours.

Frequency of collection: Annually.

Total annual burden: 3,200 burden hours [160 registrants × 20 hours].

b. Reporting Requirements

The proposed regulation contains reporting requirements that would result in a collection of information from ten or more persons over a 12-month period.

Notification of incidents to the Commission: Proposed Commission regulations 1.13(i)(1) and 23.603(i)(1) would require covered entities to notify the Commission regarding incidents that adversely impact or are reasonably likely to adversely impact: (1) information technology and security; (2) the covered entity's ability to continue its business activities; or (3) the assets or positions of a customer or counterparty. These notifications would be required to include information that may assist the Commission in assessing and responding to the incident, including the date the incident was detected, possible cause(s) of the incident, its apparent or likely impacts, and any actions the covered entity has taken or is taking to mitigate or recover from the incident. Notifications would be required to be submitted via email as soon as possible, but no later than 24 hours after an incident is detected.

The Commission anticipates that covered entities may experience one reportable incident per year and that covered entities would expend approximately 10 hours to gather the information required and provide the required notification to the Commission. This would result in an estimated total annual burden of 1,600 hours (160 respondents × 1 reportable incident per year × 10 hours per reportable incident = 1,600 hours).

The aggregate annual estimate for the reporting burden associated with this proposal would be as follows:

Number of registrants: 160.

Estimated number of responses: 1.

Estimated total annual burden per registrant: 10 hours.

Frequency of collection: As needed.

Total annual burden: 1,600 burden hours [160 registrants × 10 hours].

Notification of BCDR plan activation: Proposed Commission regulations 1.13(i)(2) and 23.603(i)(2) would require covered entities to notify the Commission of any determination to activate the BCDR plan. Covered entities would be required to provide such notices via email and include any information available at the time of the notification that may assist the Commission in assessing or responding to the emergency or disruption, including the date of the emergency or disruption, a description thereof, the possible cause(s), its apparent or likely impacts, and any actions the covered entity has taken or is taking to mitigate or recover from the emergency or disruption, including measures taken or being taken to protect customers.

The Commission anticipates that approximately 3 covered entities may activate their BCDR plan per year and that such covered entities would expend approximately 10 hours to gather the information required and to provide the required notification to the Commission. This would result in an estimated total annual burden of 30 burden hours (3 BCDR activations per year × 10 hours per BCDR activation = 30 hours).

The aggregate annual estimate for the reporting burden associated with this proposal would be as follows:

Number of registrants: 3.

Estimated number of responses per respondent: 1.

Estimated total annual burden per registrant: 10 hours.

Frequency of collection: As needed.

[310] This estimate reflects the aggregate information collection burden estimate associated with the proposed recordkeeping requirement for the first annual period following implementation of the proposed regulations. Because proposed Commission regulations 1.13(h) and 23.603(h) would require the one-time recordkeeping requirement as to developing a plan to assess the effectiveness of the ORF, Commission staff estimates that for each subsequent annual period, the number of burden hours would be reduced accordingly.

Total annual burden: 30 burden hours [3 BCDR activations per year × 10 hours].

Filing emergency contact information: Proposed Commission regulations 1.13(k) and 23.603(k) would require covered entities to provide the Commission with emergency contact information for employees to serve as contacts in connection with required incident notifications under the ORF and the activation of the covered entity's BCDR plan.

The Commission anticipates that covered entities would require an estimated 1 hour annually to provide the Commission with emergency contact information. This yields a total annual burden of 160 burden hours (160 respondents × 1 hour = 160 burden hours).

The aggregate annual estimate for the reporting burden associated with this proposal would be as follows: [311]

Number of registrants: 160.

Estimated number of responses: 1.

Estimated total annual burden per registrant: 1 hour.

Frequency of collection: As needed.

Total annual burden: 160 burden hours [160 registrants × 1 hour].

c. Disclosure Requirements

The proposed regulation contains disclosure requirements that would result in a collection of information from ten or more persons over a 12-month period.

Notification of incidents to affected customers and counterparties: Proposed Commission regulations 1.13(j) and 23.603(j) would require covered entities to notify their customers and counterparties as soon as possible of any incident that is reasonably likely to have adversely affected the confidentiality or integrity of the customer's or counterparty's covered information, assets, or positions. The proposed rule would require that notifications include information necessary for the affected customer or counterparty to understand and assess the potential impact of the incident on its information, assets, or positions and to take any necessary action. Such notifications shall include, at a minimum, a description of the incident; the way the customer or counterparty, or its covered information, may have been adversely impacted; measures being taken by the covered entity to protect against further harm; and contact information for the covered entity where the customer or counterparty may learn more about the incident or ask questions.

The Commission anticipates that covered entities may experience 17 reportable incidents per year and that covered entities would expend approximately 50 hours to gather the required information necessary to provide notice of an incident and to prepare and deliver the required notification. This would result in an estimated total annual burden of 850 burden hours (17 reportable incidents per year × 50 hours per reportable incident = 850 burden hours).

The aggregate annual estimate for the disclosure burden associated with this proposal would be as follows:

Number of registrants: 17.

Estimated number of responses per respondent: 1.

Estimated total annual burden per registrant: 50 hours.

Frequency of collection: As needed.

Total annual burden: 850 burden hours [17 reportable incidents per year × 50 hours].

d. Total Burden

Based upon the estimates above, the aggregate annual cost for all covered entities is 84,240 burden hours.

It is expected that covered entities will utilize existing software, information technology and systems. Thus, the Commission believes any additional capital/startup costs or operational/maintenance costs incurred by respondents to report the information required by the proposed regulations to the Commission would be negligible, if any.

2. Request for Comment

The Commission invites the public and other federal agencies to comment on any aspect of the reporting, recordkeeping, and disclosure burdens discussed above. Pursuant to 44 U.S.C. 3506(c)(2)(B), the Commission will consider public comments on this proposed collection of information in:

(1) Evaluating whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information will have practical utility;

(2) Evaluating the accuracy of the Commission's estimate of the burden of the proposed collection of information, including the degree to which the methodology and the assumptions that the Commission employed were valid;

(3) Enhancing the quality, utility, and clarity of the information proposed to be collected; and

(4) Minimizing the burden of the collection of information on covered entities, including through the use of appropriate automated, electronic, mechanical, or other technological information collection techniques, *e.g.,* permitting electronic submission of responses.

A copy of the supporting statements for the collections of information discussed above are available from the CFTC Clearance Officer, 1155 21st Street NW, Washington, DC 20581, 202–418–5714, or from *https://www.RegInfo.gov.* Organizations and individuals desiring to submit comments on the proposed information collection requirements should send those comments to:

- The Office of Information and Regulatory Affairs, Office of Management and Building, Room 10235, New Executive Office Building, Washington, DC 20503, Attn: Desk Officer of the Commodity Futures Trading Commission;
- 202–395–6566 (fax);
- *OIRAsubmissions@omb.eop.gov* (email).

Please provide the Commission with a copy of submitted comments so that all comments can be summarized and addressed in the final rulemaking. Please refer to the **ADDRESSES** section of this notice of proposed rulemaking for comment submission instructions to the Commission. OMB is required to decide concerning the collection of information between 30 and 60 days after publication of this document in the **Federal Register**. Therefore, a comment is best assured of receiving full consideration if OMB (and the Commission) receives it within 30 calendar days of publication of this notice. Nothing in the foregoing affects the deadline enumerated above for public comment to the Commission on the proposed rule.

C. Cost-Benefit Considerations

Section 15(a) of the CEA requires the Commission to consider the costs and benefits of its discretionary actions before promulgating a regulation under the CEA or issuing certain orders.[312] Section 15(a) further specifies that the costs and benefits shall be evaluated in light of five broad areas of market and public concern: (1) Protection of market participants and the public; (2) efficiency, competitiveness, and financial integrity of swaps markets; (3) price discovery; (4) sound risk

[311] This estimate reflects the aggregate information collection burden estimate associated with the proposed reporting requirement for the first annual period following implementation of the proposed regulations. Because proposed Commission regulations 1.13(k) and 23.603(k) would require the emergency contact information provided to the Commission to be updated only as necessary, Commission staff estimates that for each subsequent annual period, the number of burden hours would be reduced accordingly.

[312] *See* 7 U.S.C. 19(a).

management practices; and (5) other public interest considerations.[313] In conducting its analysis, the Commission may, in its discretion, give greater weight to any one of the five enumerated areas of concern. The Commission considers the costs and benefits resulting from its discretionary determinations with respect to the considerations of section 15(a) of the CEA.

As detailed above, the proposed rule would require covered entities (FCMs, SDs, and MSPs) to establish, document, implement, and maintain an ORF reasonably designed to identify, monitor, manage, and assess risks relating to (i) information and technology security, (ii) third-party service providers, and (iii) emergencies or other significant disruptions to the continuity of their normal business operations.[314] The ORF would accordingly need to include a program or plan directed at each of these three risk areas (an information and technology security program, a third-party relationship program, and a business continuity and disaster recovery plan), as well as a plan for the review and testing of the ORF, each of which would need to meet certain specified minimum requirements.[315] The proposed rule would further establish governance, training, and recordkeeping requirements related to the ORF, as well as require notification of certain ORF-related events to the Commission and customers or counterparties.[316] The main purpose of the proposed ORF, as discussed above, is to promote sound practices for managing risks relating to information and technology security, third-party relationships, and emergencies or other significant disruptions, so as to support covered entity operational resilience, to the benefit of customers, counterparties, and the derivatives markets more broadly.

The Commission identifies and considers the benefits and costs of the proposed amendments relative to the baseline of the current status quo. As discussed above, all of the proposed requirements would be new CFTC requirements for covered entities, with the exception of the BCDR plan requirement for swap entities, which the proposed rule would amend in certain respects.[317] Nevertheless, the Commission preliminarily believes that many, if not all, covered entities currently registered with the Commission have likely adopted documents, policies, and practices consistent with the proposed ORF rule. Current NFA rules and interpretive notices, for instance, address the core risks at the center of the ORF—information and technology security, third-party risks, and BCDR planning—and establish related requirements that apply to covered entities, including a BCDR plan requirement for FCMs.[318] Additionally, many covered entities are subject to prudential regulation, which includes requirements relating to information security and notifications of related incidents.[319] Prudential regulators have also provided guidance relating to operational resilience and third-party relationships.[320] Furthermore, based on its oversight activities, the Commission preliminarily believes that certain aspects of the proposed rule requirements are already employed by many covered entities as recommended best practices.

The Commission acknowledges that, no matter the degree to which a covered entity currently operates in a manner consistent with the requirements of the proposed rule, covered entities would all incur some level of costs in reviewing the proposed rule and comparing their existing practices and procedures against it to ensure they meet the minimum requirements and make any necessary updates. Nevertheless, the Commission preliminarily believes that the actual costs and benefits of the proposed rule as realized by most current covered entities may not be as significant as they would be for entities not already subject to NFA or prudential authority or that have not already adopted operational resilience practices in line with general standards and best practices. The Commission also preliminarily believes that leveraging existing standards and guidance and aligning with other applicable authorities to the degree sensible and appropriate, as recommended by the National Cyber Strategy, in itself is a benefit to covered entities and the markets more broadly, by reducing compliance burdens while promoting practices that have proven to support operational resilience and positive regulatory outcomes. Customers, counterparties, and the public more generally would likely benefit as well, as the proposed rule would allow the Commission to exercise its oversight authority to foster compliance with the ORF requirements that are currently absent from its regulations.

By its terms, section 15(a) does not specifically require the Commission to quantify the costs and benefits of a new rule or to determine whether the benefits of the adopted rule outweigh its costs. Rather, section 15(a) requires the Commission to ''consider the costs and benefits'' of a subject rule.[321] The Commission has endeavored to assess the expected costs and benefits of the proposed amendments in quantitative terms, including PRA related costs, where possible. In situations where the Commission is unable to quantify the costs and benefits, the Commission identifies and considers the costs and benefits of the applicable proposed amendments in qualitative terms. However, the Commission lacks the data necessary to reasonably quantify all of the costs and benefits considered below. Additionally, any initial and recurring compliance costs for any particular covered entity would depend on its size, existing infrastructure, practices, and cost structures, as well as the nature, size, scope, complexity, and risk profile of its operations as a covered entity. It is impossible to place a reliable dollar figure on potential future incidents that might be prevented through this rulemaking because the threats are too varied. The constantly changing nature of technology exacerbates this difficulty.[322]

[313] *Id.*

[314] *See* paragraph (b)(1) of proposed Commission regulations 1.13 and 23.603.

[315] *See* paragraphs (b)(2) (components), (d) (information and technology security program), (e) (third-party relationship program), (f) (business continuity and disaster recovery plan), and (h) (reviews and testing) of proposed Commission regulations 1.13 and 23.603.

[316] *See* paragraphs (c) (governance), (g) (training), (i) (notifications to the Commission), (j) (notification of incidents to affected customers or counterparties), (k) (emergency contacts), and (l) (recordkeeping) of proposed Commission regulations 1.13 and 23.603.

[317] *See* 17 CFR 23.603.

[318] *See supra* note 43; *see also supra* note 60 (noting that NFA's requirement to establish a business continuity and disaster recovery plan does not apply to swap entities).

[319] *See* Computer-Security Incident Notification Requirements for Banking Organizations and their Bank Service Providers, 86 FR 66424 (Nov. 23, 2021); 12 CFR part 30, app. A (Interagency Guidelines Establishing Standards for Safety and Soundness); 12 CFR part 30, app. B (Interagency Guidelines Establishing Information Security Standards).

[320] *See supra* note 43. *See also supra* note 50. The Commission notes that the Prudential Operational Resilience Paper was ''written for use by the largest and most complex domestic firms,'' including financial institutions with average total consolidated assets greater than or equal to (a) $250 billion or (b) $100 billion and have $75 billion or more in average weighted short-term wholesale funding, average nonbank assets, or average off-balance-sheet exposure. *See* Prudential Operational Resilience Paper, *supra* note 11, at 1.

[321] *See* 7 U.S.C. 19(a).

[322] FSI Cybersecurity Paper, *supra* note 15, at 1 (''The cyber threat landscape is also characterised by a significant and continuous rise in the cost of cyber incidents. Statista (2023) estimated the global cost of cyber crime in 2022 at $8.4 trillion and

Continued

Regarding covered entities' costs, while the Commission generally believes—based on anecdotal information and its general understanding—that covered entities have already instituted, to a large degree, the practices called for in the proposed rule, the Commission lacks empirical evidence or data to verify that belief (including the number of covered entities whose practices currently meet the requirements being proposed) and quantify what, if any, material costs covered entities would incur to comply with the proposed regulations. To the extent covered entities would need to make operational changes to comply with the proposed amendments, the Commission expects they would be proportionate to the nature, size, scope, complexity, and risk profile of their operations as covered entities. The Commission therefore invites comments providing data and other empirical information to allow it to quantify the degree to which: (1) covered entities currently have implemented (or independent of the proposed amendments, otherwise plan to implement) practices that are compliant with the Commission's proposed regulations and (2) the expected additional costs for any covered entities that, to date, have not completely done so or are otherwise moving independently towards doing so.

The Commission notes that this cost-benefit consideration is based on its understanding that the derivatives markets regulated by the Commission function internationally with: (1) transactions that involve U.S. entities occurring across different international jurisdictions; (2) some entities organized outside of the United States that are registered with the Commission; and (3) some entities that typically operate both within and outside the United States and that follow substantially similar business practices wherever they are located. Where the Commission does not specifically refer to matters of location, the discussion of costs and benefits below refers to the effects of the proposed regulations on all relevant derivatives activity, whether based on their actual occurrence in the United States, or on their connection with, or effect on, U.S. commerce.

In the sections that follow, the Commission discusses the costs and benefits associated with the proposed rule, as well as reasonable alternatives, relative to the baseline. The Commission generally requests comment on all aspects of its cost-benefit consideration, including the baseline; assumptions and methodology employed; the identification and measurement of costs and benefits relative to the baseline; the identification, measurement, and assessment of any costs and benefits not discussed herein; data and any other information to assist or otherwise inform the Commission's ability to better quantify or qualitatively understand and describe the costs and benefits of the proposed amendments; whether and what specific alternatives would be more reasonable in terms of their costs and benefits and why; and substantiating data, statistics, and any other information to support positions posited by commenters with respect to the Commission's discussion and/or requests for comments.

1. Costs and Benefits

The following sections discuss the costs and benefits that the Commission preliminarily expects to result from the requirements in the proposed rule.

e. Generally—Proposed Paragraph (b)

The proposed rule would require covered entities to establish, document, implement, and maintain an ORF reasonably designed to identify, monitor, manage, and assess risks relating to: (i) information and technology security; (ii) third-party relationships; and (iii) emergencies or other significant disruptions to the continuity of normal business operations as covered entities.[323] The ORF would need to, at a minimum, include an information and technology security program, a third-party relationship program, and a business continuity and disaster recovery plan, and each component program or plan would need to be supported by written policies and procedures.[324] Covered entities would further need to ensure that their ORF is appropriate and proportionate to the nature, size, scope, complexity, and risk profile of their business activities as covered entities, following generally accepted standards and best practices.[325]

The Commission anticipates that the main source of costs associated with establishing, documenting, implementing, and maintaining the ORF, as required, would derive from creating and implementing the necessary core component programs and plan, the detailed requirements and costs and benefits of which are discussed in greater detail in the sections that follow. As discussed above, although the Commission expects that most covered entities have already established at least some of elements of the ORF in place by virtue of NFA or other requirements, covered entities would, at minimum, need to devote time and resources to reviewing their existing programs to ensure they meet the requirements of the proposed rule and making any necessary amendments. Accordingly, the Commission anticipates all covered entities would incur at least a one-time fixed cost associated with reviewing their existing programs to ensure compliance, and to identify and make any potential required updates. Specifically, the Commission expects covered entities would incur a one-time initial cost of $41,000 (410 hours[326] × $100/hour) to review their existing programs and identify and make any necessary changes, or an estimated aggregate dollar cost of $6,560,000 (160 covered entities × $41,000).[327]

To the extent that covered entities' current operational resilience practices do not meet the minimum requirements

expects this to go beyond $11 trillion in 2023. This reflects an annual increase of 30% in the cost of cyber crime during the 2021–23 period. Moreover, the average cost of a data breach between 2020 and 2022 increased by 13%, with the financial industry scoring the second highest average cost after healthcare at $6 million. According to Chainalysis (202[3]), 2022 was the biggest year ever for crypto hacking, with $3.8 billion stolen from cryptocurrency businesses. Cyber insurance demand continues to outweigh supply and that the cyber protection gap appears to be widening amid a market characterised by rising premiums, narrowing coverage and tighter underwriting standards.'').

[323] *See* paragraph (b)(1) of proposed Commission regulations 1.13 and 23.603.

[324] *See* paragraph (b)(2) of proposed Commission regulations 1.13 and 23.603.

[325] *See* paragraph (b)(3) of proposed Commission regulations 1.13 and 23.603.

[326] This hour estimate reflects the aggregate amount of time the Commission estimates covered entities will expend establishing, documenting, implementing and maintaining the core component programs and plan of their ORF (*i.e.,* information and technology security program, third-party relationship program, and business continuity and disaster recovery plan). *See* section III.B (Paperwork Reduction Act) of this notice, *supra.*

[327] The cost estimates in this section were determined using an average salary of $100.00 per hour. The Commission believes that this is an appropriate salary estimate for purposes of the proposed rule based upon the May 2022 Bureau of Labor Statistics' average hourly rate for the following positions: (1) $63.08 for management occupations; (2) $41.39 for business and financial operations occupations; (3) $51.99 for computer and mathematical occupations; (4) $67.71 for computer engineering occupations; (5) $59.87 for legal occupations; and (6) $21.90 for office and administrative support occupations. Based on this data, the Commission took the mean hourly wage for these positions and increased it to $100 in recognition that some covered entities are large financial institutions whose employees' salaries may exceed the mean wage. *See* U.S. Bureau of Labor Statistics, May 2022 National Occupational Employment and Wage Estimates (last updated Apr. 25, 2023), *available at https://www.bls.gov/oes/current/oes_nat.htm#43-0000.*

of the proposed rule, they may incur more and other forms of costs in updating the programs. Such costs could include fixed costs associated with securing new technology or other services (*e.g.,* upgrading technology, incorporating penetration testing), or even adding new staffing to support new required functions, as well as new ongoing costs related to monitoring and training. By requiring that the ORF, and consequently the associated programs and plan, are appropriate and proportionate to the covered entity, the Commission expects that the extent of those costs should be reasonably mitigated, such that covered entities should be able to tailor their ORFs to their unique circumstances and not incur costs to adopt practices or technologies that would not be recommended or necessary for them.

Additionally, to the extent costs in updating programs are unavoidable, the Commission believes the proposed ORF rule is reasonably designed to ensure that the costs would support covered entities' operational resilience, and the broader security of the derivatives markets as a whole, as discussed in greater detail below. More specifically, the Commission believes the proposed ORF rule is reasonably designed to ensure customer and counterparty information and assets remain protected, and that the derivatives markets remain stable and functioning, particularly as covered entities become ever more reliant on rapidly evolving technology and/or third-party service providers to support their operations. Requiring all covered entities to have a framework directed at operational resilience that meets certain minimum requirements, including governance, training, and testing requirements, would give the CFTC, customers, counterparties, and covered entities themselves confidence that there exists among all covered entities a certain foundational level of security and resilience. Requiring covered entities to base their ORFs on generally accepted standards and best practices further buttresses that assurance by making sure adopted practices are grounded in standards that are commonly known and accepted, widely recognized as effective, and require adaptation as risk profiles change. Relying on existing known standards should also help mitigate implementation costs compared to complying with specific and detailed requirements created by the Commission and applied more uniformly. Furthermore, as the Commission engages in oversight of ORFs, it would expect to be able to identify additional recommended best practices unique to covered entities that it could share through guidance or future rulemakings, which would operate to further support the stability of the derivatives markets.

f. Governance—Proposed Paragraph (c)

The proposed rule would require that each of the three required component programs and plan (the information and technology security program, the third-party relationship program, and the business continuity and disaster recovery plan) be approved in writing, on at least an annual basis, by either the senior officer, an oversight body, or a senior-level official of the covered entity.[328] Covered entities would likely experience some costs associated with selecting the responsible official or body to provide the approval and associated costs to obtain their approval, including the time and resources needed to develop any explanatory materials, making amendments in light of any comments from leadership, and ministerial costs associated with obtaining signatures. More specifically, the Commission estimates that covered entities would incur an initial cost of $4,000 (40 hours × $100/hour) to select the responsible official or body to approve the component programs and plan of the ORF,[329] or an estimated aggregate dollar cost of $640,000 (160 covered entities × $4,000). Additionally, the Commission estimates that covered entities will incur an ongoing annual cost of $1,000 for the approval of the component programs or plan of the ORF (10 hours × $100/hour),[330] or an estimated aggregate dollar cost of $160,000 (160 covered entities × $1,000).

However, the Commission anticipates that providing a covered entity broad discretion to select whomever it deems appropriate to provide the approval would serve to mitigate some of those costs by allowing the covered entity to embed the approval process within its existing operational structures. The Commission further believes that requiring regular and formal approval of the ORF component programs and plan by senior leadership would help ensure that the ORF is in line with operational strategy and risk capacity, improving the chances that the covered entity would be adequately prepared for, and able to withstand and recover from operational shocks, that could otherwise significantly harm customers, counterparties, or even have spillover effects into the derivatives market as a whole.

