BP Energy Company
201 Helios Way
Houston, TX 77079

April 1, 2024

Christopher Kirkpatrick
Secretary of the Commission
Commodity Futures Trading Commission (CFTC)
Three Lafayette Centre
1155 21st Street NW
Washington, DC 20581

Submitted via email to https://comments.cftc.gov.

Re: Comments of BP Energy Company on Notice of Proposed Rulemaking: Operational Resilience Framework for Futures Commission Merchants, Swap Dealers and Major Swap Participants

Dear Secretary Kirkpatrick:

Please accept these comments on behalf of BP Energy Company ("BPEC") in furtherance of the Commodity Futures Trading Commission's ("CFTC" or "Commission") Notice of Proposed Rulemaking: Operational Resilience Framework for Futures Commission Merchants, Swap Dealers and Major Swap Participants ("Proposed Rulemaking").[1] BPEC, located in Houston, Texas, is a marketer of natural gas and electric power with operations throughout the continental United States, and is a registered swap dealer ("SD") with the CFTC.

- **Background**

The CFTC proposes certain minimum prescriptive requirements that covered entities should meet in establishing, documenting, implementing, and maintaining an Operational Resilience Framework (ORF) designed to identify, monitor, manage, and assess risks relating to three key risk areas that challenge operational resilience:

(i) information and technology security;
(ii) third-party relationships; and

[1] *Notice of Proposed Rulemaking, Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants*, 89 FR 4706 (Jan. 24, 2024) ("Proposed Rulemaking").

(iii) emergencies or other significant disruptions to the continuity of normal business operations as a covered entity (a business continuity and disaster recovery (BCDR) plan).

The CFTC recognizes that many of the covered entities already have advanced programs in place to cover all three of these key risk areas, and that "covered entities vary in size and complexity" and need "flexibility to design RMPs tailored to their circumstances and organizational structures." Nevertheless, the Proposed Rulemaking identifies certain elements that must, at a minimum, be included as part of the risk frameworks and requires that covered entities must document such conformance and provide compliance confirmation by senior leadership.

The CFTC describes the impetus for the Proposed Rulemaking as events such as the COVID pandemic, increased focus on cyber risk, and a ransomware attack on a critical third-party service provider, ION Cleared Derivatives, which disrupted trade settlement and reconciliation in derivatives markets.

- Operational Resilience Frameworks that Contain Policies and Procedures Designed to Ensure Compliance with Applicable Regulatory Rules and are Examined by the National Futures Association (NFA) Requirements Should be Deemed Compliant

BPEC promotes an organizational culture that encourages ethical conduct and a commitment to compliance with the law and company standards, policies and procedures. BPEC employs three lines of defense in managing business risks: (1) formal accountabilities requiring employees at every level to conduct business within their remit in a compliant manner; (2) independent oversight and monitoring of risk frameworks; and (3) periodic certification processes to ensure effectiveness of risk controls. As a covered entity under this Proposed Rulemaking, BPEC supports the Commission's goal "to establish comprehensive risk management practices to mitigate systemic risk and promote customer protection."

BPEC has put into place policies and procedures designed to ensure compliance with existing regulatory requirements and the NFA interpretive notices covering all three risk areas in the Proposed Rulemaking by virtue of being a registered swap dealer and an NFA member company.[2] Currently, in order to ensure BPEC's risk frameworks

[2] NFA regulations already cover the three risk areas included in the Proposed Rulemaking:

- NFA Interpretive Notice 9070 – Information Systems Security Programs Rules | NFA (futures.org)
- NFA Interpretive Notice 9079 – Members use of third-party service providers Rules | NFA (futures.org), which provides, "If a Member outsources a regulatory function, 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. This Interpretative Notice establishes general requirements relating to a

remain fit for purpose, BPEC conducts periodic audits and regular risk assessments to identify vulnerabilities and also responds to NFA and CME questionnaires and interviews. In addition, the NFA performs periodic examinations covering BPEC's policies and procedures. These processes introduce a reasonable mix of providing necessary oversight, while allowing a covered entity like BPEC to tailor its risk frameworks to best control the ever-changing risks it faces in the marketplace.

Also, with respect to information and technology security and business continuity and disaster recovery, BPEC complies with CFTC § 23.600[3] and CFTC § 23.603,[4] respectively. Further, BPEC is a non-FCM clearing member of CME's New York Mercantile Exchange, Inc. (NYMEX) and, therefore, must abide by their process for enforcing information security, which includes a bi-annual risk assessment of BPEC's internal processes. Finally, BPEC's larger organization must comply with (1) the UK Financial Conduct Authority (FCA) SYSC 13.7, which covers all three risk areas covered in the Proposed Rulemaking,[5] (2) similar Technology Risk Management requirements dictated by the Monetary Authority of Singapore (MAS), and (3) upcoming requirements dictated by the European Union's Digital Operational Resilience Act

---

Member's written supervisory framework, which requires Members to address, at a minimum, the following areas: (1) Initial Risk Assessment, (2) Onboarding due diligence, (3) ongoing monitoring, (4) termination, and (5) recordkeeping.

- NFA Interpretive Notice 9052 – Business Continuity and Disaster Recovery Plan Rules | NFA (futures.org)

[3] CFTC § 23.600 c4vi requires BPEC's Risk Management Program to include "operational risk policies and procedures" which must take into account, among other things: (A) Secure and reliable operating and information systems with adequate, scalable capacity, and independence from the business trading unit; (B) Safeguards to detect, identify, and promptly correct deficiencies in operating and information systems; and (C) Reconciliation of all data and information in operating and information systems.

[4] CFTC § 23.603 requires BPEC to have a Business Continuity and Disaster Recovery (BCDR) Framework that outlines the procedures to be followed in the event of an emergency or other disruption of its normal business activities. Such recovery plan must allow the participant to continue or to resume any operations by the next business day with minimal disturbance to its counterparties and the market, and to recover all documentation and data required to be maintained by applicable law and regulation.

[5] FCA SYSC 13.7 requires covered firms to establish and maintain appropriate systems and controls for managing operational risks that can arise from inadequacies or failures in its processes and systems (and, as appropriate, the systems and processes of third-party suppliers, agents and others). In doing so a firm should have regard to:

1. the importance and complexity of processes and systems used in the end-to-end operating cycle for products and activities (for example, the level of integration of systems);
2. controls that will help it to prevent system and process failures or identify them to permit prompt rectification (including pre-approval or reconciliation processes);
3. whether the design and use of its processes and systems allow it to comply adequately with regulatory and other requirements;
4. its arrangements for the continuity of operations in the event that a significant process or system becomes unavailable or is destroyed; and
5. the importance of monitoring indicators of process or system risk (including reconciliation exceptions, compensation payments for client losses and documentation errors) and experience of operational losses and exposures.

(DORA), which will go into effect January 2025. Accordingly, BPEC has significant, long-term experience managing risk frameworks associated with the three areas included in the Proposed Rulemaking.

BPEC supports the role of the CFTC to facilitate reforms that protect all participants and does not oppose adopting new requirements where they are likely to prevent the identified risks from happening. BPEC, however, opposes going through a burdensome and costly exercise that will not add material value. The objective of a successful risk framework is to identify risks and adopt a control framework that is reasonably intended to prevent the identified risks from happening. The CFTC has made no finding that existing risk frameworks are lacking in a manner that would justify requiring covered entities to reassess and repaper their existing risk frameworks. While the CFTC proposal seems to invite flexibility, the requirement to document each element of the risk frameworks and cross-reference it to which elements comply with each stated requirement within the Proposed Rulemaking would be unduly costly and burdensome. The current CFTC requirements and NFA controls are working well to enable a necessary level of oversight along with the appropriate level of flexibility to effectively assess and control these risk areas. Rather than advancing new prescriptive requirements, the CFTC should require covered entities to follow rules that are issued by a registered futures association and, in the absence of such rules, to meet the minimum CFTC requirements.