The proposed rule would further require covered entities to establish risk appetite and risk tolerance limits with respect to the risk areas underlying the ORF (information and technology security, third-party relationships, and emergencies or other significant disruptions to the continuity of normal business operations).[331] The Commission believes that establishing and operating within established risk appetite and risk tolerance limits would help ensure that covered entities do not engage in activities that would present risks beyond those they can comfortably manage, helping to mitigate the potential for covered entities to take on risk that could lead to intolerable harm to customers or disruption to the financial system at large.

Covered entities that do not currently have a practice of creating a risk appetite statement and establishing and monitoring metrics for risk tolerance limits would likely incur costs associated with establishing a methodology to identify them, which would involve time and staffing resources, or perhaps even the use of consultants, but the Commission anticipates such costs should be reduced year over year as such covered entities gain experience and streamline processes. Nevertheless, the Commission understands that establishing risk appetite and tolerance limits is common practice in the financial industry, and is included as a recommended part of governance in the NIST financial sector profile.[332] To the extent that covered entities already follow this practice, such covered entities would incur general costs associated with reviewing their risk appetite and risk tolerance limits against the rule requirements to ensure they cover the full scope of the rule, but they would avoid the heavier resource burdens of developing risk appetite and risk tolerance limits from whole cloth.

The risk appetite and risk tolerance limits would further need to be

[328] *See* paragraph (c)(1) of proposed Commission regulations 1.13 and 23.603.

[329] Covered entities may also incur subsequent costs in the event there is a change in official or body responsible for the approval of the ORF component programs or plan.

[330] As discussed *supra* in section III.B (Paperwork Reduction Act) of this notice, the Commission expects covered entities will expend a total of 20 burden hours to approve the component programs and plan of the ORF, risk appetite, and risk tolerance limits, or to prepare a written attestation.

[331] *See* paragraph (c)(2)(i) of proposed Commission regulations 1.13 and 23.603.

[332] *See* CRI Profile Workbook, *supra* note 81, at 16 (''An appropriate governing authority . . . endorses and periodically reviews the cyber risk appetite and is regularly informed about the status of and material changes in the organization's inherent cyber risk profile).

reviewed and approved in writing on at least an annual basis by the oversight body, senior officer, or other senior-level official with primary responsibility for the relevant risk area.[333] Similar to the broad approval of the ORF component programs and plan in general, covered entities would likely incur some costs preparing information for approval, making amendments in response to comments, and obtaining signatures. Specifically, the Commission estimates covered entities would incur an ongoing annual cost of $1,000 for the approval of risk appetite and risk tolerance limits (10 hours × $1,000),[334] or an estimated aggregate dollar cost of $160,000 (160 covered entities × $1,000). The Commission believes that the process of securing formal approval would encourage covered entities to think critically about the risk appetite and risk tolerance limits they establish and to justify them in light of operational strategy. This exercise should bring more awareness to activities that create operational risk and lead to better outcomes from an operational resilience standpoint, with attendant benefits to customers, counterparties, and the market more broadly.

Relatedly, the proposed rule would require covered entities to notify selected senior leadership of circumstances that exceed risk tolerance limits and incidents requiring notification to either the Commission or customers and counterparties.[335] The Commission understands that such an internal escalation requirement would require covered entities to incur some costs in developing policies and procedures that reflect this requirement, or reviewing existing escalation protocols to ensure they meet the terms of the rule, but the Commission believes the requirement is sufficiently flexible to allow covered entities to rely on existing operational structures and reporting lines, and does not anticipate that any organizational changes, or attendant costs, would be necessary. Additionally, the Commission views the involvement and awareness of senior leadership in cases where risk tolerance limits are exceeded, or where significant incidents have occurred that clearly threaten operational resilience, as critical to ensuring recovery efforts are coordinated and thus more likely to be successful.

The proposed rule would allow covered entities that form a part of a larger enterprise to satisfy the requirements of the proposed rule through their participation in a consolidated program or plan that meets the requirements of the proposed rule.[336] Additionally, a covered entity relying on a consolidated program or plan would be able to satisfy the requirements for senior leadership to approve both the component program or plan and risk appetite and risk tolerance limits by having senior leadership attest on an annual basis that the consolidated program or plan meet the requirements of the proposed ORF rule, and reflects risk appetite and risk tolerance limits appropriate to the covered entity.[337] The Commission estimates that covered entities would incur an ongoing annual cost of $2,000 (20 hours × $100/hour) to prepare an written attestation,[338] or an estimated aggregate dollar cost of $320,000 (160 covered entities × $2,000). The Commission believes allowing covered entities to rely on a consolidated program or plan would mitigate costs for such entities, specifically by benefiting from economies of scale present in relying on shared corporate infrastructure and a larger parent company's resources to manage operational risk at a broader enterprise level, and through using existing practices that meet the requirements of the proposed rule.

Nevertheless, the Commission expects that such covered entities would incur at least some costs associated with reviewing the consolidated program or plan to ensure it meets the requirements of the proposed rule and reflect risk appetite and risk tolerance limits appropriate to the covered entities. Such covered entities may face challenges in ensuring that their consolidated programs or plans, which may be written with the parent corporate entity as the primary focus, appropriately address the risks as they relate more specifically to the business and operations of the covered entity, which may be a relatively small line of business for the parent. Accordingly, a covered entity may incur some costs, in terms of time and staffing resources, associated with amending any consolidated program or plan to ensure it reflects the proposed rule's requirements and risk appetite and risk tolerance limits appropriate to the covered entity. The Commission cannot accurately quantify such costs, as these costs could range from minimal to more substantial depending on the complexity of the organization and how closely the current consolidated program or plan meets the requirements of the proposed rule, including how particularized they are with respect to identifying and managing the risks specific to the covered entity. The Commission believes that such requirements are important to ensuring that all covered entities, regardless of their operational structure, have a baseline level of operational risk management that is tailored to the entity itself, helping reduce risk to the overall financial system and the commodity derivatives markets in particular. The Commission also preliminarily believes that the overall costs of the proposed rule are reduced, without any loss of benefit, by allowing covered entities to rely on consolidated programs or plans over requiring them to duplicate existing larger corporate entity efforts to produce programs or plans that are independent and unique to the covered entity.

g. Information and Technology Security Program—Proposed Paragraph (d)

The proposed rule would require covered entities to have an information and technology security program, defined as a written program reasonably designed to identify, monitor, manage, and assess risks relating to information and technology security and that meets certain requirements.[339] Specifically, the information and technology security program would need to include (1) a risk assessment, conducted at least annually; (2) effective controls; and (3) an incident response plan.[340] The proposed risk assessment requirement would require covered entities to identify and devote resources to planning and performing the risk assessment and then analyzing its results. These resources would need to include reliance on personnel not responsible for the development or implementation of covered technology or related controls, which could impose additional staffing needs on some

[333] *See* paragraph (c)(2)(ii) of proposed Commission regulations 1.13 and 23.603.

[334] As discussed in section III.B (Paperwork Reduction Act) of this notice, the Commission expects covered entities will expend a total of 20 burden hours annually to document approval of the component plans of the ORF, risk appetite, and risk tolerance limits, or to prepare a written attestation.

[335] *See* paragraphs (c)(3)(i)–(ii) of proposed Commission regulations 1.13 and 23.603.

[336] *See* paragraph (c)(4)(i) of proposed Commission regulations 1.13 and 23.603.

[337] *See* paragraph (c)(4)(ii) of proposed Commission regulations 1.13 and 23.603.

[338] As discussed *supra* in section III.B (Paperwork Reduction Act) of this notice, the Commission expects covered entities will expend a total of 20 burden hours annually to document approval of the component programs or plans of the ORF, risk appetite, and risk tolerance limits, or to prepare a written attestation.

[339] *See* paragraphs (a) (defining ''information and technology security program'') and (b)(2) (components) of proposed Commission regulations 1.13 and 23.603.

[340] *See* paragraph (d) of proposed Commission regulations 1.13 and 23.603.

covered entities.[341] The amount of time and resources expended would likely vary depending on the size, complexity, and risk profile of the covered entity and its degree of reliance on covered technology. The Commission believes that larger covered entities with more complex business operations and broader risk profiles would likely need to devote more permanent and extensive resources, staffing and otherwise, to performing and analyzing their risk assessments. Presenting the results of the assessment to selected senior leadership would also require the devotion of time and staffing resources to prepare for and respond to leadership feedback.

In establishing effective controls, covered entities would be required to consider a broad range of categories of controls, determine which to implement in line with identified risks, implement them, and then review and revise the controls as needed over time in response to continued risk assessments. Depending on the types of controls they would need to implement, covered entities may take on additional costs to acquire new security technology and/or hire additional staff or third-party service providers to oversee and implement the controls. Again, the Commission would expect any outlays to be appropriate and proportionate to the covered entity and its risk profile, so the exact costs would vary by covered entity. Nevertheless, given that the approach of the proposed rule, and list of required categories, closely aligns with the longstanding approach adopted by prudential regulators with respect to information and technology security controls, the Commission believes that costs for at least prudentially regulated covered entities may be reduced compared to other covered entities that have not been required to apply and consider such categories of controls.[342]

Development of an incident response plan would likely require a noticeable devotion of resources at the outset, as staff would need to dedicate time and effort to forming and documenting the plan, including creating policies and procedures for identifying the types of incidents that need to be reported and to whom. Should an incident occur, the plan would require staff at the covered entity to devote time to documenting and responding to the incident, as well as identifying and taking on remediation efforts.

Nevertheless, the Commission expects that, given the NFA's ISSP Notice, covered entities would likely not need to expend resources to develop an information and technology security program from scratch. Notably, NFA requires its members to adopt and enforce a written ISSP, assess and prioritize the risks associated with its use of information technology systems, document and describe in their ISSPs safeguards deployed in light of identified and prioritized threats and vulnerabilities, and create an incident response plan.[343] Accordingly, some of the compliance burdens associated with implementing an information and technology security program should be reduced. Covered entities overseen by prudential regulators are also required to consider similar categories of controls to those in the proposed rule, so compliance costs as realized by prudentially regulated covered entities may be even further reduced.[344] Notably, however, NFA does not mandate that a risk assessment be conducted at least annually by personnel not responsible for the development or implementation of covered technology or related controls. Although the Commission believes these requirements to be consistent with generally accepted standards and best practices, such that covered entities may be following them anyway, some covered entities may nevertheless experience some additional costs associated with ensuring or otherwise acquiring staff sufficiently independent to conduct the risk assessment and in potentially conducting the risk assessment more frequently than they currently do. The Commission also recognizes that, if adopted, the proposed rule would at minimum require covered entities to expend resources to review the ISSPs they established pursuant to NFA rules to ensure they meet the requirements of the information and technology security program.

Notwithstanding the potential operational and staffing costs to covered entities associated with the proposed rule, the Commission believes the benefits of the requirements of the proposed information and technology security program are well established. Risk assessments are crucial to identifying threats and vulnerabilities, which is key to directing resources to mitigate those risks in a way that increases the effectiveness of security efforts. The Commission likewise believes the benefits of an independent risk assessment (a more unbiased and reliable assessment) and conducting it at least annually (ensuring the information and technology security program is up-to-date and responsive in light of current threat landscape and vulnerabilities at the covered entity) are important to supporting covered entity operational resilience. Likewise, controls are the methods or techniques for monitoring and managing those risks and safeguarding information, operations, and assets. Without them, the potential for a system weakness to be exploited, and for customers and counterparties, covered entities, or the market at large to be harmed is increased, as the interconnected nature of the commodity derivatives markets enhances the possibility for spillover effects. Incident response plans operate to reduce the potential magnitude of the harm should a safeguard fail by creating a concrete plan, known in advance, for how the covered entity should respond, thereby shortening response times following an incident. Accordingly, the Commission believes the proposed minimum requirements of the information and technology security program, in combination with the Commission's oversight, would further support the development of a foundational level of operational risk management practices with respect to information and technology security that would benefit customers, counterparties, and the market at large.

h. Third-Party Relationship Program—Proposed Paragraph (e)

The proposed rule would require covered entities to have a third-party relationship program, defined as a written program reasonably designed to identify, monitor, manage, and assess risks relating to third-party relationships.[345] The program would need to describe how covered entities address the risks attendant to each of the five identified stages of the third-party relationship lifestyle, ranging from pre-selection to termination, with heightened due diligence and monitoring required for critical third-party service providers.[346] The proposed rule would further require covered entities to create, maintain, and regularly update an inventory of third-party service providers engaged to support their activities as covered entities, identifying whether each is a critical third-party service provider.[347]

[341] *See* paragraph (d)(1)(ii) of proposed Commission regulations 1.13 and 23.603.

[342] *See supra* note 130 and accompanying text.

[343] *See* NFA ISSP Notice, *supra* note 43.

[344] *See* 12 CFR part 30, app. B.

[345] *See* paragraphs (a) (defining ''third-party relationship program'') and (e) (third-party relationship program) of proposed Commission regulations 1.13 and 23.603.

[346] *See* paragraphs (e)(1)(i)–(v) and (e)(2) of proposed Commission regulations 1.13 and 23.603.

[347] *See* paragraph (e)(3) of proposed Commission regulations 1.13 and 23.603.

As with the information and technology security program, complying with this aspect of the proposed rule would require covered entities to expend staff resources at the outset to develop the program and put it into writing. Although NFA requires its members, including covered entities, to have a written supervisory framework for its third-party service providers, which could help mitigate these costs, NFA's written supervisory framework only extends to outsourcing functions, *i.e.,* regulatory functions that would otherwise be undertaken by the NFA member itself to comply with NFA and CFTC requirements.[348] Accordingly, covered entities would likely experience at least some staffing burdens expanding their NFA frameworks to fit the broader scope of third-party relationships covered by the proposed rule and implementing it across their third-party service providers more broadly. However, applying the proposed (b)(3) standard, covered entities should be able to align their third-party risk management practices to the risks presented by each individual third-party service provider, which would allow covered entities to tailor and fit the costs of their third-party practices to their unique circumstances. Covered entities following prudential rules and guidance with respect to third-party service providers, which applies to all third-party relationships, would likely experience reduced costs compared to other covered entities with respect to any need to modify their existing programs.[349] Additionally, the proposed rule would not require covered entities to perform due diligence or renegotiate contracts with existing third-party service providers, which would avoid a potentially substantial initial fixed cost from implementing the third-party relationship program.

Creating an initial inventory of third-party service providers, and assessing whether they meet the definition of ''critical third-party service provider'' would also require a temporary redirection of staff resources, with the amount of time and resources required varying depending on the extent and complexity of a given covered entity's reliance on third-party service providers. With respect to critical third-party service providers, the Commission preliminarily believes that many, if not all, covered entities currently have in place a process to identify and categorize covered entities as ''critical'' or otherwise requiring enhanced supervisory activities. Additionally, NFA requires its members to have heightened due diligence for third-party service providers that obtain or have access to critical and/or confidential data and those that support critical regulatory-related systems, which could potentially reduce burdens on covered entities in designing and implementing heightened due diligence and monitoring with respect to critical third-party service providers.[350] Although the Commission preliminarily believes that its proposed definition of ''critical third-party service provider'' should identify many, if not all, of the same providers covered entities would themselves identify as ''critical,'' the Commission recognizes that the process of applying the proposed definition to an existing process would, at minimum, require some initial expenditure of staff resources to ensure existing practices and taxonomies align with the proposed rule.[351] Additionally, the process of creating an inventory of third-party service providers, which is not currently required by NFA or prudential regulators, could be particularly burdensome, especially for covered entities with a large number of complex third-party relationships, or that rely on an affiliate to secure and coordinate third-party service providers as part of a larger enterprise-wide function, potentially involving staff from many different departments or the review of multiple contracts or contract databases.

Nevertheless, the Commission believes that requiring covered entities to have a program to identify, monitor, manage, and assess risks relating to third-party relationships, and inventory their third-party service providers, would have meaningful benefits at the individual covered entity-level, as well as for customers and counterparties and the derivatives markets at large. Given their roles and interconnectedness in the derivatives markets, an operational shock at one covered entity can have ripple effects across the markets. Requiring covered entities to develop and maintain a program to help evaluate and address the risk at each stage of the third-party relationship—from before selecting a third-party service provider to how such a relationship would be supervised and terminated—may not only help covered entities be more fully aware of and manage the risks of their third-party relationships, it could also help increase overall confidence levels in the derivatives markets by ensuring customers and counterparties that there is a foundational level of third-party risk management practices across covered entities.

Additionally, the proposed rule could operate to raise minimum standards with regards to how third-party risks are managed, by introducing enhanced due diligence or monitoring practices for critical third-party service providers, for instance, which could lead to real and measurable reduction in risk to the financial system. The act of creating an inventory of third-party service providers would also help increase the likelihood of identifying interdependencies or overdependencies, which could cause covered entities to reevaluate particular relationships (*i.e.,* diversify third-party service providers to reduce concentration risk) or take on additional activities (*e.g.,* insurance) to help mitigate those risks, thereby promoting operational resilience. Identifying critical third-party service providers should also help enhance operational awareness of those entities and ensure they receive the required heightened monitoring to ensure that the risk of disruption to critical services, which could have a broader impact on the markets or customers and counterparties, is mitigated.

i. Business Continuity and Disaster Recovery Plan—Proposed Paragraph (f)

The proposed rule would require covered entities to have a BCDR plan, defined as a written plan outlining the procedures to be followed in the event of an emergency or other significant disruption to the continuity of normal business operations and that meets certain requirements.[352] This would be a new CFTC requirement for FCMs, but current Commission regulation 23.603 imposes a BCDR plan requirement on swap entities that is substantially similar to the proposed rule, as the proposed rule was modeled after the current BCDR requirement for swap entities with certain modifications.[353] Additionally, although the CFTC does not currently impose a BCDR plan requirement on FCMs, NFA and CME do, which the Commission believes should help FCMs mitigate the costs of establishing a BCDR plan for purposes of complying with the proposed rule, particularly since some of the amendments to the current BCDR plan requirement for swap entities have the effect of further aligning the regulatory

[348] *See* NFA Third-Party Notice, *supra* note 43.

[349] *See* 12 CFR part 30, app. B, III.D. (Oversee Service Provider Arrangements); Prudential Third-Party Guidance, *supra* note 43.

[350] *See* NFA Third-Party Notice, *supra* note 43.

[351] *See* paragraph (a) of proposed Commission regulations 1.13 and 23.603 (defining ''critical third-party service provider'').

[352] *See* paragraphs (a) (defining ''business continuity and disaster recovery plan'') and (b)(2) (components) of proposed Commission regulation 1.13 and 23.603.

[353] *See* 17 CFR 23.603.

text with NFA and CME BCDR plan requirements.[354]

The proposed rule would require covered entities' BCDR plans to be reasonably designed to enable the covered entities to continue or resume any activities as a covered entity with minimal disruption to counterparties, customers, and the markets, and to recover and make use of covered information, as well as any other data, information, or documentation required to be maintained by law and regulation.[355] The proposed rule would further require the BCDR plans to include certain minimum contents, including: identifying and backing up required information; identifying and developing backups for required resources, including technology, facilities, and staff; identifying potential disruptions to critical third-party service providers; identifying implicated personnel; and establishing a communication plan.[356]

To design a BCDR plan that meets that standard, covered entities would need to expend resources to establish and preserve backup resources (staffing, technology, inputs) for use in the event of the BCDR plan's activation, and to create backups of the information the BCDR plan would cover. Depending on the size and complexity of a particular covered entity's business, those costs could be sizeable, as they may require negotiating and entering into new contracts with backup resource providers, or other third-party service providers. Covered entities would also need to expend resources to establish a plan to minimize the impact of disruptions and establish a communication plan, which would include identifying implicated persons and bodies and establishing potential contacts, methods, modes, and priorities of communication. Finally, the resources to document all of this work in the plan would likely be more than simply ministerial effort, as staff would likely have to spend time working through various deliberative points, at least at the outset in first developing the BCDR plan. The costs to maintaining the plan would likely be reduced compared to the initial fixed costs, however, as the plan put into action over time.

Nevertheless, the Commission expects that most covered entities have already incurred at least some of these potential costs by virtue of either the existing CFTC BCDR plan requirements for swap entities, or the NFA and CME BCDR plan requirements applicable to FCMs. Notably, the ''essential elements'' of NFA's BCDR Notice aligns closely with the minimum requirements for the Commission's proposed BCDR plan requirement, requiring FCMs to establish backups in one more reasonably separate geographic areas, to backup or copy essential documents and data and store them off-site, to consider the impact of interruptions by third-parties and ways to minimize the impact, and to develop a communication plan.[357] Accordingly, although the Commission expects FCMs would incur at least some costs reviewing their BCDR plans to ensure they meet the proposed CFTC requirements, the Commission preliminarily believes most FCMs would be able to avoid the more substantial initial costs of developing a BCDR plan from scratch.

The Commission further believes that the expenditure of resources required to create the proposed plan would help give the derivatives markets and customers and/or counterparties confidence that covered entities' operations would be able to be quickly reestablished following an emergency or significant disruption, improving the overall resilience of the market and perhaps lowering customer/counterparty risk and its associated costs. Having a plan that centralizes key information related to an emergency—including identifying core information, personnel, systems, and resources needed to resume operations—should also help facilitate covered entities in achieving the recovery time objective of being back up and running with minimal disruption to counterparties, customers, and the derivatives markets, supporting market confidence and reducing overall systemic risk. Maintaining copies of the plan in accessible off-site locations should impose no more than ministerial costs and would help ensure that covered entities can access the plan in a crisis.

The proposed rule would amend the current BCDR plan requirement for swap entities in a few ways, some of which the Commission expects would have cost-benefit implications.[358] For instance, the proposed rule would require covered entities to ''recover and make use of all covered information, as well as any other data, information, or documentation required to be maintained by law and regulation,'' which expands the information BCDR plans would be required to cover beyond that required to be maintained by applicable law and regulation, and makes clear the information should not only be recovered but also accessible and still useable.[359] Depending on current BCDR plan practices by swap entities, the proposal could potentially cause covered entities to expand the sources of information they need to backup and/or augment their backup systems to ensure the information stored there is useable. The proposed rule would also no longer require swap entities to ensure their BCDR plans are designed to enable swap entities to continue or resume operations ''by the next business day.'' [360] Although the Commission does not believe that this change would have an impact on the actual recovery time of swap entities following an emergency or other significant disruption, given that both current Commission regulation 23.603 and the proposed rule require that the BCDR plan be designed to ensure recovery with minimal disruption to counterparties and the market, swap entities could need to dedicate at least some staff time to review their BCDR plans to ensure that they continue to meet the rule requirements.

j. Training and Distribution—Proposed Paragraph (g)

The proposed rule would require covered entities to establish, implement, and maintain training with respect to the ORF, including general cybersecurity awareness training and role-specific training for personnel involved in the ORF.[361] If the proposed rule is adopted, covered entities would need to expend resources to develop and/or evaluate and acquire externally sourced training. Those outlays would include the costs associated with establishing the training at the outset, as well as ongoing costs associated with updating and providing the training at least every year.[362] There would also be administrative costs associated with distributing copies of the component programs or plan to relevant personnel and providing them with any significant revisions.[363] Nevertheless, the

[354] *See* NFA Rule 3–38, *supra* note 43; CME Rule 983, *supra* note 185.