- To the Extent the Commission Decides to Move Forward with Adopting Its Prescribed Requirements, BPEC Offers the Following Suggestions

1. The CFTC Should Allow for More than a Six-Month Timeframe for Compliance

The CFTC asks respondents whether a six-month timeframe from the date of a final order is sufficient for covered entities to establish, document, implement, and maintain an ORF covering the three defined areas. BPEC supports a longer timeframe for compliance. If finalized as proposed, BPEC anticipates taking several months just to fully understand the requirements and assess what changes may be required to its current risk frameworks and a year or more to develop controls around and document each element of the Proposed Rulemaking.

2. BPEC Supports a Flexible Definition of Senior Officers/Leadership

The Proposed Rulemaking provides that each of the components of the operational resilience framework must be reviewed by senior leadership.[6] Duties of senior leadership would include (1) approving the Operational Resilience Framework annually; (2) reviewing and approving in writing risk appetite and risk tolerance limits annually; (3) receiving notice of breaches and ensuring the CFTC is notified of

[6] Proposed §§ 1.13(c)(1), 23.603(c)(1).

extraordinary, non-business-as usual events; and (4) attesting in writing annually that the consolidated plan meets the CFTC requirements. The Proposed Rulemaking would leave it to a company's discretion to identify a senior official or oversight body and asks for comments on whether they should prescribe which senior officials would qualify.

BPEC supports the proposed flexibility in designating senior officials, where covered entities have discretion to identify qualified employees to act as senior leadership, which is consistent with existing rules for covered entities. Without this flexibility, designating senior officials that will qualify introduces unnecessary complexity. It is appropriate to allow covered entities to select the most qualified employees to act as senior officials under the Operational Resilience Framework based on their governance structure.

3. BPEC Does Not Support Overly Prescriptive Process-Type Requirements Like Annual Documentation and Approval of Each Corresponding Element of the Risk Frameworks

The Proposed Rulemaking asks for comments on whether risk assessments should take place annually or less frequently and whether senior leadership should be required to certify in writing that they have received the results of the risk assessment or approved the results of the risk assessment. The Proposed Rule would require covered entities to perform a comprehensive assessment of Information and Technology Security and Business Continuity and Disaster Recovery Plan programs on at least an annual basis.[7] While the CFTC proposal seems to invite flexibility,[8] the requirement to document each element of the risk frameworks and cross-reference it to which elements comply with each stated requirement within the Proposed Rulemaking on an annual basis will unnecessarily limit the flexibility needed to effectuate successful risk frameworks. These types of onerous requirements are likely to detract from the essential elements of a risk framework and, unless there is clear evidence that such prescriptive processes will enhance the operational resiliency of an entity, they should not be adopted. As such, BPEC would not support rigid annual documentation and approval processes for either the Information and Technology Security or Business Continuity and Disaster Recovery Plan programs.

As mentioned, BPEC currently conducts periodic audits and regular risk assessments to identify vulnerabilities and also responds to periodic NFA and CME examinations of its risk framework. This oversight process is consistent with the existing CFTC requirements and introduces a pragmatic approach to providing necessary oversight, while allowing covered entities to tailor their risk frameworks to

[7] Proposed §§ 1.13(d)(1), 23.603(d)(1); Proposed §§ 1.13(h)(1), 23.603(h)(1).

[8] The Proposed Rulemaking provides that 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 - only to review their existing programs and plans to ensure they meet the minimum requirements of the ORF rule and make any necessary amendments.

best control the ever-changing risks they face in the marketplace. The proposed requirement to document the specifics of each risk framework and how those elements comply with minimum prescribed standards is unnecessary when the current process is working well. If finalized as proposed, BPEC would have to hire a team of individuals to constantly document new controls and cross-reference them to the CFTC requirements. Documenting all of this constant activity in one snapshot of time for senior management review and approval would be unduly, costly and burdensome.

Successful IT Security and BCDR risk frameworks will constantly evolve to incorporate the latest technological advancements and to adapt to learnings from risk events. The nature of these risk areas requires BPEC to perform regular testing, vulnerability scans and controls assessments to respond to new threats and incidents. Further, BPEC engages in regular and recurring risk assessments and penetration testing as issues warrant, not on defined annual schedules. This flexibility is desired and necessary to ensure a covered entity can assess its own internal risks and the likelihood of a risk event, can adopt the most suitable controls, including revising and updating those controls as needed to incorporate the latest technology and individual learnings from risk events, and is not subject to the cost and burden of complying with several different and sometimes conflicting risk control requirements intended to control the same risks.