[355] *See* paragraph (f)(1) of proposed Commission regulation 1.13 and 23.603.

[356] *See* paragraph (f)(2) of proposed Commission regulation 1.13 and 23.603.

[357] *See* NFA BCDR Notice, *supra* note 43.

[358] As with the other sections of this notice, portions of the BCDR plan requirement for swap entities in current Commission regulation 23.603 that have been expanded in the proposal to apply to the ORF more broadly, notably testing, are discussed in the context of the discussion of those specific requirements.

[359] *See* 17 CFR 23.603(a).

[360] *Id.*

[361] *See* paragraph (g)(1) of proposed Commission regulations 1.13 and 23.603.

[362] *See* paragraph (g)(2) of proposed Commission regulations 1.13 and 23.603

[363] *See* paragraph (g)(3) of proposed Commission regulations 1.13 and 23.603.

Commission believes that establishing, implementing, and maintaining a training program is crucial to realizing the benefits of the proposed ORF. Not only would it help ensure that employees of covered entities are kept aware of good cyber hygiene practices, which should reduce the potential for covered information to be compromised and customers and counterparties to be negatively impacted, training would help ensure that the ORF practices covered entities establish are accurately implemented and maintained by the personnel tasked with operationalizing the ORF. Although allowing covered entities to provide training less frequently than annually would reduce compliance costs for covered entities, the Commission believes that annual training is needed to preserve its benefits given the rapidly evolving pace of technology and the potential for human error to result in actual harm to operations or even customers or counterparties.[364]

k. Reviews and Testing—Proposed Paragraph (h)

The proposed rule would require covered entities to establish, implement, and maintain a plan reasonably designed to assess adherence to, and the effectiveness of, their ORF through regular reviews and risk-based testing.[365] At the outset, covered entities would need to dedicate staff resources to develop a review and testing plan for the ORF; ongoing staff resources would be needed to conduct reviews at least annually and risk-based testing at a frequency that is appropriate and proportionate to each covered entity's nature, size, scope, complexity, and risk profile, following generally accepted standards and best practices.[366] Covered entities would further assume regular costs associated with documenting the reviews and testing (*e.g.,* results of testing, assessment of effectiveness, recommendations for modifications/improvements/corrective actions) and reporting on them to the CCO and any other relevant senior-level official(s) and oversight body(ies).[367] In general, the ongoing costs of the required testing and reviews are likely to vary by covered entity, with larger, more complicated covered entities likely expending significantly more resources to conduct testing consistent with the proposed (b)(3) standard.[368]

With respect to the reviews of the ORF, the proposed rule would require that they be conducted at least annually and in connection with any material change that is reasonably likely to affect the risks addressed by the ORF. The proposed rule would further require the reviews to include an analysis of adherence to, and the effectiveness of the ORF, as well as any recommendations for improvements.[369] This standard is generally consistent with, and would replace, the current review standard in current Commission regulation 23.603 for swap entity BCDR plans, such that associated costs for reviewing the BCDR plan should not be affected by the proposal.[370] NFA's ISSP Notice and BCDR Notice also require NFA members to review their ISSPs or BCDR pans on a regular or periodic basis.[371] Accordingly, while covered entities may experience some staffing costs in assuring their reviews are at least annual, costs associated with establishing a review process more broadly should have already been realized by most covered entities.

For testing, the proposed rule would generally require that its frequency, nature, and scope would be determined consistent with the proposed (b)(3) standard.[372] The Commission believes that such a risk-based standard would allow covered entities to tailor testing to their unique business and risk profile, focusing testing efforts on areas that would be the most impactful or revealing and avoiding unnecessary costs. Nevertheless, with respect to testing of the information and technology security program, the proposed rule would require covered entities to assume costs for some specific testing, including testing of key controls and the incident response plan, as well as daily or continuous vulnerability assessments and penetration testing at least annually.[373] Although regular testing of key controls and the incident response plan is likely to require time and staff resources, the Commission believes that without testing, it would be impossible for covered entities to know whether the controls are functioning to mitigate risk as expected, and for the incident response plan to be actionable in times of emergency. Daily or continuous vulnerability assessments and penetration testing at least annually could require additional staff and technology outlays.[374] The exact cost of testing as realized by each covered entity, however, is likely to vary depending on the scope and complexity of its operations, and the degree to which it has already incorporated vulnerability assessments and penetration testing as part of its ISSP.[375]

The Commission believes that vulnerability assessments and penetration testing are essential for covered entities to know what their vulnerabilities are and how they might be exploited, so they can take steps to mitigate associated risks, including by adapting internal controls, which are a key component of preserving operational resilience. Given the dynamic, ever changing nature of technology and cybersecurity, the Commission believes that continual and active action and engagement are necessary to ensure controls are operating as intended, and for covered entities to have an accurate assessment of the risks to their covered information and technology. By not mandating specific types of penetration testing, however, the Commission believes the proposed rule is adapted to allow the wide range of covered entities subject to the proposed rule to adopt types of testing that are recommended for and best fit their unique circumstances, so as to achieve the highest level of improved cybersecurity without incurring unnecessary costs. The Commission further believes such testing is essential cyber hygiene and their use among covered entities would help ensure a base level of monitoring in the derivatives markets that is readily accessible.

[364] *See supra* note 18 and accompanying text.

[365] *See* paragraph (h) of proposed Commission regulations 1.13 and 23.603.

[366] *See* paragraph (b)(3) of proposed Commission regulations 1.13 and 23.603.

[367] *See* paragraphs (h)(4) and (h)(5) of proposed Commission regulations 1.13 and 23.603.

[368] The Commission estimates, on average, that covered entities will incur an initial annual cost of $8,000 (80 hours × $100/hour) to establish a plan to assess adherence to, and the effectiveness of, its ORF, and to document all reviews and testing of the ORF, or an estimated aggregate dollar cost of $1,280,000 (160 covered entities × $8,000).

[369] *See* paragraph (h)(1) of proposed Commission regulations 1.13 and 23.603

[370] *See* 17 CFR 23.603(f) (''A member of the senior management of each swap dealer and major swap participant shall review the business continuity and disaster recovery plan annually or upon any material change to the business. Any deficiencies found or corrective action taken shall be documented.'')

[371] *See* NFA BCDR Notice, *supra* note 43; NFA ISSP Notice, *supra* note 43.

[372] *See* paragraph (h)(2) of proposed Commission regulations 1.13 and 23.603.

[373] *See* paragraph (h)(2)(i) of proposed Commission regulations 1.13 and 23.603.

[374] CISA makes available a free vulnerability scanner, *see supra* note 248.

[375] The NFA ISSP Notice provides that a member ''may include penetration testing of the firm's systems, the scope and timing of which is highly dependent upon the Member's size, business, technology, its electronic interconnectivity with other entities and the potential threats identified in its risk assessment.'' *See* NFA ISSP Notice, *supra* note 43.

With respect to testing of the BCDR plan, the proposed rule would require covered entities to dedicate time and staff resources to conduct a walk-through or tabletop exercise designed to test the effectiveness of backup facilities and capabilities at least annually, which could involve outreach to operators of backup facilities.[376] Such a periodic effort would likely consume staff time and resources to put into place, including potentially in designing tabletop exercise scenarios. The Commission expects that this aspect of the proposed rule would not have any cost impact on swap entities, as current 23.603 requires annual testing of their BCDR plan, and the Commission does not believe the clarification that the testing be a walk-through or tabletop exercise would have substantive effect.

Because the proposed rule would require the reviews and testing to be conducted by qualified personnel who are independent of the aspect of the ORF being reviewed or tested, the Commission anticipates this work would either be conducted by internal compliance audit staff, external independent auditors, or other internal staff, provided they were not involved in creating the ORF component being tested.[377] Accordingly, this independence requirement could require covered entities to reassign duties or secure additional staffing resources, either of which would impose some additional costs.

Nevertheless, the Commission believes that annual reviews and testing are essential to ensuring that the ORF is operating as intended, and thus to ensuring the intended and expected benefits of the ORF with respect to protecting customers and mitigating systemic risk are actually realized. Without proper review and testing, determining whether the intended benefits of the ORF are being achieved would not be possible. Although eliminating the independence requirement could alleviate some potential staffing burdens on covered entities, the Commission believes that independence in reviews and testing is critical to preserving their benefits by helping to ensure that the results are reliable and unbiased. The Commission further believes that by allowing covered entities to adjust the frequency, nature, and scope of their risk-based testing of the ORF in a manner that is appropriate and proportionate to the circumstances, following generally accepted standards and best practices, the proposed rule would ensure that costs of the rule would be as well tailored to the covered entity as possible to realize benefits at the least cost.

With respect to the BCDR plan requirement for swap entities in particular, the Commission believes the proposed rule could reduce review and testing costs. First, it would eliminate costs associated with securing an independent auditor to audit the plan every three years.[378] Although there may be some benefits to having an independent audit of a BCDR plan, including having an external party with fresh eyes identify issues and potential improvements that might not be readily apparent to internal staff, the Commission preliminarily believes, based on its experience, that the internal reviews and testing of the BCDR plan are sufficient to achieve iterative improvements to the BCDR plan, making the costs associated with the independent audit unnecessary. Second, the proposed rule would eliminate the separate requirement that a member of senior management for a swap entity review the BCDR plan annually or upon any material change to the business and to document any deficiencies found or corrective action taken.[379] While the proposed rule would retain the annual review requirement for the BCDR plan, not requiring the review to be undertaken by a member of senior management may result in at least some burden reduction for senior management.

l. Notification Provisions—Proposed Paragraphs (i) and (j)

The proposed rule would require covered entities to provide certain notifications to either the Commission or affected customers or counterparties.[380] Notifications to the Commission, made electronically via email, would relate either to the covered entity's determination to activate the BCDR plan, or an ''incident,'' as defined in the proposed rule, that adversely impacts, or is reasonably likely to adversely impact information and technology security, the covered entity's ability to operate, or the assets or positions of a customer or counterparty.[381] In both cases, the notifications to the Commission would be intended to function as early warnings and thus would not need to be complete or detailed. Understanding that the information available to covered entities would be preliminary and incomplete at the time of the notification, the Commission would not expect covered entities to expend considerable resources to assemble notifications that are perfectly accurate and complete. Rather, the proposed rule would only require that the information provided to the Commission would be whatever the covered entity has available at the time that could assist the Commission in its oversight or response, with the understanding that resources should predominantly be directed at mitigating and recovering from the incident, emergency, or significant disruption.[382] Prioritizing an early warning over complete information should not only reduce the costs for covered entities in delivering the notification, but also allow the Commission the best opportunity to take quick responsive action, if appropriate.

Accordingly, while the Commission recognizes that there would be at least some information gathering and administrative costs associated with providing the notice, the Commission does not intend or expect the resource burden for providing the notification to be significant.[383] This limited early-warning function for the notice requirement is further supported by the relatively brief 24-hour time period for providing the notices.[384]

With respect to the BCDR plan in particular, the Commission does not believe covered entities would expend significant resources to notify the Commission, since the notification trigger (activation of the BCDR plan) is relatively bright-line. The Commission recognizes that with respect to the incident notification, however, covered entities may need to engage in some deliberation to determine whether an incident has or is reasonably likely to have an adverse impact, which would consume some staff resources. Preliminarily, the Commission estimates that covered entities activating their BCDR plan would incur a cost of $1000 (10 hours × $100/hour) to notify the Commission, or an estimated aggregate dollar cost of $160,000 (160 covered entities × $1,000). The Commission believes, however, that these costs may go down over time, as covered entities

[376] *See* paragraph (h)(2)(i) of proposed Commission regulations 1.13 and 23.603.

[377] *See* proposed paragraph (h)(3) of proposed Commission regulations 1.13 and 23.603.

[378] *See* 17 CFR 23.603(g).

[379] *See* 17 CFR 23.603(f).

[380] *See* paragraphs (i) and (j) of proposed Commission regulations 1.13 and 23.603.

[381] *See* paragraph (i) of proposed Commission regulations 1.13 and 23.603.

[382] *See* paragraphs (i)(1)(ii) and (i)(2)(ii) of proposed Commission regulations 1.13 and 23.603.

[383] The Commission estimates that for each ''incident'' requiring notification, covered entities will incur a cost of $1,000 (10 hours × $100/hour) to gather the information required and to provide notification to the Commission, or an estimated aggregate dollar cost of $160,000 (160 covered entities × $1,000).

[384] *See* paragraphs (i)(1)(iii) and (i)(2)(iii) of proposed Commission regulations 1.13 and 23.603.

gain familiarity in applying the notification provision. The Commission also preliminarily believes that an adverse impact standard would be potentially easier to apply than one that included a materiality limiter, which could introduce further need for interpretation and internal deliberation for covered entities to determine whether the impact is ''material'' or ''significant.'' Additionally, scoping notifications to incidents with a likely adverse impact and to BCDR activation would help focus the Commission's oversight activities and responsive efforts on cases where it could act to support the derivatives markets and customers and counterparties, potentially reducing the potential for ripple effects.

In addition to notifications to the Commission, the proposed rule would require covered entities to notify affected customers or counterparties as soon as possible of any incident that is reasonably likely to have adversely affected the confidentiality or integrity of their covered information, assets, or positions.[385] Because the rule does not contain a specific timing limit for providing this notification, the Commission does not expect that this notification requirement would cause covered entities to need to divert any resources while managing the incident to draft the notification. Rather, the Commission expects that most of the costs associated with this notification requirement would be in spending the necessary staff resources to gather and report facts as accurately as possible to aid affected customers and counterparties in understanding and assessing the potential impact of the incident on their information, assets, or positions and to take any necessary action.[386] Covered entities may also need to dedicate staff resources to interacting with customers or counterparties after the notification is given to provide more information or answer questions. The Commission estimates that for each ''incident'' requiring notification, covered entities will incur a cost of $5,000 (50 hours × $100/hour) to gather the required information necessary to provide notice to customers or counterparties and to prepare and deliver the required notification, or an estimated aggregate dollar cost of $800,000 (160 covered entities × $5,000). The Commission believes that this notification could produce substantial benefits to customers and counterparties, especially where state or other federal law does not otherwise require such notifications, as they would give customers and counterparties the information they would need to further protect their information and assets and allow them to seek other avenues of redress.

m. Emergency Contacts and Recordkeeping—Proposed Paragraphs (k) and (l)

The proposed rule would require covered entities to provide the Commission with the name and contact information of employees in connection with incidents triggering notification to the Commission and in connection with the activation of the covered entity's BCDR plan.[387] The identified employees would need to be authorized to make key decisions on behalf of the covered entity and have knowledge of the covered entity's incident response plan or BCDR plan, as appropriate.[388] Covered entities would also need to update their contacts with the Commission, as necessary.[389] The Commission believes that ensuring it has knowledgeable contacts with whom to direct communications during a crisis would aid the Commission's ability to take any necessary responsive action, and that the costs associated with identifying and updating the appropriate contacts would be ministerial in nature.[390] With respect to BCDR plan emergency contacts for swap entities, the proposed rule is identical in substance to current Commission regulation 23.603, such that it should impose no additional costs on swap entities.[391]

The proposed rule would also further require covered entities to maintain all records required to be maintained pursuant to this section in accordance with Commission regulation 1.31, and make them available promptly upon request to representatives of the Commission and to representatives of applicable prudential regulators.[392] Covered entities would incur costs associated with maintaining a recordkeeping system that allows for easy records retrieval, which would require both staff resources and likely reliance on electronic recordkeeping systems. The Commission believes these costs are likely mitigated for most covered entities, as they would be able to rely on existing recordkeeping systems designed to maintain other records in accordance with Commission regulation 1.31, and proper recordkeeping would help covered entities demonstrate compliance with the ORF rule, and ensure their ORFs are operating as expected as they conduct required reviews and testing.

2. Section 15(a) Factors

a. Protection of Market Participants and the Public

The Commission believes the proposed rule would support protection of market participants and the public. The Commission preliminarily believes the proposed rule will help protect market participants and the public by increasing the operational resiliency of covered entities to disruptions caused by natural disasters, cyber-attacks, and failures at third-party service providers. As covered entities are responsible for safeguarding customers' accounts, executing trades, maintaining records, and reporting to relevant agencies, their operational resiliency will mitigate the negative impact on customers, clients, and counterparties in case of an incident. The proposed rule may also help reduce the likelihood of an incident due to proposed proactive measures such as penetration and vulnerability testing and cyber security training. For market participants and the public more generally, the benefits include enhanced market protection against the spread of contagion risk to the financial system from operational risks.

b. Efficiency, Competitiveness, and Financial Integrity of Markets

The Commission believes the proposed rule would enhance the financial integrity of CFTC-regulated derivatives markets. SDs, MSPs, and FCMs are essential intermediaries in the financial markets regulated by the Commission. Due to the interconnectedness of markets, disruptions to the business operations of these intermediaries pose risks to other markets. The Commission believes that increasing and helping to ensure the operational resiliency of these covered entities would help improve the financial integrity of the derivatives markets. The proposed rule's requirement to report to the Commission incidents and BCDR plan

[385] *See* paragraph (j)(1) of proposed Commission regulations 1.13 and 23.603.

[386] *See* paragraph (j)(2) of proposed Commission regulations 1.13 and 23.603.

[387] *See* paragraph (k)(1) of proposed Commission regulations 1.13 and 23.603.

[388] *See* paragraph (k)(2) of proposed Commission regulations 1.13 and 23.603.

[389] *See* paragraph (k)(3) of proposed Commission regulations 1.13 and 23.603.

[390] The Commission estimates that covered entities will incur a cost of $100 (1 hour × $100/hour) to provide the Commission with emergency contact information, or an estimated aggregate dollar cost of $16,000 (160 covered entities × $100).

[391] *See* 17 CFR 23.603(3).

[392] *See* paragraph (l) of proposed Commission regulations 1.13 and 23.603.

activation would assist the Commission effectuate a timely response to business disruptions, which will help mitigate the impact on other market participants and promote financial stability and confidence. Additionally, to the degree that the proposed rule aligns with other existing applicable requirements, including NFA rules and interpretive notices, and incorporates generally accepted standards and best practices currently broadly relied on by covered entities, the proposed rule would support regulatory convergence and the efficiencies that may generate.

c. Price Discovery

The Commission does not anticipate the proposed rule directly impacting the price discovery process. Nevertheless, if a trading disruption would be prevented or shortened by this proposed rulemaking, then price discovery would be improved.

d. Sound Risk Management Practices

The Commission believes the proposed rule would promote the development of sound risk management practices among covered entities. Programs, plans, policies, and procedures are required for operational risks, which now explicitly include cybersecurity and third-party risks that adhere to current best practices. These processes seek to help covered entities identify, protect, detect, respond, and recover from such risks. As such, the operational risk management processes of covered entities may be improved.

e. Other Public Interest Considerations

The proposed rule relies on and incorporates aspects of existing standards and practices developed by other regulators and standard-setting bodies, including NFA rules and interpretive notices; prudential rules and guidance; and NIST, ISO, FFIEC and other sources of cyber and operational resilience standards. Accordingly, the proposed rule should support the development of further convergence in the area of operational resilience and allow covered entities to develop ORFs that are adaptive and responsive to rapidly changing circumstances and technology, which the Commission believes could lead to better protection of markets against the spread of contagion risks to the financial system from operational risks, in general.

3. Request for Comments

As noted, the Commission invites public comment on all aspects of its cost-benefit consideration, including, but not limited to the baseline and the identification and measurement of costs and benefits relative to it; the identification, measurement, and assessment of any costs and benefits not discussed herein; whether the Commission has misidentified any costs or benefits; what, if any, alternatives would be more reasonable in terms of their costs and benefits; and the Section 15(a) factors described above. The Commission asks that commenters explain and support the reasons for positions asserted in their comment letters and, further, include in them any data or other information that they may have to assist the Commission's ability to better quantify the costs and benefits of the Proposal.

1. Has the Commission misidentified any costs or benefits? If so, please explain.

2. Please explain whether compliance costs would increase or decrease as a result the proposed rule. Please provide all quantitative and qualitative costs, including, but not limited to personnel costs and technological costs.

3. The Commission seeks additional information on the costs and benefits of the proposed rule's requirement for covered entities to have a governance regime for their ORF, including risk appetite and tolerance limits, consolidated programs or plans, and internal escalation policies. Specifically, to what extent do covered entities already have or plan to have relevant programs or plans, policies, and procedures compliant with those prescribed in the proposed rule? To what practical extent do NFA's requirements, prudential regulation and/or best practices currently duplicate or differ from the ORF governance regime, including risk appetite limits, consolidated programs or plans, and internal escalation policies, being proposed? Will covered entities experience additional or lowered costs to comply with the proposed rule, and if so, to what degree?

4. The Commission seeks additional information regarding the costs and benefits of establishing an information and technology security program. Specifically, to what extent are covered entities already conducting comprehensive risk assessments that follow standards described in the proposed rule? Are these assessments being conducted on at least an annual basis? Do existing effective controls likewise meet the standards in the proposed rule? Will covered entities experience additional or lowered costs relative to current practice to establish, document, and maintain an incident response plan as called for in the proposed rule, and if so, to what degree?

5. The Commission seeks additional information regarding the costs and benefits of establishing a business continuity and disaster recovery plan. In particular, is the Commission's proposed rule different from current practice, and, if so, how? Would covered entities experience additional or lowered costs to comply with the proposed rule, and, if so, to what degree?

6. The Commission seeks additional information regarding the costs and benefits of the proposed rule's required notice of ORF events to the Commission. Will covered entities experience additional or lowered costs to comply with the proposed rule, and, if so, to what degree? Will compliance with the 24-hour cap for as-soon-as-possible notification entail additional costs relative to some shorter or longer cap and, if so, why and to what degree?

7. The Commission seeks additional information on the costs and benefits of the proposed rule's requirement that covered entities provide notification to customers and counterparties following an incident. In particular, is the Commission's proposed rule different from current practice, and, if so, how? Would covered entities experience additional or lowered costs to comply with the proposed rule, and, if so, to what degree?

8. The Commission seeks additional information regarding the costs and benefits of ORF review and testing. In particular, to what extent, if any, does the proposed rule differ from existing procedures? How do covered entities determine the amount of review and testing that is appropriate? Do all covered entities currently undertake penetration and vulnerability testing, and at what frequency? Would covered entities experience additional or lowered costs to comply with the proposed rule, and, if so, to what degree?

9. The Commission seeks additional information regarding the costs and benefits of the cross-border application of the proposed rule. Would added specificity in the proposed regulations improve the cost-benefit calculus for those covered entities impacted by their cost-benefit application? If so, in what areas would more specificity be helpful and how would costs and benefits be impacted?

D. Antitrust Laws

Section 15(b) of the CEA requires the Commission to ''take into consideration the public interest to be protected by the antitrust laws and endeavor to take the least anticompetitive means of achieving the purposes of the CEA, in

issuing any order or adopting any Commission rule or regulation (including any exemption under CEA section 4(c) or 4c(b)), or in requiring or approving any bylaw, rule, or regulation of a contract market or registered futures association established pursuant to section 17 of this Act.'' [393]

The Commission preliminarily believes that the public interest to be protected by the antitrust laws is generally to protect competition. The Commission invites comment on whether the proposed rule implicates any other specific public interest to be protected by the antitrust laws.

The Commission has also assessed the proposal for potential anticompetitive effects. To the extent that there are substantial fixed costs associated with improved operational risk management, there may be competitive implications, though likely anticompetitive impacts have not been identified. Smaller firms may bear a disproportionate cost relative to larger firms in total asset size due to this proposed rule. Nevertheless, smaller firms may be able to realize economies of scope and scale through outsourcing to third-parties, albeit at the cost of raising their third-party risk exposure. In addition, the proposed rule allows smaller firms to choose programs or plans, policies, and procedures that are appropriate to their businesses, further mitigating competitive concerns.

The Commission invites comment on its CEA section 15(b) assessment, including what other means, if any, would be more procompetitive than what the Commission now proposes and why.

List of Subjects

17 CFR Part 1

Brokers, Commodity futures, Consumer protection, Reporting and recordkeeping requirements.

17 CFR Part 23

Banks, Banking, Commodity futures, Reporting and recordkeeping requirements, Swaps.

For the reasons stated in the preamble, the Commodity Futures Trading Commission proposes to amend 17 CFR parts 1 and 23 as set forth below:

PART 1—GENERAL REGULATIONS UNDER THE COMMODITY EXCHANGE ACT

■ 1. The authority citation for part 1 continues to read as follows:

Authority: 7 U.S.C. 1a, 2, 5, 6, 6a, 6b, 6c, 6d, 6e, 6f, 6g, 6h, 6i, 6k, 6l, 6m, 6n, 6o, 6p, 6r, 6s, 7, 7a–1, 7a–2, 7b, 7b–3, 8, 9, 10a, 12, 12a, 12c, 13a, 13a–1, 16, 16a, 19, 21, 23, and 24 (2012).

■ 2. Add § 1.13 to read as follows:

§ 1.13 Operational Resilience Framework for Futures Commission Merchants

(a) *Definitions.* For purposes of this section:

Affiliate means, with respect to any person, a person controlling, controlled by, or under common control with, such person.

Business continuity and disaster recovery plan means a written plan outlining the procedures to be followed in the event of an emergency or other significant disruption to the continuity of normal business operations and that meets the requirements of paragraph (f) of this section.

Consolidated program or plan means any information and technology security program, third-party relationship program, or business continuity and disaster recovery plan in which the futures commission merchant participates with one or more affiliates and that is managed and approved at the enterprise level.

Covered information means any sensitive or confidential data or information maintained by a futures commission merchant in connection with its business activities as a futures commission merchant.

Covered technology means any application, device, information technology asset, network service, system, and other information-handling component, including the operating environment, that is used by a futures commission merchant to conduct its business activities, or to meet its regulatory obligations, as a futures commission merchant.

Critical third-party service provider means a third-party service provider, the disruption of whose performance would be reasonably likely to:

(i) Significantly disrupt a futures commission merchant's business operations as a futures commission merchant; or

(ii) Significantly and adversely impact the futures commission merchant's customers.

Information and technology security means the preservation of:

(i) The confidentiality, integrity, and availability of covered information; and

(ii) The reliability, security, capacity, and resilience of covered technology.

Incident means any event, occurrence, or circumstance that could jeopardize information and technology security, including if it occurs at a third-party service provider.

Information and technology security program means a written program reasonably designed to identify, monitor, manage, and assess risks relating to information and technology security and that meets the requirements of paragraph (d) of this section.

Key controls mean controls that an appropriate risk analysis determines are either critically important for effective information and technology security or intended to address risks that evolve or change more frequently and therefore require more frequent review to ensure their continuing effectiveness in addressing such risks.

Oversight body means any board, body, or committee of a board or body of the futures commission merchant specifically granted the authority and responsibility for making strategic decisions, setting objectives and overall direction, implementing policies and procedures, or overseeing the implementation of operations for the futures commission merchant.

Risk appetite means the aggregate amount of risk a futures commission merchant is willing to assume to achieve its strategic objectives.

Risk tolerance limit means the amount of risk, beyond its risk appetite, that a futures commission merchant is prepared to tolerate through mitigating actions.

Senior officer means the chief executive officer or other equivalent officer of the futures commission merchant.

Third-party relationship program means a written program reasonably designed to identify, monitor, manage, and assess risks relating to third-party relationships and that meets the requirements of paragraph (e) of this section.

(b) *Generally.* (1) *Purpose and scope.* Each futures commission merchant shall establish, document, implement, and maintain an Operational Resilience Framework reasonably designed to identify, monitor, manage, and assess risks relating to:

(i) information and technology security;

(ii) third-party relationships; and

(iii) emergencies or other significant disruptions to the continuity of normal business operations as a futures commission merchant.

(2) *Components.* The Operational Resilience Framework shall include an information and technology security program, a third-party relationship program, and a business continuity and disaster recovery plan. Each component program or plan shall be supported by written policies and procedures.

(3) *Standard.* The Operational Resilience Framework shall be

[393] 7 U.S.C. 19(b).

appropriate and proportionate to the nature, size, scope, complexity, and risk profile of its business activities as a futures commission merchant, following generally accepted standards and best practices.

(c) *Governance.* (1) *Approval of components.* Each component program or plan required by paragraph (b)(2) of this section shall be approved in writing, on at least an annual basis, by either the senior officer, an oversight body, or a senior-level official of the futures commission merchant.

(2) *Risk appetite and risk tolerance limits.* (i) Each futures commission merchant shall establish and implement appropriate risk appetite and risk tolerance limits with respect to the risk areas identified in paragraph (b)(1) of this section.

(ii) The risk appetite and risk tolerance limits established pursuant to paragraph (c)(2)(i) of this section shall be reviewed and approved in writing on at least an annual basis by either the senior officer, an oversight body, or a senior-level official of the futures commission merchant.

(3) *Internal escalations.* The senior officer, an oversight body, or a senior-level official of the futures commission merchant shall be notified of:

(i) circumstances that exceed risk tolerance limits established and approved pursuant to paragraph (c)(2)(i) of this section; and

(ii) incidents that require notification pursuant to paragraphs (i) or (j) of this section.

(4) *Futures commission merchants forming part of a larger enterprise.* (i) *Generally.* A futures commission merchant may satisfy the requirements of paragraph (b)(2) of this section through its participation in a consolidated program or plan, provided that each consolidated program or plan meets the requirements of this section.

(ii) *Attestation.* A futures commission merchant that relies on a consolidated program or plan pursuant to paragraph (c)(4)(i) of this section may satisfy the requirements in paragraphs (c)(1) and (c)(2)(ii) of this section provided that either the senior officer, an oversight body, or a senior-level official of the futures commission merchant attests in writing, on at least an annual basis, that the consolidated program or plan meets the requirements of this section and reflects a risk appetite and risk tolerance limits appropriate to the futures commission merchant.

(d) *Information and technology security program.* (1) Risk assessment.

(i) The information and technology security program shall require the futures commission merchant to conduct and document the results of a comprehensive risk assessment reasonably designed to identify, assess, and prioritize risks to information and technology security.

(ii) Such risk assessment shall be conducted at a frequency consistent with the standard set forth in paragraph (b)(3) of this section, but at least annually, and be conducted by personnel not responsible for the development or implementation of covered technology or related controls.

(iii) The results of the risk assessment shall be provided to the oversight body, senior officer, or other senior-level official who approves the information and technology security program upon the risk assessment's completion.

(2) *Effective controls.* The information and technology security program shall require the futures commission merchant to establish, document, implement, and maintain controls reasonably designed to prevent, detect, and mitigate identified risks to information and technology security. Each futures commission merchant shall consider, at a minimum, the following types of controls and adopt those consistent with the standard set forth in paragraph (b)(3) of this section:

(i) Access 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;

(ii) Access restrictions designed to permit only authorized individuals to access physical locations containing covered information, including, but not limited to, buildings, computer facilities, and records storage facilities;

(iii) Encryption of electronic covered information, including while in transit or in storage on networks or systems, to which unauthorized individuals may have access;

(iv) Dual control procedures, segregation of duties, and background checks for employees or third-party service providers with responsibilities for or access to covered information;

(v) Change management practices, including defined roles and responsibilities, logging, and monitoring practices;

(vi) Systems development and configuration management practices, including practices for initializing, changing, testing, and monitoring configurations;

(vii) Flaw remediation, including vulnerability patching practices;

(viii) Measures to protect against destruction, loss, or damage of covered information due to potential environmental hazards, such as fire and water damage or technological failures;

(ix) Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into covered technology;

(x) Response programs that specify actions to be taken when the futures commission merchant suspects or detects that unauthorized individuals have gained access to covered technology, including appropriate reports to regulatory and law enforcement agencies; and

(xi) Measures to promptly recover and secure any compromised covered information.

(3) *Incident response plan.* The information and technology security program shall include a written incident response plan that is reasonably designed to detect, assess, contain, mitigate the impact of, and recover from an incident. This incident response plan shall include, at a minimum:

(i) The roles and responsibilities of the futures commission merchant's management, staff, and third-party service providers in responding to incidents;

(ii) Escalation protocols, including a requirement to timely inform the oversight body, senior officer, or other senior-level official that has primary responsibility for overseeing the information and technology security program; the chief compliance officer of the futures commission merchant; and any other relevant personnel of incidents that may significantly impact the futures commission merchant's regulatory obligations or require notification to the Commission;

(iii) The points of contact for external coordination of incident responses as determined necessary by the futures commission merchant based on the severity of incidents;

(iv) The required reporting of incidents, whether by internal policy, contract, or law, including as required in this section;

(v) Procedures for documenting incidents and managements' response; and

(vi) The remediation of weaknesses in information and technology security, controls, and training, if any.

(e) *Third-party relationship program.* (1) *Third-party relationship lifecycle stages.* The third-party relationship program shall describe how the futures commission merchant addresses the risks attendant to each stage of the third-party relationship lifecycle, including:

(i) Pre-selection risk assessment;

(ii) Due diligence of prospective third-party service providers;

(iii) Contractual negotiations;

(iv) Ongoing monitoring; and

(v) Termination, including preparations for planned and unplanned terminations.

(2) *Heightened duties for critical third-party service providers.* The third-party relationship program shall establish heightened due diligence practices for potential critical third-party service providers and heightened monitoring for critical third-party service providers.

(3) *Third-party service provider inventory.* As part of its third-party relationship program, each futures commission merchant shall create, maintain, and regularly update an inventory of third-party service providers the futures commission merchant has engaged to support its activities as a futures commission merchant, identifying whether each third-party service provider in the inventory is a critical third-party service provider.

(3) *Retention of responsibility.* Notwithstanding a futures commission merchant's determination to rely on a third-party service provider, each futures commission merchant remains responsible for meeting its obligations under the Act and Commission regulations.

(4) *Guidance on third-party relationship program.* For guidance outlining potential risks, considerations, and strategies for developing a third-party relationship program consistent with paragraph (e), see Appendix A to this part.

(f) *Business continuity and disaster recovery plan.* (1) *Purpose.* The business continuity and disaster recovery plan shall be reasonably designed to enable the futures commission merchant to:

(i) Continue or resume normal business operations with minimal disruption to customers and the markets; and

(ii) Recover and make use of covered information, as well as any other data, information, or documentation required to be maintained by law and regulation.

(2) *Minimum contents.* The business continuity and disaster recovery plan shall, at a minimum:

(i) Identify covered information, as well as any other data or information required to be maintained by law and regulation, and establish and implement procedures to backup or copy all such data and information with sufficient frequency to meet the requirements of this section, and to store such data and information off-site in either hard-copy or electronic format;

(ii) Identify any resources, including covered technology, facilities, infrastructure, personnel, and competencies, essential to the operations of the futures commission merchant or to fulfill the regulatory obligations of the futures commission merchant, and establish and maintain procedures and arrangements to provide for their backup in a manner that is sufficient to meet the requirements of this section. Such arrangements must provide for backups that are located in one or more areas that are geographically separate from the futures commission merchant's primary systems, facilities, infrastructure, and personnel, and may include the use of resources provided by third-party service providers;

(iii) Identify potential disruptions to critical third-party service providers and establish a plan to minimize the impact of such disruptions;

(iv) Identify supervisory personnel responsible for implementing each aspect of the business continuity and disaster recovery plan, including the emergency contacts required to be provided pursuant to paragraph (k) of this section; and

(v) Establish a plan for communicating with the following persons in the event of an emergency or other significant disruption, to the extent applicable: employees; customers; swap data repositories; execution facilities; trading facilities; clearing facilities; regulatory authorities; data, communications and infrastructure providers and other vendors; disaster recovery specialists; and other persons essential to the recovery of documentation and data, the resumption of operations, and compliance with the Act and Commission regulations.

(3) *Accessibility.* Each futures commission merchant shall maintain copies of its business continuity and disaster recovery plan at one or more accessible off-site locations.

(g) *Training and distribution.* (1) *Training.* Each futures commission merchant shall establish, implement, and maintain training with respect to all aspects of the Operational Resilience Framework, including, but not limited to:

(i) Cybersecurity awareness training for all personnel; and

(ii) Role-specific training for personnel involved in establishing, documenting, implementing, and maintaining the Operational Resilience Framework.

(2) *Frequency.* Each futures commission merchant shall provide and update the training required in paragraph (g)(1) as necessary, but no less frequently than annually.

(3) *Distribution.* Each futures commission merchant shall distribute copies of each component program or plan required by paragraph (b)(2) of this section to relevant personnel and promptly provide any significant revisions thereto.

(h) *Reviews and Testing.* Each futures commission merchant shall establish, implement, and maintain a plan reasonably designed to assess its adherence to, and the effectiveness of, its Operational Resilience Framework through regular reviews and risk-based testing.

(1) *Reviews.* Reviews of the Operational Resilience Framework shall be conducted at least annually and in connection with any material change to the activities or operations of the futures commission merchant that is reasonably likely to affect the risks identified in paragraph (b)(1) of this section. Reviews shall include an analysis of adherence to, and the effectiveness of, the Operational Resilience Framework and any recommendations for modifications or improvements that address root causes of any issues identified by the review.

(2) *Testing.* The frequency, nature, and scope of risk-based testing of the Operational Resilience Framework shall be determined by the futures commission merchant, consistent with the standard in paragraph (b)(3) of this section.

(i) Testing of the information and technology security program shall include, at a minimum:

(A) Testing of key controls and the incident response plan at least annually;

(B) Vulnerability assessments, including daily or continuous automated vulnerability scans; and

(C) Penetration testing at least annually.

(ii) Testing of the business continuity and disaster recovery plan shall include, at a minimum, a walk-through or tabletop exercise designed to test the effectiveness of backup facilities and capabilities at least annually.

(3) *Independence.* The reviews and testing shall be conducted by qualified personnel who are independent of the aspect of the Operational Resilience Framework being reviewed or tested.

(4) *Documentation.* Each futures commission merchant shall document all reviews and testing of the Operational Resilience Framework. The documentation shall, at a minimum, include:

(i) The date the review or testing was conducted;

(ii) The nature and scope of the review or testing, including methodologies employed;

(iii) The results of the review or testing, including any assessment of effectiveness;

(iv) Any identified deficiencies and recommendations for remediation; and

(v) Any corrective action(s) taken or initiated, including the date(s) such action(s) were taken.

(5) *Internal reporting.* Each futures commission merchant shall report on the results of its reviews and testing to the futures commission merchant's chief compliance officer and any other relevant senior-level official(s) and oversight body(ies).

(i) *Notifications to the Commission.* (1) *Incidents.* (i) *Notification trigger.* Each futures commission merchant shall 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 futures commission merchant to continue its business activities as a futures commission merchant; or

(C) the assets or positions of a customer of the futures commission merchant.

(ii) *Contents.* The notification shall provide any information available to the futures commission merchant at the time of notification that may assist the Commission in assessing and responding to the incident, including the date the incident was detected, possible cause(s) of the incident, its apparent or likely impacts, and any actions the futures commission merchant has taken or is taking to mitigate or recover from the incident, including measures to protect customers.

(iii) *Timing and method.* Each futures commission merchant shall provide the incident notification as soon as possible but in any event no later than 24 hours after such incident has been detected. The notification shall be provided via email to *ORFnotices@cftc.gov.*

(2) *Business continuity and disaster recovery plan activation.* (i) *Notification trigger.* Each futures commission merchant shall notify the Commission of any determination to activate the business continuity and disaster recovery plan.

(ii) *Contents.* The notification shall provide any information available to the futures commission merchant at the time of notification that may assist the Commission in assessing or responding to the emergency or disruption, including the date of the emergency or disruption, a description thereof, the possible cause(s), its apparent or likely impacts, and any actions the futures commission merchant has taken or is taking to mitigate or recover from the emergency or disruption, including measures taken or being taken to protect customers.

(iii) *Timing and method.* Each futures commission merchant shall provide the business continuity and disaster recovery plan activation notification within 24 hours of determining to activate the business continuity and disaster recovery plan. The notification shall be provided via email to *ORFnotices@cftc.gov.*

(j) *Notification of incidents to affected customers.* (1) *Notification trigger.* Each futures commission merchant shall notify a customer as soon as possible of any incident that is reasonably likely to have adversely affected the confidentiality or integrity of the customer's covered information, assets, or positions.

(2) *Contents.* The notification to affected customers shall include information necessary for the affected customer to understand and assess the potential impact of the incident on its information, assets, or positions, and to take any necessary action. Such notification shall include, at a minimum:

(i) a description of the incident;

(ii) the particular way in which the customer, or its covered information, may have been adversely impacted;

(iii) measures being taken by the futures commission merchant to protect against further harm; and

(iv) contact information for the futures commission merchant where the customer may learn more about the incident or ask questions.

(k) *Emergency Contacts.* (1) Each futures commission merchant shall provide the Commission the name and contact information of:

(i) two employees whom the Commission may contact in connection with incidents triggering notification to the Commission under paragraph (i)(1) of this section; and

(ii) two employees whom the Commission may contact in connection with the activation of the futures commission merchant's business continuity and disaster recovery plan triggering notification to the Commission under paragraph (i)(2) of this section.

(2) The identified employees shall be authorized to make key decisions on behalf of the futures commission merchant and have knowledge of the futures commission merchant's incident response plan or business continuity and disaster recovery plan, as appropriate.

(3) The futures commission merchant shall update its emergency contacts with the Commission as necessary.

(l) *Recordkeeping.* Each futures commission merchant shall maintain all records required to be maintained pursuant to this section in accordance with section 1.31 of this chapter and shall make them available promptly upon request to representatives of the Commission and to representatives of applicable prudential regulators, as defined in section 1a(39) of the Act.

■ 3. Add appendix A to part 1 to read as follows:

Appendix A to Part 1—Guidance on Third-Party Relationship Programs

The following guidance offers factors, actions, and strategies for futures commission merchants to consider in preparing and implementing third-party relationship programs reasonably designed to identify, monitor, manage, and assess risks relating to third-party relationships, as required by Commission regulation 1.13. The guidance is also not intended to reduce or replace the obligation of futures commission merchants to comply with the requirements in Commission regulation 1.13, including the requirement to ensure that each futures commission merchant's Operational Resilience Framework is appropriate and proportionate to the nature, size, scope, complexity, and risk profile of its business activities as a futures commission merchant, following generally accepted standards and best practices. The guidance is not exhaustive and is nonbinding.

The guidance is written to be broadly relevant to all futures commission merchants, but it may not be universally applicable. The degree to which the guidance would be applicable to a particular futures commission merchant would depend on its unique facts and circumstances and may vary from relationship to relationship. Each futures commission merchant should assess the relevance of the guidance as it applies to its particular risk profile and tailor its third-party relationship program accordingly.

Comparable guidance for swap dealers and major swap participants is included in Appendix A to subpart J of part 23 of the Commission's regulations.

A. Pre-Selection Risk Assessment—Commission Regulation 1.13(e)(1)(i)

Before entering into a third-party relationship, futures commission merchants should determine which services should be performed by a third-party and plan for how to manage associated risks. The Commission appreciates that reliance on third-party service providers may be unavoidable, particularly given the rapid pace of technological innovation, which may render it uneconomical or even infeasible for financial institutions to meet all of their technological needs in-house.

Nevertheless, given the risks associated with relying on third-party service providers, and that each additional third-party relationship a futures commission merchant

employs is likely to add further risk and complexity, a futures commission merchant's third-party relationship program should include a deliberative process for affirmatively determining whether to source a particular service from a third-party service provider. In determining whether a particular function should be performed by a third-party service provider, futures commission merchants should consider whether:

- The service would support the futures commission merchant's strategic goals and objectives.
- The same goals and objectives could be addressed through an alternative means that may not require reliance on a third-party service provider.
- The futures commission merchant has or could otherwise secure the resources, financial and otherwise, to effectively monitor the third-party service provider.
- Relevant and reputable third-party service providers are available.
- The provision of the service would implicate information and technology security concerns, including by requiring the third-party service provider to obtain access to covered information or provide covered technology.
- A disruption of the service would have a negative impact on customers or regulatory compliance.
- The relationship could be structured to reduce associated risks, such as by limiting the third-party service provider's access to covered information or covered technology.
- Lack of direct control over performance of the service would present unacceptable risk, *i.e.,* risk outside the futures commission merchant's risk tolerance limits.

As the above considerations illustrate, futures commission merchants should consider ways in which they might structure their third-party relationships to reduce the associated risks. For example, where giving a third-party service provider direct access to its technology or data may be outside a futures commission merchant's risk tolerance, structuring the relationship to provide the third-party service provider access on a read-only basis or via reports delivered by the futures commission merchants could render the relationship more acceptable. Futures commission merchants should therefore consider the availability of safer means of performing the service as part of their assessment.

Changes in technology, businesses practices, regulation, market structure, market participants (*e.g.,* new entrants to the market), or service delivery may change the risk profile of the third-party relationship over time. Accordingly, futures commission merchants should consider periodically reassessing their selection of services to be performed by third-party service providers. Futures commission merchants should stay abreast of these changes by monitoring the external environment and communicating with current and prospective service providers and other participants in industry.

B. Due Diligence in Selecting Third-Party Service Providers—Commission Regulation 1.13(e)(1)(ii)

After a futures commission merchant has determined that a service is suitable for a third-party to perform, it should conduct due diligence on prospective third-party service providers. Due diligence provides futures commission merchants with the information they need to assess and conclude, with a reasonable level of assurance, that the prospective third-party service provider is capable of effectively providing the service as expected, adhering to the futures commission merchant's policies, maintaining the futures commission merchant's compliance with Commission regulations, and protecting covered information. Appropriate due diligence should also enable futures commission merchants to evaluate whether they would be able to effectively monitor and manage the risks associated with a particular third-party relationship.

Due diligence may be conducted before or contemporaneously with contractual negotiations with prospective third-party service providers but should be concluded prior to executing any agreements. Futures commission merchants should conduct due diligence even in situations where, for a particular service, there may only be one or a small number of providers with a dominant market share whose services are used by all or most of the futures commission merchants' industry peers, and futures commission merchants should not rely solely on those providers' reputations or prior experience with them. The depth and rigor of the due diligence should be proportionate to the nature of the third-party relationship, with the required heightened due diligence for potential critical third-party service providers pursuant to Commission regulation 1.13(e)(2). Specifically, when conducting due diligence for a potential critical third-party servicer provider, futures commission merchants should expand the type and sources of information they rely on, the rigor and scrutiny they apply in reviewing the information to identify potential risks, and the level of confidence in their assessment of the third-party service provider's ability to perform.