In addition, flexibility is needed to align the various U.S. requirements and international standards and minimize disruptions across regulatory bodies and jurisdictions. The identified risk areas involve global markets and do not stop at the U.S. border. As mentioned, the bp organization must comply with various global risk management requirements, especially around IT Security, so the CFTC should keep its process-type requirements as flexible as possible to enable covered entities to align their risk frameworks with standards being implemented by other countries and should retain flexibility in its process-type requirements so covered entities are not subject to mis-aligned U.S. obligations. The current requirements enable member companies to tailor their risk frameworks in a manner that can be applied across jurisdictions and meet the intended results.

4. The CFTC Should Not Require Covered Entities to Follow any Particular Standards (e.g., the NIST or ISO Standards)

The CFTC also asks whether it should mandate use of any specific controls, including firewalls, antivirus, and or multi-factor authentication. With respect to IT Security, bp has a global perspective where we have adopted a hybrid approach for the risk framework where we leverage relevant aspects of the National Institute of Technology (NIST) NIST, ISO standards and other information security frameworks. bp, however, is not officially accredited by the NIST or ISO. BPEC prefers the existing level of flexibility where it can adopt the provisions that make sense for the organization and not be forced to implement every NIST and ISO requirement; therefore, BPEC would

not support the CFTC mandating covered entities follow any particular standards like the NIST or ISO standards. In accordance with the above comments, the CFTC should focus on the results it wants from risk frameworks, but not prescribe specific tools companies need to employ.

5. The CTFC Should Clarify its Third-Party Relationship Framework Requirements are Merely Guidance, and Covered Entities Will Not Be Held to Provisions They Cannot Realistically Implement

In the Proposed Rulemaking, 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.[9] The Commission lists numerous relevant considerations a covered entity "should" evaluate when implementing each stage of the risk control framework. Also, the Proposed Rulemaking would impose 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.[10] While BPEC supports conducting rigorous third-party due diligence in order to protect its counterparties and to ensure we remain compliant with CFTC regulations, the Commission has prescribed a lengthy list of obligations that are unrealistic to implement with respect to all third-party vendors.

In a fast-paced market environment, it simply is not realistic to expect vendors to respond to a lengthy list of data and documentation requests prior to contracting and throughout the relationship, or for BPEC to document compliance with each and every listed item and, where the data or documentation is not available, for BPEC to document the limitations of the due diligence, the attendant risks, and any available methods for mitigating them (e.g., obtaining alternate information, implementing enhanced monitoring or controls, and negotiating protective contractual provisions). Business simply could not get done under this scenario. BPEC seeks clarification that these listed considerations are in the form of guidance, that covered entities do not need to document review of every listed consideration, and that covered entities will not be held accountable for following each and every listed consideration. Covered entities remain responsible for rule compliance when contracting with third party service providers and are incentivized to perform adequate due diligence on such providers.

[9] Proposed §§ 1.13(e)(1), 23.603(e)(1).
[10] Proposed §§ 1.13(e)(2), 23.603(e)(2).

6. The CFTC Should Adopt an Exemption or Safe Harbor from the Third-Party Relationship Framework Requirements When a Covered Entity is Dealing with Another Covered Entity or Commission Registrant (e.g., Designated Contract Market (DCM), Swap Execution Facility (SEF) or Swap Data Repository (SDR))

The Proposed Rulemaking provides that each covered entity remains responsible for meeting its obligations under the Commodity Exchange Act (CEA) and Commission regulations.[11] In addition, Commissioner Johnson has called for parallel regulations for other Commission Registrants.[12] Given that these covered entities all have similar obligations to adopt operational resilience frameworks covering the same three risk areas, covered entities should have a safe harbor when dealing with each other and be able to assume that proper procedures are in place to manage these three risk areas.