When establishing their due diligence protocols, futures commission merchants should consider the full range of risks that reliance on the third-party service providers could introduce in light of the nature of the service they would be performing. Relevant considerations with respect to the potential third-party service provider include its:

- Financial condition, business experience and reputation, and business prospects, particularly the third-party service provider's experience providing services to financial institutions.
- Background, experience, and qualifications with respect to key personnel.
- Information and technology security practices, including incident reporting and incident management programs, and whether there are clearly documented processes for identifying and escalating incidents.
- Risk management practices, including governance, controls, testing, and issue management practices, as well as the results of any independent risk assessments.
- Regulatory environment, including the legal jurisdiction in which it is based and applicable regulatory or licensing requirements.
- History of disruptions to operations, including whether the third-party service provider has suffered incidents that would meet the standard for reporting to the Commission in Commission regulation 1.13(i).
- Violations of legal, compliance, or contractual obligations, including civil or criminal proceedings or administrative enforcement actions, including from self-regulatory organizations.
- Understanding of Commission regulatory requirements applicable to the futures commission merchant.
- Use of and reliance on subcontractors, including the volume and types of subcontracted activities, and the third-party service provider's process for identifying, assessing, managing, and monitoring associated risks.
- Business continuity and contingency plans.
- Financial protections, such as insurance coverage against losses or liabilities from intentional or negligent acts or hazards involving physical destruction and data or documentation losses.

Futures commission merchants should memorialize their assessment of these factors and identify how the review was heightened for critical third-party service providers. Futures commission merchants should not rely solely on their prior knowledge of or experience with a potential third-party. Potential sources of due diligence information include:

- Audit reports, including pooled audit plans and System and Organizational Controls (SOC) reports.
- Financial statements and projections and relevant accompanying information (*e.g.,* annual or quarterly reports, management commentary, auditors' opinions, and investor relations materials).
- Incident response plans, including the results of recent testing or assessments thereof.
- Business continuity and disaster recovery plans, as well as the result of recent testing or assessments thereof.
- Public filings.
- News reports, trade publications, and press releases.
- Reports from market intelligence providers.
- References from current or previous customers, or other parties which have had business relationships with the third-party service provider.
- Informal industry discussions.
- Information provided directly by the third-party service provider, such as internal performance metrics.

Obtaining and reviewing audit reports, including SOC reports, may be of particular value for conducting heightened due diligence of critical third-party service providers. In certain circumstances, futures commission merchants may not be able to gather all the information necessary to reach an informed conclusion that a prospective third-party service provider is an adequate provider. Examples include instances where the third-party service provider is a new entrant into the market and little information exists; where information provided by the

third-party service provider is insufficient or appears unreliable; or where the third-party service provider is reluctant to provide internal information. In such cases, the futures commission merchant should identify and document the limitations of its due diligence, the attendant risks, and any available methods for mitigating them (*e.g.,* obtaining alternate information, implementing enhanced monitoring or controls, negotiating protective contractual provisions). Ultimately, such factors could weigh against the use of the potential third-party service provider, particularly a potential critical third-party service provider. Futures commission merchants that proceed with the third-party service arrangements notwithstanding the limited due diligence should do so with caution, applying heightened scrutiny of the information they do receive, and consider the implementation of their own mitigating controls to compensate for the uncertainty.

C. Contractual Negotiations—Commission Regulation 1.13(e)(1)(iii)

After selecting a third-party service provider, futures commission merchants should proceed to finalizing the agreement, typically through entering into an enforceable written contract. Written contracts are an important tool for clarifying the scope of services to be delivered, establishing standards or performance benchmarks, allocating risks and responsibilities, and facilitating resolution of disputes. They can also reduce the risks of non-performance and assist in monitoring the third-party service provider. Because of their importance, the Commission recommends that futures commission merchants enter written agreements with third-party service providers before services are delivered, particularly with critical third-party service providers.

In negotiating a written contract, futures commission merchants should seek to negotiate contractual provisions that would support their ability to mitigate, manage, and monitor the risks associated with the relationship, as identified through their initial pre-selection and due diligence activities. The contractual provisions should be informed by the nature of the service provided and be proportionate to the criticality of the services provided. In particular, futures commission merchants should consider negotiating for the contract to include the following provisions:

- Timely notification to the futures commission merchant of any incidents suffered by third-party service providers, or of significant disruptions to the operations of the third-party service provider.
- Timely notification to the futures commission merchant of any material changes to the services provided.
- Required periodic, independent audits of the third-party service provider, the results of which would be shared with the futures commission merchant.
- Restrictions on the third-party service provider's use of the futures commission merchant's covered information, except as necessary to deliver the service or meet legal obligations.
- Security measures to protect the futures commission merchant's covered information and covered technology to which the third-party service provider has access.
- Insurance, guarantees, indemnification, and limitations on liability.
- Dispute resolution procedures.
- Performance measures or benchmarks.
- Remediation of identified performance issues.
- Dispute resolution procedures.
- Compliance with regulatory requirements, including reasonable assurances that the third-party service provider is willing and able to coordinate with the futures commission merchant for the purpose of ensuring the futures commission merchant complies with its legal and regulatory obligations.
- Use of subcontractors, including notification or approval procedures for their use, the extension of contractual rights of the futures commission merchant against the third-party service provider to its subcontractors, and contractual obligations for reporting on or oversight of subcontractors.
- Termination provisions, including rights to terminate following breaches of the third-party service provider's obligations, notice requirements, obligations of the third-party service provider to provide support for a successful transition, and the return or destruction of records or covered information, as further described in section E of this guidance.
- Information sharing necessary to facilitate other provisions of this proposed guidance (for example, reporting requirements to support ongoing monitoring, as discussed in section D of this guidance, or notice requirements for termination, as discussed in section E of this guidance).

These provisions focus on key risk factors generally associated with third-party service provider relationships. They are not exhaustive of all contractual provisions futures commission merchants should seek to include in their written contracts, including ordinary commercial contract terms (*e.g.,* choice of law provisions) and terms that may relate only to specific services, among other provisions. While third-parties may initially offer a standard contract, a futures commission merchant may seek to request modifications, additional contractual provisions, or addendums to satisfy its needs. Futures commission merchants should work to tailor the level of detail and comprehensiveness of the contractual provisions based on the risk and complexity posed by the particular third-party relationship, contracts with critical third-party service providers likely being the most tailored.

In some circumstances, a futures commission merchant may be at a bargaining power disadvantage, which prevents it from negotiating optimal contractual provisions. For example, a prospective third-party service provider may be the sole provider of a service or may have such dominant market share that it can offer its services on a ''take-it-or-leave-it'' basis. In such situations, the futures commission merchant should work to understand any resulting limitations in the contract and attendant risks and consider whether it can achieve outcomes comparable to those provided by contractual protections through non-contractual means. Examples could include the futures commission merchant implementing additional controls, augmenting its monitoring of the third-party service provider using public sources or market intelligence services, or purchasing insurance. The futures commission merchant should make an assessment, however, of whether these alternatives would provide an adequate substitute for the unobtained contractual protections and document its assessment and mitigation plan, considering its risk appetite and risk tolerance limits. Where a third-party service provider is unable or unwilling to agree to provisions necessary for the futures commission merchant to meet its obligations under Commission regulations, particularly a critical third-party service provider, the futures commission merchant should consider finding an alternative third-party service provider.

D. Ongoing Monitoring—Commission Regulation 1.13(e)(1)(iv)

After a third-party service provider has initiated performance, futures commission merchants should engage in ongoing monitoring. Ongoing monitoring is important to ensure the third-party service provider is properly carrying out its outsourced function and contractual obligations, as well as meeting quality or performance expectations. Effective monitoring can aid futures commission merchants in the early identification of performance deficits, allowing for a quicker response that may then mitigate the impact.

Ongoing monitoring should occur throughout the duration of a third-party relationship, commensurate with the level of risk and complexity of the relationship and the activity performed by the third-party. Examples of possible monitoring activities include:

- Reviewing reports on performance and effectiveness of controls, including independent audit reports and SOC reports.
- Periodic on-site visits or meetings to discuss open issues and plans for changes to the relationship.
- Reviewing updated due diligence information.
- Documenting service-level agreements with the third-party service provider to establish performance targets.
- Establishing measures for the third-party service provider to identify, record, and remediate instances of failure to meet contractual obligations or unsatisfactory performance and to report such instances to the futures commission merchant on a timely basis.
- Direct testing of the third-party service provider's control environment.

The frequency and depth of the futures commission merchant's monitoring activities should reflect the nature of the third-party relationship, including heightened monitoring for critical third-party service providers, and may change over the duration of the relationship. The futures commission merchant should dedicate sufficient staffing

resources to its monitoring activities and be particularly alert to any circumstances that could signal that a third-party service provider may not be able to perform to an acceptable standard. A futures commission merchant should be cognizant that certain events may trigger the need for it to take further action, including terminating its relationship with the third-party service provider. Such events could include cyberattacks, natural disasters, financial distress or insolvency, adverse or qualified audit opinions, or litigation or enforcement actions.

In addition to the continuous monitoring described above, futures commission merchants should periodically review and reevaluate their relationships with third-party service providers holistically. Such reviews should be more thorough than routine monitoring and may involve additional personnel, such as in-house or outside auditors, compliance and risk functions, information technology staff, or by a central function or committee whose visibility into other third-party relationships could provide valuable context for the relationship at issue. Additionally, to the extent a futures commission merchant uses enterprise risk management techniques, it should seek to integrate the information gathered from its ongoing monitoring with those practices. For example, to the extent that a futures commission merchant maintains a standardized approach across risk types to escalate concerns or issues to senior management or governance bodies (*e.g.,* through the use of predefined criteria or escalation paths), the futures commission merchant should consider using the same protocols for escalating concerns identified through its ongoing monitoring of third-party service providers. The ongoing monitoring approach itself may be subject to enterprise risk management practices, such as periodic self-assessment for effectiveness, independent testing, and quality assurance.

To the extent that monitoring activities reveal a change in their assessment of the risks associated with the third-party relationship, futures commission merchants should adjust the frequency and types of monitoring they conduct, including reports, regular testing, and on-site visits. One example of information that may change the level of monitoring is a notification that a third-party service provider has suffered or may suffer from a severe adverse event that could trigger a material change in the systems or process used to carry out an outsourced function.

E. Terminating the Third-Party Relationship—Commission Regulation 1.13(e)(1)(v)

Futures commission merchants should ensure that their third-party service provider relationship programs include advance preparation for the termination of the third-party relationship to ensure an orderly transition. Futures commission merchants should prepare for both planned terminations (*i.e.,* where one or both parties elects to end the relationship pursuant to their contract) and unplanned terminations (*e.g.,* following a sudden withdrawal of the third-party service). The plans should include both the contractual provisions for terminating the service (termination provisions), and the futures commission merchant's plan to facilitate an orderly transition of the function to an alternative provider or to bring it in-house (exit strategy). The goal of termination planning is to support an efficient transition to alternative arrangements for the provision of the service, regardless of the circumstances of the termination.

Termination provisions include all terms needed by the futures commission merchant to wind down a third-party service relationship while ensuring that the futures commission merchant can continue to serve its customers without interruption and to meet its regulatory compliance obligations. Because information, data, staff training, and knowledge may reside in the third-party service provider, there is an increased risk of disruption during the termination phase. When negotiating termination provisions, a futures commission merchant should ensure that the terms negotiated support its exit strategy. For example, a futures commission merchant should ensure that termination rights are accompanied by notice periods that leave the futures commission merchant enough time to find an alternative provider (or to provide the service itself) to ensure an orderly transition.

Similarly, the futures commission merchant should ensure that all customer data or other covered information in the third-party service provider's possession is promptly returned to the futures commission merchant or destroyed, as appropriate. The futures commission merchant should also verify that the third-party's access to its systems and covered information ceases at termination. Futures commission merchants should also consider negotiating more stringent terms for third-party service providers that breach their obligations under the agreement, other than for ''no-fault'' terminations. Such breaches may signal an inability of the third-party service provider to provide the services contracted for and thereby threaten the ability of the futures commission merchant to serve its customers and meet its regulatory obligations. (*See* section C of this guidance for examples of termination provisions.)

Futures commission merchants' exit strategies should include the steps needed to end the service provision with the third-party service provider and retain a new service provider or begin providing the service in-house. Although elements of an exit strategy may be reflected in termination provisions, not all elements of the exit strategy may be suitable for the contract. Examples include approvals, identification of alternative providers, description of the roles of staff in the futures commission merchant, and other internal matters. These elements may be memorialized in a procedure or similar document, such as the third-party relationship program. The exit strategy should contain the internal steps to be taken to ensure notification to the third-party service provider, identification of the proposed new provider, or, if bringing the function in-house, the hiring and training of personnel, development of procedures, and launch of new technology, along with the time periods and responsible personnel for each.

Futures commission merchants should be aware that, in practice, implementing an exit strategy may be complex and time-consuming and that the exercise of termination arrangements may be difficult. Futures commission merchants should also be aware that some third parties possess expertise that is not readily available and plan accordingly. Futures commission merchants should ensure that their plans are flexible enough to account for a range of plausible termination scenarios, including situations where the third-party service provider rapidly becomes unviable. Futures commission merchants may need to design backup or interim procedures sufficient to meet regulatory requirements in such situations.

PART 23—SWAP DEALERS AND MAJOR SWAP PARTICIPANTS

■ 4. The authority citation for part 23 continues to read as follows:

Authority: 7 U.S.C. 1a, 2, 6, 6a, 6b, 6b–1, 6c, 6p, 6r, 6s, 6t, 9, 9a, 12, 12a, 13b, 13c, 16a, 18, 19, 21.

Section 23.160 also issued under 7 U.S.C. 2(i); Sec. 721(b), Pub. L. 111–203, 124 Stat. 1641 (2010).

■ 5. Revise § 23.603 to read as follows:

§ 23.603 Operational Resilience Framework for Swap Dealers and Major Swap Participants.

(a) *Definitions.* For purposes of this section:

Affiliate means, with respect to any person, a person controlling, controlled by, or under common control with, such person.

Business continuity and disaster recovery plan means a written plan outlining the procedures to be followed in the event of an emergency or other significant disruption to the continuity of normal business operations and that meets the requirements of paragraph (f) of this section.

Consolidated program or plan means any information and technology security program, third-party relationship program, or business continuity and disaster recovery plan in which the swap entity participates with one or more affiliates and that is managed and approved at the enterprise level.

Covered information means any sensitive or confidential data or information maintained by a swap entity in connection with its business activities as a swap entity.

Covered technology means 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.

Critical third-party service provider means a third-party service provider, the disruption of whose performance would be reasonably likely to:

(1) Significantly disrupt a swap entity's business operations as a swap entity; or

(2) Significantly and adversely impact the swap entity's counterparties.

Information and technology security means the preservation of:

(1) The confidentiality, integrity, and availability of covered information; and

(2) The reliability, security, capacity, and resilience of covered technology.

Incident means any event, occurrence, or circumstance that could jeopardize information and technology security, including if it occurs at a third-party service provider.

Information and technology security program means a written program reasonably designed to identify, monitor, manage, and assess risks relating to information and technology security and that meets the requirements of paragraph (d) of this section.

Key controls mean controls that an appropriate risk analysis determines are either critically important for effective information and technology security or intended to address risks that evolve or change more frequently and therefore require more frequent review to ensure their continuing effectiveness in addressing such risks.

Oversight body means any board, body, or committee of a board or body of the swap entity specifically granted the authority and responsibility for making strategic decisions, setting objectives and overall direction, implementing policies and procedures, or overseeing the implementation of operations for the swap entity.

Risk appetite means the aggregate amount of risk a swap entity is willing to assume to achieve its strategic objectives.

Risk tolerance limit means the amount of risk, beyond its risk appetite, that a swap entity is prepared to tolerate through mitigating actions.

Senior officer means the chief executive officer or other equivalent officer of the swap entity.

Swap entity means a person that is registered with the Commission as a swap dealer or major swap participant pursuant to the Act.

Third-party relationship program means a written program reasonably designed to identify, monitor, manage, and assess risks relating to third-party relationships and that meets the requirements of paragraph (e) of this section.

(b) *Generally.* (1) *Purpose and scope.* Each swap entity shall establish, document, implement, and maintain an Operational Resilience Framework reasonably designed to identify, monitor, manage, and assess risks relating to:

(i) information and technology security;

(ii) third-party relationships; and

(iii) emergencies or other significant disruptions to the continuity of normal business operations as a swap entity.

(2) *Components.* The Operational Resilience Framework shall include an information and technology security program, a third-party relationship program, and a business continuity and disaster recovery plan. Each component program or plan shall be supported by written policies and procedures.

(3) *Standard.* 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.

(c) *Governance.* (1) *Approval of components.* Each component program or plan required by paragraph (b)(2) of this section shall be approved in writing, on at least an annual basis, by either the senior officer, an oversight body, or a senior-level official of the swap entity.

(2) *Risk appetite and risk tolerance limits.* (i) Each swap entity shall establish and implement appropriate risk appetite and risk tolerance limits with respect to the risk areas identified in paragraph (b)(1) of this section.

(ii) The risk appetite and risk tolerance limits established pursuant to paragraph (c)(2)(i) of this section shall be reviewed and approved in writing on at least an annual basis by either the senior officer, an oversight body, or a senior-level official of the swap entity.

(3) *Internal escalations.* The senior officer, an oversight body, or a senior-level official of the swap entity shall be notified of:

(i) circumstances that exceed risk tolerance limits established and approved pursuant to paragraph (c)(2)(i) of this section; and

(ii) incidents that require notification pursuant to paragraphs (i) or (j) of this section.

(4) *Swap entities forming part of a larger enterprise.* (i) *Generally.* A swap entity may satisfy the requirements of paragraph (b)(2) of this section through its participation in a consolidated program or plan, provided that each consolidated program or plan meets the requirements of this section.

(ii) *Attestation.* A swap entity that relies on a consolidated program or plan pursuant to paragraph (c)(4)(i) of this section may satisfy the requirements in paragraphs (c)(1) and (c)(2)(ii) of this section provided that either the senior officer, an oversight body, or a senior-level official of the swap entity attests in writing, on at least an annual basis, that the consolidated program or plan meets the requirements of this section and reflects a risk appetite and risk tolerance limits appropriate to the swap entity.

(d) *Information and technology security program.* (1) *Risk assessment.*

(i) The information and technology security program shall require the swap entity to conduct and document the results of a comprehensive risk assessment reasonably designed to identify, assess, and prioritize risks to information and technology security.

(ii) Such risk assessment shall be conducted at a frequency consistent with the standard set forth in paragraph (b)(3) of this section, but at least annually, and be conducted by personnel not responsible for the development or implementation of covered technology or related controls.

(iii) The results of the risk assessment shall be provided to the oversight body, senior officer, or other senior-level official who approves the information and technology security program upon the risk assessment's completion.

(2) *Effective controls.* The information and technology security program shall require the swap entity to establish, document, implement, and maintain controls reasonably designed to prevent, detect, and mitigate identified risks to information and technology security. Each swap entity shall consider, at a minimum, the following types of controls and adopt those consistent with the standard set forth in paragraph (b)(3) of this section:

(i) Access 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;

(ii) Access restrictions designed to permit only authorized individuals to access physical locations containing covered information, including, but not limited to, buildings, computer facilities, and records storage facilities;

(iii) Encryption of electronic covered information, including while in transit or in storage on networks or systems, to which unauthorized individuals may have access;

(iv) Dual control procedures, segregation of duties, and background checks for employees or third-party service providers with responsibilities for or access to covered information;

(v) Change management practices, including defined roles and responsibilities, logging, and monitoring practices;

(vi) Systems development and configuration management practices, including practices for initializing, changing, testing, and monitoring configurations;

(vii) Flaw remediation, including vulnerability patching practices;

(viii) Measures to protect against destruction, loss, or damage of covered information due to potential environmental hazards, such as fire and water damage or technological failures;

(ix) Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into covered technology;

(x) Response programs that specify actions to be taken when the swap entity suspects or detects that unauthorized individuals have gained access to covered technology, including appropriate reports to regulatory and law enforcement agencies; and

(xi) Measures to promptly recover and secure any compromised covered information.

(3) *Incident response plan.* The information and technology security program shall include a written incident response plan that is reasonably designed to detect, assess, contain, mitigate the impact of, and recover from an incident. This incident response plan shall include, at a minimum:

(i) The roles and responsibilities of the swap entity's management, staff, and third-party service providers in responding to incidents;

(ii) Escalation protocols, including a requirement to timely inform the oversight body, senior officer, or other senior-level official that has primary responsibility for overseeing the information and technology security program; the chief compliance officer of the swap entity; and any other relevant personnel of incidents that may

significantly impact the swap entity's regulatory obligations or require notification to the Commission;

(iii) The points of contact for external coordination of incident responses as determined necessary by the swap entity based on the severity of incidents;

(iv) The required reporting of incidents, whether by internal policy, contract, or law, including as required in this section;

(v) Procedures for documenting incidents and managements' response; and

(vi) The remediation of weaknesses in information and technology security, controls, and training, if any.

(e) *Third-party relationship program.* (1) *Third-party relationship lifecycle stages.* The third-party relationship program shall describe how the swap entity addresses the risks attendant to each stage of the third-party relationship lifecycle, including:

(i) Pre-selection risk assessment;

(ii) Due diligence of prospective third-party service providers;

(iii) Contractual negotiations;

(iv) Ongoing monitoring; and

(v) Termination, including preparations for planned and unplanned terminations.

(2) *Heightened duties for critical third-party service providers.* The third-party relationship program shall establish heightened due diligence practices for potential critical third-party service providers and heightened monitoring for critical third-party service providers.

(3) *Third-party service provider inventory.* As part of its third-party relationship program, each swap entity shall create, maintain, and regularly update an inventory of third-party service providers the swap entity 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.

(3) *Retention of responsibility.* Notwithstanding a swap entity's determination to rely on a third-party service provider, each swap entity remains responsible for meeting its obligations under the Act and Commission regulations.

(4) *Guidance on third-party relationship programs.* For guidance outlining potential risks, considerations, and strategies for developing a third-party relationship program consistent with paragraph (e), see Appendix A to Subpart J of this part.

(f) *Business continuity and disaster recovery plan.* (1) *Purpose.* The business continuity and disaster recovery plan shall be reasonably designed to enable the swap entity to:

(i) Continue or resume normal business operations with minimal disruption to counterparties and the markets; and

(ii) Recover and make use of covered information, as well as any other data, information, or documentation required to be maintained by law and regulation.

(2) *Minimum contents.* The business continuity and disaster recovery plan shall, at a minimum:

(i) Identify covered information, as well as any other data or information required to be maintained by law and regulation, and establish and implement procedures to backup or copy all such data and information with sufficient frequency to meet the requirements of this section and to store such data and information off-site in either hard-copy or electronic format;

(ii) Identify any resources, including covered technology, facilities, infrastructure, personnel, and competencies, essential to the operations of the swap entity or to fulfill the regulatory obligations of the swap entity, and establish and maintain procedures and arrangements to provide for their backup in a manner that is sufficient to meet the requirements of this section. Such arrangements must provide for backups that are located in one or more areas that are geographically separate from the swap entity's primary systems, facilities, infrastructure, and personnel, and may include the use of resources provided by third-party service providers;

(iii) Identify potential disruptions to critical third-party service providers and establish a plan to minimize the impact of such disruptions;

(iv) Identify supervisory personnel responsible for implementing each aspect of the business continuity and disaster recovery plan, including the emergency contacts required to be provided pursuant to paragraph (k) of this section; and

(v) Establish a plan for communicating with the following persons in the event of an emergency or other significant disruption, to the extent applicable: employees; counterparties; swap data repositories; execution facilities; trading facilities; clearing facilities; regulatory authorities; data, communications and infrastructure providers and other vendors; disaster recovery specialists; and other persons essential to the recovery of documentation and data, the resumption of operations, and compliance with the Act and Commission regulations.