7. The CFTC Should Include a Materiality Threshold for Notification in the Event of a BCDR Incident and Provide for Flexibility on the Timing of Notification

The CFTC asks for comment on whether the agency should consider including a materiality limiter 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.[13] They also ask for comments on the proposal 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.[14] The Commission indicates it wants a more bright-line notification test that centers on the decision to activate the BCDR plan versus the current system where there have been "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."[15] BPEC supports having a materiality limiter for notifications to the Commission and supports continuation of a "prompt"

[11] Proposed §§ 1.13(e)(3), 23.603(e)(3).

[12] Statement of Commissioner Kristin N. Johnson Regarding the CFTC's Notice of Proposed Rulemaking on Operational Resilience Program for FCMs, SDs, and MSPs | CFTC

[13] The CFTC proposes to establish a new CFTC notification requirement that "would relate to incidents that have an adverse impact, or a covered entity's decision to activate its BCDR plan." *See* paragraph (i) of proposed Commission regulations 1.13 and 23.603.

[14] The Proposed Rulemaking details that "[c]urrent 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." *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.'').

[15] Proposed Rulemaking at p. 4732.

notification requirement for emergencies/disruptions rather than a strict 24-hour timeframe.

BPEC supports continuation of the existing notification provision, which ties CFTC notification to the inability of a swap entity to fulfil a regulatory obligation or an emergency or disruption that will have a significant adverse effect on the swap entity, its counterparties, or the market. In the post-COVID world, activation of the BCDR plan does not have the same disruptive character given employees have learned how to work effectively in an alternative location. The current CFTC regulation strikes the right balance of requiring some level of materiality to the CFTC, the market or counterparties before notification is required.

Also, the CFTC should allow for flexibility in the timing of notifications. Under the proposal, covered entities would need to provide the notification as soon as possible after an incident that puts in danger information and technology security (within 24 hours), a covered entity's determination to activate its BCDR plan (within 24 hours), or any incident that could have adversely affected the confidentiality or integrity of such customer or counterparty's covered information or their assets or positions.[16] BPEC supports added flexibility with respect to notifications rather than a prescribed 24-hour window. In a true emergency, a strict 24-hour time limit for notification may not be practical for all types of events, especially when details are emerging and uncertain and a company is required to ensure they are providing the most accurate information available to their regulator. BPEC supports a more reasonable "as soon as possible" standard rather than a strict 24-hour upper limit.

8. With Respect to the BCDR Risk Framework, the CFTC Should Adopt a More Flexible Approach to Resuming Operations.

The Proposed Rulemaking would require that the BCDR plan be ''reasonably'' designed to continue or resume operations with minimal disruption, which is a change from the requirement that such operations be resumed ''by the next business day.'' The CFTC asks for comments on whether the next business day standard has posed challenges for swap entities to implement. BPEC supports moving away from the next business day standard.

In some cases, circumstances do not allow for an obvious next day solution. BPEC experienced an example where a "next business day" standard could have proven impractical due to a series of unexpected events requiring continuous workarounds to ensure minimal disruption in operations. During the power outages in Winter Storm Uri, employees were already working from home due to COVID. BPEC responded by sending certain employees to a hotel. When the hotel experienced a loss of water due to freezing, BPEC implemented actions such as catering water and food

[16] See paragraph (i)(1)(iii) of proposed Commission regulations 1.13 and 23.63.

to its employees working from the hotel. Had another obstacle hit at the same time or circumstances not aligned in our favor, BPEC's operations could have been disrupted beyond a 24-hour period. However, ongoing effective dialogue with BPEC's regulators was occurring without the need for strict notice requirements.

BPEC agrees that flexibility is warranted and the BCDR plan standard should be ''reasonably'' designed to continue or resume operations with minimal disruption. The focus should be on getting operations back up and running within a reasonable period given the individual circumstances of the event and history indicates that regulators are aware and getting the information that they need related to such events.

Conclusion

Thank you for allowing BPEC this opportunity to comment on this Proposed Rulemaking. Please feel free to contact me at Jennifer.Minnis@bp.com if you would like to discuss these comments further.

Sincerely,

/s/ Jennifer Minnis

Jennifer Minnis
Managing Counsel
Gas and Power Trading Americas, BPEC