(3) *Accessibility.* Each swap entity shall maintain copies of its business continuity and disaster recovery plan at one or more accessible off-site locations.

(g) *Training and distribution.* (1) *Training.* Each swap entity shall establish, implement, and maintain training with respect to all aspects of the Operational Resilience Framework, including, but not limited to:

(i) Cybersecurity awareness training for all personnel; and

(ii) Role-specific training for personnel involved in establishing, documenting, implementing, and maintaining the Operational Resilience Framework.

(2) *Frequency.* Each swap entity shall provide and update the training required in paragraph (g)(1) as necessary, but no less frequently than annually.

(3) *Distribution.* Each swap entity shall distribute copies of each component program or plan required by paragraph (b)(2) of this section to relevant personnel and promptly provide any significant revisions thereto.

(h) *Reviews and Testing.* Each swap entity shall establish, implement, and maintain a plan reasonably designed to assess its adherence to, and the effectiveness of, its Operational Resilience Framework through regular reviews and risk-based testing.

(1) *Reviews.* Reviews of the Operational Resilience Framework shall be conducted at least annually and in connection with any material change to the activities or operations of the swap entity that is reasonably likely to affect the risks identified in paragraph (b)(1) of this section. Reviews shall include an analysis of adherence to, and the effectiveness of, the Operational Resilience Framework and any recommendations for modifications or improvements that address root causes of any issues identified by the review.

(2) *Testing.* The frequency, nature, and scope of risk-based testing of the Operational Resilience Framework shall be determined by the swap entity, consistent with the standard in paragraph (b)(3) of this section.

(i) Testing of the information and technology security program shall include, at a minimum:

(A) Testing of key controls and the incident response plan at least annually;

(B) Vulnerability assessments, including daily or continuous automated vulnerability scans; and

(C) Penetration testing at least annually.

(ii) Testing of the business continuity and disaster recovery plan shall include, at a minimum, a walk-through or tabletop exercise designed to test the effectiveness of backup facilities and capabilities at least annually.

(3) *Independence.* The reviews and testing shall be conducted by qualified personnel who are independent of the aspect of the Operational Resilience Framework being reviewed or tested.

(4) *Documentation.* Each swap entity shall document all reviews and testing of the Operational Resilience Framework. The documentation shall, at a minimum, include:

(i) The date the review or testing was conducted;

(ii) The nature and scope of the review or testing, including methodologies employed;

(iii) The results of the review or testing, including any assessment of effectiveness;

(iv) Any identified deficiencies and recommendations for remediation; and

(v) Any corrective action(s) taken or initiated, including the date(s) such action(s) were taken.

(5) *Internal reporting.* Each swap entity shall report on the results of its reviews and testing to the swap entity's chief compliance officer and any other relevant senior-level official(s) and oversight body(ies).

(i) *Notifications to the Commission.* (1) *Incidents.*

(i) *Notification trigger.* Each swap entity shall 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 swap entity to continue its business activities as a swap entity; or

(C) The assets or positions of a counterparty of the swap entity.

(ii) *Contents.* The notification shall provide any information available to the swap entity at the time of notification that may assist the Commission in assessing and responding to the incident, including the date the incident was detected, possible cause(s) of the incident, its apparent or likely impacts, and any actions the swap entity has taken or is taking to mitigate or recover from the

incident, including measures to protect counterparties.

(iii) *Timing and method.* Each swap entity shall provide the incident notification as soon as possible but in any event no later than 24 hours after such incident has been detected. The notification shall be provided via email to *ORFnotices@cftc.gov.*

(2) *Business continuity and disaster recovery plan activation.* (i) *Notification trigger.* Each swap entity shall notify the Commission of any determination to activate the business continuity and disaster recovery plan.

(ii) *Contents.* The notification shall provide any information available to the swap entity at the time of notification that may assist the Commission in assessing or responding to the emergency or disruption, including the date of the emergency or disruption, a description thereof, the possible cause(s), its apparent or likely impacts, and any actions the swap entity has taken or is taking to mitigate or recover from the emergency or disruption, including measures taken or being taken to protect counterparties.

(iii) *Timing and method.* Each swap entity shall provide the business continuity and disaster recovery plan activation notification within 24 hours of determining to activate the business continuity and disaster recovery plan. The notification shall be provided via email to *ORFnotices@cftc.gov.*

(j) *Notification of incidents to affected counterparties.* (1) *Notification trigger.* Each swap entity shall notify a counterparty as soon as possible of any incident that is reasonably likely to have adversely affected the confidentiality or integrity of the counterparty's covered information, assets, or positions.

(2) *Contents.* The notification to affected counterparties shall include information necessary for the affected counterparty to understand and assess the potential impact of the incident on its information, assets, or positions, and to take any necessary action. Such notification shall include, at a minimum:

(i) A description of the incident;

(ii) The particular way in which the counterparty, or its covered information, may have been adversely impacted;

(iii) Measures being taken by the swap entity to protect against further harm; and

(iv) Contact information for the swap entity where the counterparty may learn more about the incident or ask questions.

(k) *Emergency Contacts.* (1) Each swap entity shall provide the Commission the name and contact information of:

(i) Two employees whom the Commission may contact in connection with incidents triggering notification to the Commission under paragraph (i)(1) of this section; and

(ii) Two employees whom the Commission may contact in connection with the activation of the swap entity's business continuity and disaster recovery plan triggering notification to the Commission under paragraph (i)(2) of this section.

(2) The identified employees shall be authorized to make key decisions on behalf of the swap entity and have knowledge of the swap entity's incident response plan or business continuity and disaster recovery plan, as appropriate.

(3) The swap entity shall update its emergency contacts with the Commission as necessary.

(l) *Recordkeeping.* Each swap entity shall maintain all records required to be maintained pursuant to this section in accordance with section 1.31 of this chapter and shall make them available promptly upon request to representatives of the Commission and to representatives of applicable prudential regulators, as defined in section 1a(39) of the Act.

■ 6. Add appendix A to subpart J of part 23 to read as follows:

Appendix A to Subpart J of Part 23—Guidance on Third-Party Relationship Programs

The following guidance offers factors, actions, and strategies for swap entities to consider in preparing and implementing third-party relationship programs reasonably designed to identify, monitor, manage, and assess risks relating to third-party relationships, as required by Commission regulation 23.603. The guidance is also not intended to reduce or replace the obligation of swap entities to comply with the requirements in Commission regulation 23.603, including the requirement to ensure that each swap entity's Operational Resilience Framework is 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. The guidance is not exhaustive and is nonbinding.

The guidance is written to be broadly relevant to all swap entities, but it may not be universally applicable. The 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. Each swap entity should assess the relevance of the guidance as it applies to its particular risk profile and tailor its third-party relationship program accordingly.

Comparable guidance for futures commission merchants is included in Appendix A to part 1 of the Commission's regulations.

A. Pre-Selection Risk Assessment—Commission Regulation 23.603(e)(1)(i)

Before entering into a third-party relationship, swap entities should determine which services should be performed by a third-party and plan for how to manage associated risks. The Commission appreciates that reliance on third-party service providers may be unavoidable, particularly given the rapid pace of technological innovation, which may render it uneconomical or even infeasible for financial institutions to meet all of their technological needs in-house.

Nevertheless, given the risks associated with relying on third-party service providers, and that each additional third-party relationship a swap entity employs is likely to add further risk and complexity, a swap entity's third-party relationship program should include a deliberative process for affirmatively determining whether to source a particular service from a third-party service provider. In determining whether a particular function should be performed by a third-party service provider, swap entities should consider whether:

- The service would support the swap entity's strategic goals and objectives.
- The same goals and objectives could be addressed through an alternative means that may not require reliance on a third-party service provider.
- The swap entity has or could otherwise secure the resources, financial and otherwise, to effectively monitor the third-party service provider.
- Relevant and reputable third-party service providers are available.
- The provision of the service would implicate information and technology security concerns, including by requiring the third-party service provider to obtain access to covered information or provide covered technology.
- A disruption of the service would have a negative impact on counterparties or regulatory compliance.
- The relationship could be structured to reduce associated risks, such as by limiting the third-party service provider's access to covered information or covered technology.
- Lack of direct control over performance of the service would present unacceptable risk, *i.e.,* risk outside the swap entity's risk tolerance limits.

As the above considerations illustrate, swap entities should consider ways in which they might structure their third-party relationships to reduce the associated risks. For example, where giving a third-party service provider direct access to its technology or data may be outside a swap entity's risk tolerance, structuring the relationship to provide the third-party service provider access on a read-only basis or via reports delivered by the swap entity could render the relationship more acceptable. Swap entities should therefore consider the availability of safer means of performing the service as part of their assessment.

Changes in technology, businesses practices, regulation, market structure, market participants (*e.g.,* new entrants to the market), or service delivery may change the risk profile of the third-party relationship over time. Accordingly, swap entities should consider periodically reassessing their selection of services to be performed by third-party service providers. Swap entities should stay abreast of these changes by monitoring the external environment and communicating with current and prospective service providers and other participants in industry.

B. Due Diligence in Selecting Third-Party Service Providers—Commission Regulation 23.603(e)(1)(ii)

After a swap entity has determined that a service is suitable for a third-party to perform, it should conduct due diligence on prospective third-party service providers. Due diligence provides swap entities with the information they need to assess and conclude, with a reasonable level of assurance, that the prospective third-party service provider is capable of effectively

providing the service as expected, adhering to the swap entity's policies, maintaining the swap entity's compliance with Commission regulations, and protecting covered information. Appropriate due diligence should also enable swap entities to evaluate whether they would be able to effectively monitor and manage the risks associated with a particular third-party relationship.

Due diligence may be conducted before or contemporaneously with contractual negotiations with prospective third-party service providers but should be concluded prior to executing any agreements. Swap entities should conduct due diligence even in situations where, for a particular service, there may only be one or a small number of providers with a dominant market share whose services are used by all or most of the swap entities' industry peers, and swap entities should not rely solely on those providers' reputations or prior experience with them. The depth and rigor of the due diligence should be proportionate to the nature of the third-party relationship, with the required heightened due diligence required for potential critical third-party service providers pursuant to Commission regulation 23.603(e)(2). Specifically, when conducting due diligence for a potential critical third-party servicer provider, swap entities should expand the type and sources of information they rely on, the rigor and scrutiny they apply in reviewing the information to identify potential risks, and the level of confidence in their assessment of the third-party service provider's ability to perform.

When establishing their due diligence protocols, swap entities should consider the full range of risks that reliance on the third-party service providers could introduce in light of the nature of the service they would be performing. Relevant considerations with respect to the potential third-party service provider include its:

- Financial condition, business experience and reputation, and business prospects, particularly the third-party service provider's experience providing services to financial institutions.
- Background, experience, and qualifications with respect to key personnel.
- Information and technology security practices, including incident reporting and incident management programs, and whether there are clearly documented processes for identifying and escalating incidents.
- Risk management practices, including governance, controls, testing, and issue management practices, as well as the results of any independent risk assessments.
- Regulatory environment, including the legal jurisdiction in which it is based and applicable regulatory or licensing requirements.
- History of disruptions to operations, including whether the third-party service provider has suffered incidents that would meet the standard for reporting to the Commission in Commission regulation 23.603(i).
- Violations of legal, compliance, or contractual obligations, including civil or criminal proceedings or administrative enforcement actions, including from self-regulatory organizations.
- Understanding of Commission regulatory requirements applicable to the swap entity.
- Use of and reliance on subcontractors, including the volume and types of subcontracted activities, and the third-party service provider's process for identifying, assessing, managing, and monitoring associated risks.
- Business continuity and contingency plans.
- Financial protections, such as insurance coverage against losses or liabilities from intentional or negligent acts or hazards involving physical destruction and data or documentation losses.

Swap entities should memorialize their assessment of these factors and identify how the review was heightened for critical third-party service providers. Swap entities should not rely solely on their prior knowledge of or experience with a potential third-party. Potential sources of due diligence information include:

- Audit reports, including pooled audit plans, and System and Organizational Controls (SOC) reports.
- Financial statements and projections and relevant accompanying information (*e.g.,* annual or quarterly reports, management commentary, auditors' opinions, and investor relations materials).
- Incident response plans, including the results of recent testing or assessments thereof.
- Business continuity and disaster recovery plans, as well as the result of recent testing or assessments thereof.
- Public filings.
- News reports, trade publications, and press releases.
- Reports from market intelligence providers.
- References from current or previous customers, or other parties which have had business relationships with the third-party service provider.
- Informal industry discussions.
- Information provided directly by the third-party service provider, such as internal performance metrics.

Obtaining and reviewing audit reports, including SOC reports, may be of particular value for conducting heightened due diligence of critical third-party service providers. In certain circumstances, swap entities may not be able to gather all the information necessary to reach an informed conclusion that a prospective third-party service provider is an adequate provider. Examples include instances where the third-party service provider is a new entrant into the market and little information exists; where information provided by the third-party service provider is insufficient or appears unreliable; or where the third-party service provider is reluctant to provide internal information. In such cases, the swap entity should identify and document the limitations of its due diligence, the attendant risks, and any available methods for mitigating them (*e.g.,* obtaining alternate information, implementing enhanced monitoring or controls, negotiating protective contractual provisions). Ultimately, such factors could weigh against the use of the potential third-party service provider, particularly a potential critical third-party service provider. Swap entities that proceed with the third-party service arrangements notwithstanding the limited due diligence should do so with caution, applying heightened scrutiny of the information they do receive, and consider the implementation of their own mitigating controls to compensate for the uncertainty.

C. Contractual Negotiations—Commission Regulation 23.603(e)(1)(iii)

After selecting a third-party service provider, swap entities should proceed to finalizing the agreement, typically through entering into an enforceable written contract. Written contracts are an important tool for clarifying the scope of services to be delivered, establishing standards or performance benchmarks, allocating risks and responsibilities, and facilitating resolution of disputes. They can also reduce the risks of non-performance and assist in monitoring the third-party service provider. Because of their importance, the Commission recommends that swap entities enter written agreements with third-party service providers before services are delivered, particularly with critical third-party service providers.

In negotiating a written contract, swap entities should seek to negotiate contractual provisions that would support their ability to mitigate, manage, and monitor the risks associated with the relationship, as identified through their initial pre-selection and due diligence activities. The contractual provisions should be informed by the nature of the service provided and be proportionate to the criticality of the services provided. In particular, swap entities should consider negotiating for the contract to include the following provisions:

- Timely notification to the swap entity of any incidents suffered by third-party service providers, or of significant disruptions to the operations of the third-party service provider.
- Timely notification to the swap entity of any material changes to the services provided.
- Required periodic, independent audits of the third-party service provider, the results of which would be shared with the swap entity.
- Restrictions on the third-party service provider's use of the swap entity's covered information, except as necessary to deliver the service or meet legal obligations.
- Security measures to protect the swap entity's covered information and covered technology to which the third-party service provider has access.
- Insurance, guarantees, indemnification, and limitations on liability.
- Dispute resolution procedures.
- Performance measures or benchmarks.
- Remediation of identified performance issues.
- Compliance with regulatory requirements, including reasonable assurances that the third-party service provider is willing and able to coordinate with the swap entity for the purpose of ensuring the swap entity complies with its legal and regulatory obligations.
- Use of subcontractors, including notification or approval procedures for their use, the extension of contractual rights of the

swap entity against the third-party service provider to its subcontractors, and contractual obligations for reporting on or oversight of subcontractors.

- Termination provisions, including rights to terminate following breaches of the third-party service provider's obligations, notice requirements, obligations of the third-party service provider to provide support for a successful transition, and the return or destruction of records or covered information, as further described in section E of this guidance.
- Information sharing necessary to facilitate other provisions of this proposed guidance (for example, reporting requirements to support ongoing monitoring, as discussed in section D of this guidance, or notice requirements for termination, as discussed in section E of this guidance).

These provisions focus on key risk factors generally associated with third-party service provider relationships. They are not exhaustive of all contractual provisions swap entities should seek to include in their written contracts, including ordinary commercial contract terms (*e.g.,* choice of law provisions) and terms that may relate only to specific services, among other provisions. While third-parties may initially offer a standard contract, a swap entity may seek to request modifications, additional contractual provisions, or addendums to satisfy its needs. Swap entities should work to tailor the level of detail and comprehensiveness of the contractual provisions based on the risk and complexity posed by the particular third-party relationship, contracts with critical third-party service providers likely being the most tailored.

In some circumstances, a swap entity may be at a bargaining power disadvantage, which prevents it from negotiating optimal contractual provisions. For example, a prospective third-party service provider may be the sole provider of a service or may have such dominant market share that it can offer its services on a ''take-it-or-leave-it'' basis. In such situations, the swap entity should work to understand any resulting limitations in the contract and attendant risks and consider whether it can achieve outcomes comparable to those provided by contractual protections through non-contractual means. Examples could include the swap entity implementing additional controls, augmenting its monitoring of the third-party service provider using public sources or market intelligence services, or purchasing insurance. The swap entity should make an assessment, however, of whether these alternatives would provide an adequate substitute for the unobtained contractual protections and document its assessment and mitigation plan, considering its risk appetite and risk tolerance limits. Where a third-party service provider is unable or unwilling to agree to provisions necessary for the swap entity to meet its obligations under Commission regulations, particularly a critical third-party service provider, the swap entity should consider finding an alternative third-party service provider.

D. Ongoing Monitoring—Commission Regulation 23.603(e)(1)(iv)

After a third-party service provider has initiated performance, swap entities should engage in ongoing monitoring. Ongoing monitoring is important to ensure the third-party service provider is properly carrying out its outsourced function and contractual obligations, as well as meeting quality or performance expectations. Effective monitoring can aid swap entities in the early identification of performance deficits, allowing for a quicker response that may then mitigate the impact.

Ongoing monitoring should occur throughout the duration of a third-party relationship, commensurate with the level of risk and complexity of the relationship and the activity performed by the third-party. Examples of possible monitoring activities include:

- Reviewing reports on performance and effectiveness of controls, including independent audit reports and SOC reports.
- Periodic on-site visits or meetings to discuss open issues and plans for changes to the relationship.
- Reviewing updated due diligence information.
- Documenting service-level agreements with the third-party service provider to establish performance targets.
- Establishing measures for the third-party service provider to identify, record, and remediate instances of failure to meet contractual obligations or unsatisfactory performance and to report such instances to the swap entity on a timely basis.
- Direct testing of the third-party service provider's control environment.

The frequency and depth of the swap entity's monitoring activities should reflect the nature of the third-party relationship, including heightened monitoring for critical third-party service providers, and may change over the duration of the relationship. The swap entity should dedicate sufficient staffing resources to its monitoring activities and be particularly alert to any circumstances that could signal that a third-party service provider may not be able to perform to an acceptable standard. A swap entity should be cognizant that certain events may trigger the need for it to take further action, including terminating its relationship with the third-party service provider. Such events could include cyberattacks, natural disasters, financial distress or insolvency, adverse or qualified audit opinions, or litigation or enforcement actions.

In addition to the continuous monitoring described above, swap entities should periodically review and reevaluate their relationships with third-party service providers holistically. Such reviews should be more thorough than routine monitoring and may involve additional personnel, such as in-house or outside auditors, compliance and risk functions, information technology staff, or by a central function or committee whose visibility into other third-party relationships could provide valuable context for the relationship at issue. Additionally, to the extent a swap entity uses enterprise risk management techniques, it should seek to integrate the information gathered from its ongoing monitoring with those practices. For example, to the extent that a swap entity maintains a standardized approach across risk types to escalate concerns or issues to senior management or governance bodies (*e.g.,* through the use of predefined criteria or escalation paths), the swap entity should consider using the same protocols for escalating concerns identified through its ongoing monitoring of third-party service providers. The ongoing monitoring approach itself may be subject to enterprise risk management practices, such as periodic self-assessment for effectiveness, independent testing, and quality assurance.

To the extent that monitoring activities reveal a change in their assessment of the risks associated with the third-party relationship, swap entities should adjust the frequency and types of monitoring they conduct, including reports, regular testing, and on-site visits. One example of information that may change the level of monitoring is a notification that a third-party service provider has suffered or may suffer from a severe adverse event that could trigger a material change in the systems or process used to carry out an outsourced function.

E. Terminating the Third-Party Relationship—Commission Regulation 23.603(e)(1)(v)

Swap entities should ensure that their third-party service provider relationship programs include advance preparation for the termination of the third-party relationship to ensure an orderly transition. Swap entities should prepare for both planned terminations (*i.e.,* where one or both parties elects to end the relationship pursuant to their contract) and unplanned terminations (*e.g.,* following a sudden withdrawal of the third-party service). The programs should include both the contractual provisions for terminating the service (termination provisions), and the swap entity's plan to facilitate an orderly transition of the function to an alternative provider or to bring it in-house (exit strategy). The goal of termination planning is to support an efficient transition to alternative arrangements for the provision of the service, regardless of the circumstances of the termination.

Termination provisions include all terms needed by the swap entity to wind down a third-party service relationship while ensuring that the swap entity can continue to serve its counterparties without interruption and to meet its regulatory compliance obligations. Because information, data, staff training, and knowledge may reside in the third-party service provider, there is an increased risk of disruption during the termination phase. When negotiating termination provisions, a swap entity should ensure that the terms negotiated support its exit strategy. For example, a swap entity should ensure that termination rights are accompanied by notice periods that leave the swap entity enough time to find an alternative provider (or to provide the service itself) to ensure an orderly transition.

Similarly, the swap entity should ensure that all customer data or other covered information in the third-party service provider's possession is promptly returned to

the swap entity or destroyed, as appropriate. The swap entity should also verify that the third-party's access to its systems and covered information ceases at termination. Swap entities should also consider negotiating more stringent terms for third-party service providers that breach their obligations under the agreement, other than for ''no-fault'' terminations. Such breaches may signal an inability of the third-party service provider to provide the services contracted for and thereby threaten the ability of the swap entity to serve its customers and meet its regulatory obligations. (*See* section C of this guidance for examples of termination provisions.)

Swap entities' exit strategies should include the steps needed to end the service provision with the third-party service provider and retain a new service provider or begin providing the service in-house. Although elements of an exit strategy may be reflected in termination provisions, not all elements of the exit strategy may be suitable for the contract. Examples include approvals, identification of alternative providers, description of the roles of staff in the swap entity, and other internal matters. These elements may be memorialized in a procedure or similar document, such as the third-party relationship program. The exit strategy should contain the internal steps to be taken to ensure notification to the third-party service provider, identification of the proposed new provider, or, if bringing the function in-house, the hiring and training of personnel, development of procedures, and launch of new technology, along with the time periods and responsible personnel for each.

Swap entities should be aware that, in practice, implementing an exit strategy may be complex and time-consuming and that the exercise of termination arrangements may be difficult. Swap entities should also be aware that some third parties possess expertise that is not readily available and plan accordingly. Swap entities should ensure that their plans are flexible enough to account for a range of plausible termination scenarios, including situations where the third-party service provider rapidly becomes unviable. Swap entities may need to design backup or interim procedures sufficient to meet regulatory requirements in such situations.

Issued in Washington, DC, on December 22, 2023, by the Commission.

Robert Sidman,

Deputy Secretary of the Commission.

NOTE: The following appendices will not appear in the Code of Federal Regulations.

Appendices to Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants—Voting Summary and Chairman's and Commissioners' Statements

Appendix 1—Voting Summary

On this matter, Chairman Behnam, Commissioners Johnson, Goldsmith Romero, Mersinger and Pham voted in the affirmative. No Commissioner voted in the negative.

Appendix 2—Statement of Support of Chairman Rostin Behnam

I support the Commission's approval of the notice of proposed rulemaking to require futures commission merchants (FCMs), swap dealers (SDs), and major swap participants (MSPs) to establish an operational resilience framework (ORF).

The proposal recognizes that while FCMs, SDs, and MSPs (collectively, ''covered entities'') have generally withstood challenging market conditions since the Commission promulgated its risk management program requirements over a decade ago, the Commission must bolster that foundational framework to promote operational resilience in the face of increasingly sophisticated cyberattacks and heightened technological disruptions. A strong ORF is especially important as the financial sector increasingly relies on third-party service providers; the disruption of which can lead to major interruptions in—and potential corruption of—FCM and SD operations. In addition to market impacts, events like these may impact covered entities' ability to comply with the Commission's statutory and regulatory requirements.

FCMs' customers and SDs' counterparties expect covered entities to take a 360-degree approach to identify, monitor, manage, and assess risks for potential vulnerabilities. Similarly, the Commission must identify, monitor, manage, and assess any potential gaps in its own risk management requirements that could impede sound risk management practices, expose the U.S. financial system to unmanaged risk, or weaken customer protection. Operational disruptions that place a covered entity's financial resources at risk; disrupt the segregation and protection of customer funds; hinder recordkeeping; introduce uncertainty or delay; or otherwise inject operational risk into the derivatives market must be avoided to the extent possible to ensure customers, counterparties, and market participants have confidence in the integrity of our markets.

The operational resilience framework proposal is the product of many months of in-depth research regarding operational resilience standards and guidance issued by the prudential regulators, the U.S. Securities and Exchange Commission, the National Futures Association, the International Organization of Securities Commissions, the Financial Stability Board, and other subject matter experts to avoid those operational disruptions and failures. The proposal also reflects staff's own observations and lessons learned from its own oversight activities.

The proposal is a holistic, principles-based approach that is calibrated with certain minimum requirements. Specifically, the proposed rule would require covered entities to establish, document, implement, and maintain an ORF reasonably designed to identify, monitor, manage, and assess risks relating to three key risk areas: (1) information and technology security, (2) third-party relationships, and (3) emergencies and other significant disruptions. The ORF would also include requirements related to governance, training, testing, and recordkeeping.

The proposal would require covered entities to establish risk appetite and risk tolerance limits and would allow these registrants to rely on an information and technology security program, third-party relationship program, or business continuity and disaster recovery plan in which the covered entity participates with one or more affiliates and that is managed and approved at the enterprise level. Testing would need to be risk-based and include, at a minimum, daily or continuous vulnerability assessment and annual penetration testing, among others. The proposed rule would also require certain notifications to the Commission and customers or counterparties. The Commission is also proposing non-binding guidance that FCMs and SDs could consider to identify factors, actions, and strategies as they design their third-party relationship programs.

The Commission recognizes that covered entities subject to this proposal include many different business models. As a result, the proposal is tailored to accommodate firms that vary in size and complexity, including corporate structures in which operational resilience frameworks may be managed at an enterprise level and have governance arrangements with different reporting line structures. In the same vein, the proposed ORF standard would require covered entities to implement an ORF that is appropriate and proportionate to the nature, size, scope, complexity, and risk profile of the firm's business as an FCM or SD, following generally accepted standards and best practices.

I look forward to reading the public's comments on how the proposed operational resilience framework requirements and guidance can strengthen the operational resilience of FCMs, SDs, and MSPs as well as help protect their respective customers and counterparties in the derivatives markets. The 75-day comment period will begin upon the Commission's publication of the release on its website.

I thank staff in the Market Participants Division, Office of the General Counsel, and the Office of the Chief Economist for all of their work on the proposal.

Appendix 3—Statement of Commissioner Kristin N. Johnson

Cyberattacks are an ever-increasing threat. The rising cost, frequency, and severity of cyber threats represent one of the most critical issues facing city, state, and federal government authorities, businesses in each sector of our economy, educational and philanthropic institutions, and significant energy and transportation infrastructure, and national security resources.

Less than a month before the White House released its National Cybersecurity Strategy in March of this year, international media headlines reported a ransomware attack that demonstrated that ''big financial firms'' are among the most attractive targets of cyber threats.[1] Even for firms that have successfully

[1] James Rundle, Wall Street Journal, Cyberattack on ION Derivatives Unit Had Ripple Effects on Financial Markets (Feb. 10, 2023), *https://www.wsj.com/articles/cyberattack-on-ion-*

developed business continuity plans to identify, assess, or mitigate cyber threats, the networked or interconnected systems that comprise our operational market infrastructure may still render sophisticated, well-resourced firms vulnerable to the knock-on effects of cyberattacks leveled against critical third-party service providers.

The ransomware attack, carried out on a critical third-party service provider, ION Cleared Derivatives,[2] disrupted trade settlement and reconciliation in derivatives markets.

ION provides trading, clearing, analytics, treasury, and risk management services for capital markets and futures and derivatives markets. A significant number of market participants, including a notable number of futures commission merchants (FCMs), rely on ION for back-office trade processing and settlement of exchange-traded derivatives.

The cyber-incident that disrupted ION's operations caused a ripple effect across markets, halting deal matching, requiring affected parties to rely on manual (old school) trade processing, and causing delays in reconciliation and information sharing and reporting.

MRAC Leads on Cyber Reform Discussions

I sponsor the Market Risk Advisory Committee (MRAC). On March 8, 2023, the MRAC held a first-of-its-kind convening focused on the interconnectedness of our markets and the potential for interconnectedness and correlation to amplify contagion in the event of successful cyberattacks against critical infrastructure resources.[3] At the March MRAC meeting, Futures Industry Association (FIA) President Walt Lukken announced the creation of a Cyber Risk Taskforce, charged with ''recommend[ing] ways to improve the ability of the exchange-traded and cleared derivatives industry to withstand the disruptive impacts of a cyberattack.''[4]

The After Action Report issued by the FIA at the conclusion of the Taskforce's work outlines the challenges that both markets and regulators faced as a result of the ION cyber-incident. Trade reconciliation for affected firms continued to lag. For weeks following the ION cyberattack, the Commission continued to work to consistently publish the Commitments of Traders (COT) report on a timely basis because ''reporting firms continu[ed] to experience . . . issues submitting timely and accurate data to the CFTC.''[5] The COT report is designed to help the public understand the dynamics of the futures and options on futures markets.[6] The COT report is a reflection of the effectiveness of the Commission's surveillance of markets; it increases transparency and aids in price discovery. Thus, indirectly, the ION incident disrupted regulatory functions even though the cyberattack was not directed at the Commission nor any of the Commission's registrants.

As a consequence, it is imperative to begin to examine the scope of our regulations governing cyber-system safeguards not only for registered market participants, but for mission-critical third-party service providers. There is increasing reliance on third parties for the provision of important services, particularly, for example, services that facilitate digital connectivity and cloud-based services.

While outsourcing may allow companies to rely on outside expertise, reduce operating costs, and enhance operational infrastructure necessary for executing business activities, reliance, may, in some instances, create vulnerability and risks that must be identified, managed, and mitigated.

Operational Resilience Proposed Rulemaking

Today, the Market Participants Division (MPD) has introduced a robust and comprehensive proposed rulemaking that addresses: business continuity and disaster planning, cybersecurity, and assessment of the risk posed by reliance on third parties. I want to commend MPD, in particular Pamela Geraghty, Elise Bruntel, Fern Simmons, and Amanda Olear.

The Commission has the authority to direct swap entities (swap dealers and major swap participants) to establish this operational resilience framework under Section 4s(j)(2) and (7) of the Commodity Exchange Act (CEA), which require swap entities to establish risk management systems over their day-to-day business and their operational risk.[7] Likewise, the Commission may require operational resilience framework of FCMs (collectively with swap entities, ''covered entities'') under Section 8a(5) of the CEA,[8] which authorizes the Commission to promulgate regulations sufficient to accomplish the purposes of the CEA, including, for example, the need to maintain records of the operational risk of affiliates,[9] and to establish safeguards to protect the confidentiality of nonpublic personal information.[10]

The proposed rulemaking sets out three major pillars of its operational resilience framework: (1) information and technology security; (2) a third-party relationship program to manage risks presented by mission-critical third-party service providers; and (3) a business continuity and disaster recovery plan.[11]

Layered on top of the of the three pillars are *corporate governance* reforms that will dictate how each covered entity will incorporate the components of the plan into existing organizational structures. Each of the components of the operational resilience framework must be reviewed by senior leadership.[12] Covered entities must also establish a risk appetite—the level of risk acceptable on an ongoing basis—and risk tolerance limits—the level of excess risk the entity is willing to accept should a particular risk materialize [13]—and the entities will be required to escalate incidents that exceed their risk tolerance limit.[14] The rule also allows for flexibility for entities that function as a division or affiliate of a larger organization; such entities will be allowed to operate under the umbrella company's operational resilience plan so long as that plan meets the rule's requirements and considers the covered entity's particular risks.[15]

The *information and technology security program* requires the covered entities to comprehensively assess, on at least an annual basis, the types of threats the entity faces, the entity's internal and external vulnerabilities, the likely impact of those threats or the exploitation of those vulnerabilities, and appropriate priorities for addressing those risks.[16] With that background, covered entities must then implement controls reasonably designed to prevent, detect, and mitigate the identified risks, threats, and vulnerabilities.[17] The program then requires the covered entities to develop a written incident response plan, reasonably designed to detect incidents where risks to information and technology are realized, and then provide for how the entity will mitigate the impact of and recover from such an incident.[18]

The *third-party relationship plan* requires covered entities to understand the risks posed by all third-party service providers at each stage of the relationship: pre-selection, diligence, contract negotiation, ongoing monitoring, and termination.[19] The proposed rule then imposes a heightened level of required diligence and monitoring for ''critical'' third parties, defined as those parties for whom disruption of performance on their service contract would either ''significantly disrupt'' the covered entity's business operations, or ''significantly and adversely impact'' the entity's counterparties or customers.[20] Covered entities will also have to maintain an inventory of their critical and non-critical third-party service providers.[21] Finally, regardless of any

derivatives-unit-had-ripple-effects-on-financial-markets-11675979210.

[2] *See* Press Release, ION Markets, Cleared Derivatives Cyber Event (Jan. 31, 2023), *https://iongroup.com/press-release/markets/cleared-derivatives-cyber-event/.*

[3] Kristin N. Johnson, Commissioner, CFTC, Opening Statement Before the Market Risk Advisory Committee Meeting (Mar. 8, 2023), *https://www.cftc.gov/PressRoom/SpeechesTestimony/johnsonstatement030823.*

[4] Futures Industry Association, FIA Taskforce on Cyber Risk, After Action Report and Findings, at 3 (Sept. 28, 2023), *https://www.fia.org/sites/default/files/2023-09/FIA_Taskforce%20on%20Cyber%20Risk_Recommendations_SEPT2023_Final2.pdf.*

[5] Press Release No. 8662–23, CFTC, CFTC Announces Postponement of Commitments of Traders Report (Feb. 16, 2023), *https://www.cftc.gov/PressRoom/PressReleases/8662-23.*

[6] CFTC, Commitments of Traders Reports Descriptions, *https://www.cftc.gov/MarketReports/CommitmentsofTraders/index.htm.*

[7] 7 U.S.C. 6s(j)(2), (7).

[8] 7 U.S.C. 12a(5).

[9] 7 U.S.C. 6f.

[10] 7 U.S.C. 7b–2; 15 U.S.C. 6801.

[11] Proposed §§ 1.13(b)(2), 23.603(b)(2).

[12] Proposed §§ 1.13(c)(1), 23.603(c)(1).

[13] Proposed §§ 1.13(c)(1), 23.603(c)(2).

[14] Proposed §§ 1.13(c)(3), 23.603(c)(3).

[15] Proposed §§ 1.13(c)(4), 23.603(c)(4).

[16] Proposed §§ 1.13(d)(1), 23.603(d)(1).

[17] Proposed §§ 1.13(d)(2), 23.603(d)(2).

[18] Proposed §§ 1.13(d)(3), 23.603(d)(3).

[19] Proposed §§ 1.13(e)(1), 23.603(e)(1).

[20] Proposed §§ 1.13(e)(2), 23.603(e)(2).

[21] Proposed §§ 1.13(e)(3), 23.603(e)(3).

decision to rely on a third-party service provider, each covered entity remains responsible for meeting its obligations under the CEA and Commission regulations.[22]

Each entity's *business continuity and disaster recovery plan* (BCDR plan) must ''outline[ ] the procedures to be followed in the event of an emergency or other disruption of its normal business activities.'' [23] The goal of a BCDR plan will be to enable covered entities to continue or resume business operations with minimal disruption to customers, counterparties, or the markets, and recover any affected data or information.[24] At minimum, the BCDR plan must define backup plans for covered information and data; identify essential technology, facilities, infrastructure, and personnel; identify potential disruptions to critical third-party service providers; and identify supervisory personnel responsible for carrying out the plan in the event of an emergency.[25] Covered entities must also maintain the plan at one or more off-site locations.[26]

To support the pillars of the operational resilience framework, the proposed rule also lays out training,[27] review, and testing requirements to ensure the framework evolves with newly generated risks. Covered entities must review their framework annually,[28] and engage in regular independent and documented testing, including penetration testing, vulnerability assessments, and testing of the incident response and BCDR plans.[29] Results of that testing must be reported to the entity's chief compliance officer and other relevant senior personnel.[30] Finally, the proposed rule lays out the instances in which the Commission must be notified of incidents and of activation of the BCDR plan.[31]

This proposed rulemaking is both expansive and thoroughly considered. It galvanizes much of the preexisting guidance on these subjects, recognizing that the vast majority of our market participants already have programs in place to address these risks and often already are subject to other regulators' rules and obligations, both domestically and internationally. The rule also recognizes the vast range in the size of the operations of our registered market participants—from some of the world's largest financial institutions acting as swap dealers to small, independent futures commissions merchants—and consequently builds flexibility into the proposed rule to allow businesses to tailor their operational resilience frameworks to the realities of their business needs.

The Need for Operational Resilience for Other Commission Registrants

This rule is necessarily limited in scope to FCMs and the swap entities overseen by MPD. The risks that this rule intends to mitigate, however, are not similarly siloed. Designated Contract Markets (DCM), Swap Execution Facilities (SEF), and Swap Data Repositories (SDR), overseen by the Division of Market Oversight, and Derivative Clearing Organizations (DCO), overseen by the Division of Clearing and Risk, similarly rely on mission-critical third-party service providers, similarly are targeted by cyberattacks, and similarly risk business disruption caused by unforeseen disaster scenarios.

Rulemakings completed in 2016 created system safeguard testing requirements for each of these entities, currently codified in Parts 37, 38, 39, and 49 of the CFR.[32] These rules include obligations for business continuity and disaster recovery and cybersecurity. Since 2016, however, the core issues surrounding the concept of operational resilience have shifted, most importantly around the ideas of mission-critical third parties. DCOs are increasingly contracting with third parties to manage and conduct aspects of their regulatory obligations, and just like with the covered entities subject to the rule at issue today, the onboarding of these new third parties also onboards new risks. The proposed rulemaking today considers the system safeguards provisions already on the books; [33] the Commission now needs to continue to press forward by considering this proposed rule for future parallel regulations, for DCOs in particular.

The pandemic underscored the importance of business operational resilience, namely the ability of our registrants to react to and withstand unforeseen disasters. The FIA conducted its annual Disaster Recovery Exercise this fall with the stated goal of probing participants' ability to ''conduct critical business functions'' in the wake of a large-scale disaster.[34] Last year's exercise saw participation from 19 major U.S. and international futures exchanges and clearinghouses, who indicated that this type of probing helped them to: ''Exercise their business continuance/disaster resilience plans[, i]dentify internal and external single points of failure . . . [, and t]ighten up and improve the documentation of their business continuity procedures.'' [35]

In 2021, the International Organization of Securities Commissions (IOSCO) initiated a consultation examining business continuity planning.[36] IOSCO's initial recommendations to member jurisdictions stated that all regulators should require firms to have in place ''mechanisms to help ensure the resiliency, reliability and integrity (including security) of critical systems'' including an appropriate ''Business Continuity Plan.'' [37]

Every industry advisory board and oversight group to have studied cybersecurity has reached the same conclusion: risks to financial institutions from cyberattacks continue to grow. The Financial Stability Oversight Council noted in its 2022 annual report that from 2015 to 2020 the finance and insurance industries were subject to the most cyberattacks of any industry, and that the current global geopolitical climate has only increased the need for vigilance against cyber threats.[38] In April 2020, the Financial Stability Board (FSB) issued a guide on cyber incident response that explained that ''[a] significant cyber incident, if not properly contained, could seriously disrupt the financial system, including critical financial infrastructure, leading to broader financial stability implications.'' [39] Similarly, in its 2019 Cyber Task Force report, IOSCO reiterated that cyber risk is one of the top threats to financial markets today given the ''economic costs of such events can be immense . . . and could potentially undermine the integrity of global financial markets.'' [40] IOSCO went further in their recommendations to the crypto industry earlier this year that ''[r]egulators should require a [crypto-asset service provider] to put in place sufficient measures to address cyber and system resiliency.'' [41]

Next Steps for Derivatives Clearing Organizations

At the MRAC meeting this past Monday, I announced a new workstream for the CCP Risk and Governance subcommittee that will focus on third-party risk for central clearing counterparties. Work will begin imminently, with the goal of presenting a proposal for

[22] *Id.*

[23] *See* 17 CFR 23.603(a).

[24] Proposed §§ 1.13(f)(1)(i)–(ii), 23.603(f)(1)(i)–(ii).

[25] Proposed §§ 1.13(f)(2), 23.603(f)(2).

[26] Proposed §§ 1.13(f)(3), 23.603(f)(3).

[27] Proposed §§ 1.13(g), 23.603(g).

[28] Proposed §§ 1.13(h)(1), 23.603(h)(1).

[29] Proposed §§ 1.13(h)(2)–(3), 23.603(h)(2)–(3).

[30] Proposed §§ 1.13(h)(5), 23.603(h)(5).

[31] Proposed §§ 1.13(i)–(j), 23.603(i)–(j).

[32] *See* Final Rule, System Safeguards Testing Requirements, 81 FR 64272 (Sept. 19, 2016) (covering DCMs, SEFs, and SDRs); Final Rule, System Safeguards Testing Requirements for Derivatives Clearing Organizations, 81 FR 64322, 64329 (Sept. 19, 2016) (''System Safeguards for DCOs'') (describing the CFTC's approach to system safeguards for DCOs as providing DCOs with ''flexibility to design systems and testing procedures based on the best practices that are most appropriate for that DCO's risks'').

[33] *C.f., e.g.,* System Safeguards for DCOs, 81 FR 64322–23; 17 CFR 39.18(b)(3) (requiring DCOs to follow generally accepted standards and best practices with respect to the development, operation, reliability, security, and capacity of automated systems).

[34] Presentation, Futures Industry Association, Business Continuity Disaster Recovery Test, at 4 (Aug. 23, 2023), *https://www.fia.org/sites/default/files/2023-10/FIA_DR_Test_Briefing_2023_1010_0.pptx.*

[35] Summary Report, Futures Industry Association, 2022 FIA Industry-Wide Disaster Recovery Test, at 4 (Dec. 16, 2021), *https://www.fia.org/sites/default/files/2023-05/2022_DR_Test_Results_v2.pdf.*

[36] The Board of The International Organization of Securities Commissions, Thematic Review on Business Continuity Plans with respect to Trading Venues and Intermediaries (May 21, 2021), *https://www.iosco.org/library/pubdocs/pdf/IOSCOPD675.pdf.*

[37] *Id.* at 1.

[38] Financial Stability Oversight Council, 2002 Annual Report, at 37 (Dec. 16, 2022), *https://home.treasury.gov/system/files/261/FSOC2022AnnualReport.pdf.*

[39] The Financial Stability Board, Effective Practices for Cyber Incident Response and Recovery, at 1 (Oct. 19, 2020), *https://www.fsb.org/wp-content/uploads/P191020-1.pdf.*

[40] The Board of The International Organization of Securities Commissions, Cyber Task Force: Final Report, at 3 (June 19, 2019), *https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf.*

[41] The Board of The International Organization of Securities Commissions, Policy Recommendations for Crypto and Digital Asset Markets Consultation Report, at 39 (Nov. 16, 2023), *https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf.*

vote by the parent committee in the first quarter of 2024. DCOs already retain responsibility for meeting regulatory requirements when entering into contractual outsourcing arrangements;[42] the question now is how DCOs should be required to assess and monitor the risks associated with doing so.

Such a rule should in my view broadly track the rule for FCMs and swap entities proposed today, but deep consideration must be given to the ways in which the core DCO business differs. For example, DCOs already occupy a quasi-oversight role with respect to their clearing members; should a rule on third-party risk require DCOs to consider not only the risk posed by their own outsourcing contracts, but also require that DCOs consider their clearing members' third-party risks, perhaps as an aspect of a DCO's assessment of its counterparty risk? How else might the rule differ given the disparity between DCOs' and FCMs' relative frequency of interaction with end users? How might these rules coordinate with prudential regulators?

A cyberattack on a third party that affected FCMs last winter was already disruptive enough, but given their status as SIFMUs some DCOs are quite literally systemically important entities. DCOs serve irreplaceable market functions, and we need update their operational resilience requirements to take into account this new conception of third-party risk. I look forward to the new MRAC workstream diving into this critical issue, and of course to what Division of Clearing and Risk staff might bring forward in an eventual proposed rulemaking.

I once again commend the staff of MPD on their tremendous effort bringing forth this proposed rule, and look forward to hearing the thoughts of my fellow Commissioners.

Appendix 4—Statement of Commissioner Christy Goldsmith Romero

Today we have before us our first proposed cyber and operational resilience rule that would apply to swap dealers (including banks) and futures commission merchants (FCMs). I'm excited to see the proposed rule up for vote today. I support the rule and thank the staff for their more than one year of hard work. I also thank all who engaged with us in an extensive collaborative effort. I also thank Chairman Behnam for entrusting me to help with this rule.

This is a critical rule for the CFTC. FBI Director Christopher Wray recently said ''that today's cyber threats are more pervasive, hit a wider array of victims, and carry the potential for greater damage than ever before'' and we face ''some of our most complex, most severe, and most rapidly evolving threats.'' [1] This rule proposes to help advance our markets from a mentality of incident response to one of cyber resilience. This would further President Biden's White House National Cybersecurity Strategy and Executive Order on Improving the Nation's Cybersecurity.[2]

Cyber resilience is one of my top priorities, and a critical issue on which I am engaged. Over the last year, the CFTC staff and I have been engaged with the White House, other financial regulators, the Department of Commerce's National Institute of Standards and Technology (NIST), the National Futures Association (NFA), swap dealers, FCMs, trade groups like the Futures Industry Association, the International Swaps and Derivatives Association, and the Securities Industry and Financial Markets Association, public interest groups, and third-party vendors. I also sponsor the Technology Advisory Committee that covers cybersecurity, and has a dedicated Cybersecurity subcommittee stacked with well-regarded cybersecurity experts.[3]

It takes this type of collective public and private engagement to thwart cybercrime, stay ahead of the continuously changing threat, and protect our nation's critical infrastructure. Director Wray has spoken about how malicious cyber actors seeking to cause destruction are working to hit us somewhere that's going to hurt—U.S. critical infrastructure sectors.[4] According to the FBI, in 2021, there were ransomware incidents against 14 of the 16 U.S. critical infrastructure sectors.[5] That includes an attack on Colonial Pipeline that led to gas shortages, and an attack on the world's largest meat supplier JBS, that led to meat shortages and spiking prices.[6]

As Director Wray has said, ''ransomware gangs love to go after things we can't do without.'' [7] Our nation cannot do without the commercial agriculture, energy, metals, and financial markets, on which derivatives markets are based.

In June, I presented five key pillars of cyber resilience, pillars that are contained in the proposed rule: [8]

1. A proportionate and appropriate approach;
2. Following generally accepted standards and best practices;
3. Elevating responsibility through governance;
4. Building resilience to third-party risk; and
5. Leveraging the important work already done in this space, including by prudential regulators and NFA.

Taking a Proportionate and Appropriate Approach

There is no one-size fits all approach. The proposed rule would require swap dealers and FCMs to ensure that their operational resilience programs are appropriate and proportionate to the nature and risk profile of their business. This follows the White House National Cybersecurity Strategy.[9] Our swap dealers include Globally Systemically Important Banks (GSIBs). Additionally, some of our swap dealers and FCMs are involved in U.S. critical infrastructure such as in the energy or agricultural sectors, or in supply chains.

FBI Director Wray testified before Congress this month that one of the most worrisome facets of state-sponsored adversaries is their focus on compromising U.S. critical infrastructure, especially during a crisis, and that there is often no bright line that separates where nation state activity ends and cybercriminal activity begins.[10] He testified about the disruptive impact of a supply chain attack in the SolarWinds attack, conducted by the Russian Foreign Intelligence Service.[11] This summer, Director Wray said that the FBI is seeing the effects of Russia's invasion of Ukraine here at home, as the FBI has seen Russia conducting reconnaissance on the U.S. energy sector.[12]

Director Wray also has said that, ''China operates on a scale Russia doesn't come close to. They've got a bigger hacking program than all other major nations combined. They've stolen more American personal and corporate data than all nations combined.'' [13] Director Wray has said that ''the Chinese government has hacked more than a dozen U.S. oil and gas pipeline operators, not just stealing their

[42] 17 CFR 39.18(d) (2022) (providing that registered entities such as DCOs retain responsibility for meeting relevant regulatory requirements when entering into contractual outsourcing arrangements).

[1] *See* FBI, *Director Wray's Remarks at the Mandiant/mWISE 2023 Cybersecurity Conference* (Sept. 18, 2023).

[2] The E.O.'s policy statement of policy is ''Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.'' The White House, Executive Order on Improving the Nation's Cybersecurity (May 12, 2021).

[3] *See* CFTC, *Commissioner Goldsmith Romero Announces Technology Advisory Committee Subcommittee Co-Chairs and Members* (July 14, 2023); *see also* CFTC Technology Advisory Committee July 18 Meeting (July 18, 2023); CFTC Technology Advisory Committee March 22 Meeting (March 22, 2023).

[4] *See* FBI, *Director's Remarks to the Boston Conference on Cyber Security 2022* (June 1, 2022).

[5] See FBI, FBI Partnering with the Private Sector to Counter the Cyber Threat, Remarks at the Detroit Economic Club (Mar. 22, 2022).

[6] *See Id.* (discussing how an attack led to Colonial shutting down pipeline operations and a panic among people in the Southeast that led to a run on gas and how an attack on JBS resulted in a complete stoppage of meat production, leading to spiking prices and less availability of meat).

[7] See FBI, Director's Remarks to the Boston Conference on Cyber Security 2022 (June 1, 2022).

[8] Commissioner Christy Goldsmith Romero, *Advancing from Incident Response to Cyber Resilience,* (June 20, 2023).

[9] *See* The White House, *National Cybersecurity Strategy* (March 2023) (recommending that organizations ''demonstrate a principles-based approach that is sufficiently nimble to adapt to meet the challenges of the ever-evolving technological threat landscape and to fit the unique business and risk profile of each individual covered entity.''

[10] *See* FBI, Statement of Christopher A. Wray Director Federal Bureau of Investigation Before the Committee on the Judiciary United States Senate (Dec. 5, 2023).

[11] See Id.

[12] *See* FBI, *Director Wray's Remarks at the FBI Atlanta Cyber Threat Summit* (July 26, 2023).

[13] *See* FBI, Director's Remarks to the Boston Conference on Cyber Security 2022 (June 1, 2022).

information, but holding them, and all of us, at risk.'' [14] Swap dealers and FCMs involved in critical infrastructure sectors will need to build resilience for these cyber threats.

The proposal also recognizes that cyber resilience requires continuous attention. What is appropriate or proportionate may change with the changing threat vector. It may also change when a swap dealer or FCM enters a new line of business, onboards a new vendor, or takes other action that can carry cyber risk.

Following Generally Accepted Standards and Practices

The proposal, like the CFTC's rules for exchanges and clearinghouses, would require swap dealers and FCMs to follow generally accepted standards and industry best practices, like NIST or ISO (for international companies). The NIST Cybersecurity Framework creates a clear set of cybersecurity expectations that are risk-and outcome-based rather than prescriptive, and adaptable to the size and types of businesses.[15] These standards are regularly updated to reflect the evolving technology and threat landscape. The proposed rule also requires at least annual assessment, testing and updates to the operational resilience framework.

Elevating Responsibility Through Governance

The vision of the Biden Administration's National Cybersecurity Strategy is to rebalance the responsibility to defend cyberspace by shifting the burden for cybersecurity away from individuals and small businesses, and onto the organizations that are most capable and best positioned to reduce risks.[16] This strategy gets away from vulnerability caused by one person in an organization clicking on the wrong thing that leads to total disruption. The banks and commodity firms this rule would apply to are capable and best positioned to reduce cyber risk and cybercrime losses.

Building cyber resilience requires elevating responsibility to those who make strategic decisions about the business. The stakes for businesses are high. There is potential legal risk, reputational risk, risk to national security, as well as financial risk. In 2022, the FBI reported $10.3 billion in cybercrime losses, shattering the record from the prior year.[17] Tone at the top, including the C-suite's active participation in cyber resilience programs as well as making cyber resilience a top priority, can determine whether an organization will successfully be cyber resilient and operationally resilient.

The proposed rule would require operational resilience plans to be approved annually by a senior leader and for incidents to be escalated promptly. It also would require senior leaders to set and approve the firm's risk appetite and risk tolerance limit. Leaders should make strategic decisions about the risk they are willing to take on, as well as the metrics they will monitor. I am interested in hearing if the proposal's definitions of these terms set a clear expectation and align with generally accepted standards.

Building Resilience to Third-Party Risk

Swap dealers and FCMs routinely rely upon third party (as well as fourth party) service providers to access new technologies and expertise, and for efficiencies in business functions. The rule requires building resilience to third party risk, an issue brought sharply into focus with this year's cyber-attack on third-party vendor ION Markets.

Because third parties create points of entry that need to be secured from cyber criminals, the banking regulators released updated interagency guidance on third party risk management that would apply to many of the swap dealers subject to the proposed rule.[18] The staff and I met with the Federal Reserve, Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency about their guidance and their efforts to promote cyber resilience. Like that interagency guidance, the proposed rule includes an inventory of all third-party service providers, assessments of risk throughout the lifecycle of the third-party relationship, the identification of critical third-parties, and subjects those critical third parties to heightened due diligence and monitoring.

The proposed definition of who is a critical third-party service provider takes a flexible approach, asking entities to consider the impact of a disruption.[19] At his TAC presentation, Todd Conklin, Deputy Assistant Secretary of Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) and TAC member discussed how ION Markets received less scrutiny because it was not treated as a critical third-party vendor by most firms.[20] I look forward to comment.

The CFTC also proposes separate guidance on managing third-party risks. I am interested in commenters' views on this guidance, and whether we have it right for harmonization.

Leveraging the Important Work of Others, Including Prudential Regulators and the NFA

The White House's 2023 Cybersecurity Strategy recommends organizations ''harmonize where sensible and appropriate to achieve better outcomes.'' [21] The proposal recognizes that many of our regulated entities are part of a larger enterprise, with cyber and operational resilience programs managed at the enterprise level, and can use those programs under this rule. I am interested in commenters' views on whether we have achieved appropriate harmonization or whether we need greater harmonization with bank regulators' rules and guidance and NFA guidance.[22]

Stronger Together

We are stronger together. The CFTC is part of coordinated government efforts to learn about and disseminate information about emerging cyber threats. We want to work with our swap dealers and FCMs to help strengthen their operational resilience, especially prior to any disruptive event.

Should a disruptive event occur, resilience requires rapid collaboration among the CFTC and all those who are potentially affected to contain any potential damage and to keep critical market functions running. The proposed rule includes specific requirements for notifying the CFTC of an incident as soon as possible, but no later than 24 hours after detection. I support immediate notification to the CFTC because if we know, we can work with regulated entities and markets to assess and minimize damage, trigger appropriate regulatory and law enforcement action, help in recovery, and protect customers. I note that this time frame and reporting standards differs from other regulators, and look forward to comment.

A two-way flow of information can play a significant role in the ability to build resilience, which means the ability to recover quickly after an attack. According to Deputy Assistant Secretary Conklin, collaboration between the government and industry helped mitigate the impact of the ION Markets attack.[23] The proposal would also require notification to customers and counterparties as soon as possible of attacks that affect them. Early notice helps minimize the impact of an

[14] See FBI, FBI Partnering with the Private Sector to Counter the Cyber Threat, Remarks at the Detroit Economic Club (Mar. 22, 2022).

[15] *See* Presentation of Kevin Stine, Chief of the Applied Security Division at NIST Information Technology Laboratory, ''Managing Cybersecurity Risks,'' CFTC Technology Advisory Committee Meeting (March 22, 2023).

[16] *See* The White House, *National Cybersecurity Strategy* (March 2023).

[17] *FBI,* Internet Crime Report 2022 (March 22, 2023).

[18] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, *Interagency Guidance on Third Party Relationships: Risk Management* (Jun. 6, 2023).

[19] I heard from many banks and brokers that identifying who is a critical third-party service provider is an issue they regularly grapple with, and that it often comes down to specific facts and circumstances, and not just the products and service they provide.

[20] *See* Presentation of Todd Conklin, Deputy Assistant Secretary of Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), ''The Cyber Threat Landscape for Financial Markets: Lessons Learned from ION Markets, Cloud Use in Financial Services, and Beyond,'' CFTC Technology Advisory Committee Meeting (March 22, 2023) (''many institutions didn't even classify [ION Markets] necessarily as a 'critical' third-party vendor. So many firms who onboarded ION didn't use the highest-level scrutiny that they use for their most critical third-party vendors.'').

[21] *See* The White House, *National Cybersecurity Strategy,* (March 2023).

[22] These requirements and guidance include the prudential regulator's Sound Practices to Strengthen Operational Resilience paper, the Interagency Guidelines Establishing Standards for Safeguard Customer Information, and the recently released Interagency Guidance on Third-Party Relationships: Risk Management, as well as NFA guidance on information security, third-party service provider risk management, and notification of regulators and business continuity and disaster recovery.

[23] *See* Presentation of Todd Conklin, Deputy Assistant Secretary of Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), ''The Cyber Threat Landscape for Financial Markets: Lessons Learned from ION Markets, Cloud Use in Financial Services, and Beyond,'' CFTC Technology Advisory Committee Meeting (Mar. 22, 2023).

attack by allowing them to secure their personal data, monitor affected accounts, and make alternative arrangements for accessing critical funds or markets.

If we can all work together, we can harden our defenses, thwart cyber criminals, and protect critical U.S. infrastructure and national security. Together, we can build a safer and more resilient cyberspace.

Appendix 5—Statement of Commissioner Caroline D. Pham

I support the Notice of Proposed Rulemaking on Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants (Operational Resilience Proposal)[1] because I believe this approach is largely consistent with international standards for operational resilience, as well as U.S. prudential regulations and non-U.S. regulations, which have been implemented for several years now. I thank the staff of the Market Participants Division (MPD), especially Pamela Geraghty, Elise Bruntel, and Amanda Olear, as well as Chairman Behnam and Commissioner Goldsmith Romero, for working with me over the past year to address my concerns.

Background

My discussions with MPD staff, formerly the Division of Swap Dealer and Intermediary Oversight (DSIO), in fact date back to 2016 when I was in the private sector. MPD staff have been considering many of the elements of an operational resilience framework for years, including operational risk and cybersecurity risk. I appreciate the staff's focus on all of these important issues that contribute to ensuring that our registrants have robust risk management and compliance programs, and that the CFTC is doing our job to uphold financial stability and protect against systemic risk.

I would like to mention my background and experience, as well as familiarity, with the subject areas covered by the Operational Resilience Proposal to provide context for my efforts to support the development of this Proposal and address my concerns that the CFTC's approach should not be overly prescriptive and generally takes a principles-based approach in recognition of the extensive years-long global implementation of operational resilience requirements by U.S. and non-U.S. regulators and banking organizations.

In my previous roles at a global systemically important bank (GSIB), I have been involved with operational resilience since 2019, including the oversight and coordination of global regulatory advocacy with the Financial Stability Board (FSB) and regulatory authorities such as the U.S. prudential regulators,[2] the Bank of England, and European Union (EU) authorities. I also was on the enterprise-wide operational resilience program steering committee, and I have implemented enterprise-wide programs across a global financial institution across all regions and both institutional or wholesale and consumer businesses.

Among the specific elements encompassed in the Operational Resilience Proposal, I have enhanced the swap dealer and futures commission merchant (FCM) risk management programs. I have drafted an enterprise-wide risk appetite statement. I have implemented the National Futures Association's (NFA) update to its information systems security programs requirements, which addresses cybersecurity risk. I have participated in tabletop exercises, drills, and simulations of responses to cyber attacks. I was the lead from the Compliance department on the third-party risk management program for cross-asset activities or other programmatic aspects across the global markets business. I have enhanced the business continuity and disaster recovery (BCDR) swap dealer policies and procedures and integration with the enterprise-wide continuity of business program. I have delivered training for, respectively, 9,000 and 17,000 employees across nearly 100 countries and multiple languages. I have had a compliance monitoring team that reported directly to me. I have advised on the design and implementation of the enterprise-wide Volcker Rule independent testing program. I was part of global regulatory notification protocols for cybersecurity or other incidents. And also, of course, I have been subject to regulatory examinations on each one of these areas. This practical experience has informed my engagement on this significant rulemaking initiative.

The CFTC's Approach to Operational Resilience Must Be Consistent With International Standards and Prudential Regulations

I am pleased that the CFTC is seeking an approach that is consistent with international standards and best practices for regulators in addressing operational resilience. I will reiterate my previous remarks on the many years of work by policymakers such as the FSB, the Basel Committee on Banking Supervision (BCBS), the International Organization of Securities Commissions (IOSCO), and other regulatory authorities around the world to implement laws, regulations, and standards for operational resilience. Operational resilience, as noted by U.S. prudential regulators in 2020, encompasses governance, operational risk management, business continuity management, third-party risk management, scenario analysis, secure and resilient information system management, surveillance and reporting, and cyber risk management. Regulated entities, including the vast majority of our swap dealers and FCMs that are part of banking organizations, have already implemented comprehensive enterprise-wide operational resilience programs.[3]

Issuing this Proposal can be beneficial to initiate an open process to request information and stimulate dialogue with the public. That is why, although there has been some hesitation or trepidation around what the Commission might do since we are coming onto the tail end of operational resilience implementation globally, I do think it is important that we are taking this step today, because it is critical that the public has the opportunity to provide input on any amendment or expansion of our existing programmatic requirements that is informed by actual experience from risk management and compliance officers, other control functions, and practitioners who have implemented and complied with operational resilience requirements pursuant to other regulations.

Further, as I have noted previously, because the CFTC's rules are often only one part of a much broader risk governance framework for financial institutions, the Commission must ensure that it has the full picture before coming to conclusions to ensure that our rules not only address any potential regulatory gaps or changes in risk profiles, but also to avoid issuing rules that are conflicting, duplicative, or unworkable with other regulatory regimes.[4]

For example, when I last checked earlier this year, the CFTC currently has 106 provisionally registered swap dealers. Of these 106 entities, both U.S. and non-U.S., all but a handful are also registered with and supervised by another agency or authority, such as a prudential, functional, or market regulator. Most of these swap dealers are subject to three or more regulatory regimes.[5]

It is imperative that the Commission and the staff consider how our rules work in practice together with the rules of other regulators, whether foreign or domestic. This key point is easily apparent in looking at the CFTC's substituted compliance regime for non-U.S. swap dealers, where the Commission has expressly found that non-U.S. swap dealers in certain jurisdictions are subject to comparable and comprehensive regulation, and therefore, our rules permit such non-U.S. swap dealers to, for example, substitute compliance with their home jurisdiction risk management regulations to satisfy our risk management program rules under CFTC Regulation 23.600.[6]

Specific Areas for Public Comment

As a preliminary matter, regarding discussion of the CFTC's approach to system safeguards requirements for designated contract markets (DCMs) and derivatives clearing organizations (DCOs) and its impact on the development of today's Operational Resilience Proposal, I note that swap dealers

[1] Because there are no registered major swap participants, as a practical matter, this statement will refer to swap dealers and futures commission merchants (FCMs).

[2] U.S. prudential regulators refers to the Board of Governors of the Federal Reserve System (Fed), the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC).

[3] Opening Statement of Commissioner Caroline D. Pham before the Technology Advisory Committee, U.S. Commodity Futures Trading Commission (Jul. 18, 2023), *https://www.cftc.gov/PressRoom/SpeechesTestimony/phamstatement071823.*

[4] Statement of Commissioner Caroline D. Pham on Risk Management Program for Swap Dealers and Futures Commission Merchants Advance Notice of Proposed Rulemaking, U.S. Commodity Futures Trading Commission (Jun. 1, 2023), *https://www.cftc.gov/PressRoom/SpeechesTestimony/phamstatement060123.*

[5] Id.

[6] Id.

and FCMs are very different from exchanges and clearinghouses. The CFTC should not overly rely upon its approach to the system safeguards rulesets because it is akin to the difference between, for example, the Securities and Exchange Commission's (SEC) Regulation SCI and the U.S. prudential regulators' Heightened Standards for Risk Governance. I believe that the staff has tried to balance these considerations, and I welcome public comment on this approach.

Definitions

Words matter, and it is very important for the Commission to be precise in the words that we use for defined terms. I encourage all commenters to review the Proposal's definitions and advise whether the definitions are appropriate or need to be revised.

Third-Party Relationship Program Guidance

The Operational Resilience Proposal includes an appendix to the rule text with more prescriptive guidance on third-party relationships (third-party risk management). This is unusual because I do not believe that the CFTC has this level of prescriptiveness for any other category of risk, such as credit risk. I question whether this heralds a change to the CFTC's approach to setting forth risk management requirements, and why would the Commission issue prescriptive guidance for third-party risk, but not other risks such as operational risk or market risk.

I also question the approach of issuing Commission guidance, which would have to undergo notice-and-comment rulemaking and that could take a year or two to update, instead of issuing staff guidance, which could be updated more flexibly. I believe that any prescriptive guidance would be more appropriate as staff guidance, not Commission guidance, because staff guidance can be kept up-to-date more easily to address changes in best practices or to adapt to emerging risks. This is similar to how, for example, U.S. prudential regulators update their bank examiners handbook or circulars.

I am interested in public comment on the CFTC's requirements for third-party risk management, and whether it should be issued as Commission guidance or staff guidance.

Risk Appetite

The Operational Resilience Proposal refers to risk appetite, which is a new concept to CFTC regulations. I am interested in whether commenters believe risk appetite is workable under the CFTC's regulatory framework, which is focused on enforcement rather than ongoing supervision. Indeed, I have repeatedly noted that the CFTC lacks a swap dealer examination program. As a consequence, non-material operational or technical issues are the subject of enforcement actions, rather than addressed more appropriately through supervisory findings and exam reports like every other regulatory authority in the world. This makes the CFTC an outlier amongst U.S. and non-U.S. regulators, and therefore prudential concepts like risk appetite may not be workable.

Risk Tolerance Limits

Risk tolerance limits are a requirement under the CFTC's risk management program (RMP) rules for swap dealers and FCMs. The Operational Resilience Proposal also requires risk tolerance limits, but sets forth a different definition and does not refer to the risk tolerance limits under the RMP rules. I am interested in public comment on whether the two differing requirements may cause confusion or can be implemented without any issues.

Annual Attestation

The Operational Resilience Proposal requires an annual attestation by the senior officer, an oversight body, or a senior-level official of a swap dealer or FCM that relies on a consolidated operational resilience program. Such attestation is to the effect that the consolidated program meets CFTC requirements and reflects the risk appetite and risk tolerance limits appropriate to the swap dealer or FCM. I encourage commenters to discuss the attestation requirement and suggest appropriate attestation language.

Substituted Compliance

Under the Operational Resilience Proposal, substituted compliance would be available for non-U.S. swap dealers subject to a comparability determination issued by the Commission. I appreciate the recognition in the Proposal of the importance of a home-host regulator approach to maintaining regulatory cohesion and addressing systemic risk and financial stability. I am interested in whether commenters believe the Proposal presents any cross-border issues in implementation.

Conclusion

I believe in continuous improvement for not only our market participants, but also for the Commission and its regulations, and that is why I would like to thank the MPD staff again for being proactive in thinking about these issues. I want to particularly recognize the leadership of Commissioner Goldsmith Romero in first highlighting these risks and exploring ways to address them through the work of the CFTC's Technology Advisory Committee, which she sponsors.

As I have stated before, the benefit of the CFTC's principles-based regulatory framework is that it can quickly anticipate and adapt to changes in risk profiles or the operating environment. That is why I believe our rules must be broad and flexible enough to be forward-looking and evergreen, because it is simply not possible to prescribe every last requirement for the unknown future. Consistent with international standards, I have discussed the importance of utilizing existing risk governance frameworks and risk management disciplines to identify, measure, monitor, and control emerging risks and new technologies. Swap dealers and FCMs must be vigilant and address new and emerging risks through various risk stripes as appropriate, whether from changing market conditions, technological developments, geopolitical concerns, or any other event, and maintain operational resilience.

With that, I welcome the input from the public comments to inform the Commission and the staff regarding the application of the Operational Resilience Proposal to swap dealers and FCMs, especially those entities that are part of a banking organization and have already implemented operational resilience requirements pursuant to U.S. or non-U.S. regulations.

[FR Doc. 2023–28745 Filed 1–23–24; 8:45 am]

BILLING CODE 6351–01–P