FIA PTG
PRINCIPAL TRADERS GROUP

2001 K Street NW, Suite 725, Washington, DC 20006 | Tel +1 202.466.5460

June 5, 2023

Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549

Re: 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
Release No. 34-97142; File No. S7-06-23

Dear Ms. Countryman:

The FIA Principal Traders Group ("FIA PTG")[1] appreciates the opportunity to submit this letter to the Securities and Exchange Commission ("SEC" or the "Commission") in response to the above-captioned rule proposal (the "Proposal or Rule 10").[2] As the SEC considers rulemaking on cybersecurity, FIA PTG recommends following cybersecurity risk management best practices to focus cyber risk efforts, leverage existing market cyber organizations and avoid duplication with other SEC cyber proposals.

Specifically, FIA PTG recommends that the Commission:

- Prioritize critical operations as focus of rule scope and requirements.
- Take into account firm attributes, market structure and service provider due diligence mechanisms as part of reasonably designed policies and procedures.

[1] FIA PTG is an association of firms, many of whom are broker-dealers, who trade their own capital on exchanges in futures, options and equities markets worldwide. FIA PTG members engage in manual, automated and hybrid methods of trading, and they are active in a wide variety of asset classes, including equities, fixed income, foreign exchange and commodities. FIA PTG member firms serve as a critical source of liquidity, allowing those who use the markets, including individual investors, to manage their risks and invest effectively. The presence of competitive professional traders contributing to price discovery and the provision of liquidity is a hallmark of well-functioning markets. FIA PTG advocates for open access to markets, transparency and data-driven policy.

[2] *See* 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, Exchange Act Release No. 97142 (Mar. 15, 2023) [88 FR 20212 (Apr. 5, 2023)] ("Proposal").

- Leverage the Financial Services Information Sharing and Analysis Center (FS-ISAC) for incident reporting and threat analysis.
- Eliminate public disclosure requirements and associated risk in favor of Reg S-P customer notifications.
- Address implementation and enforcement concerns in adopting release.

Prioritize Critical Operations as Focus of Rule Scope and Requirements

Prioritization is an essential component of cyber risk management with NIST recommending prioritization of information and information systems "based on their importance to the goals of an organization and the impact that their inadequate operation or loss may present to those goals."[3] In order to prioritize cybersecurity risk management on a firm's critical operations, FIA PTG recommends explicitly defining this term and using it in the definitions of "information," "information systems," and "significant cybersecurity incident."

As written, the Proposal does not define the term "critical operations" and instead discusses it in the context of significant cyber security incident:

> "Generally, critical operations would be activities, processes, and services that if disrupted could prevent the Market Entity from continuing to operate or prevent it from performing a service that supports the fair, orderly, and efficient functioning of the U.S. securities markets."[4]

Using the discussion above as a guide, FIA PTG recommends including a definition for the term "critical operations" that includes the following components: (1) critical operations directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance; and (2) critical operations are those that have a significant impact on the securities market as a whole or a Market Entity's ability to operate in the securities market: The rationale for the first component is based on Regulation SCI ("Reg SCI") which identifies these functions as being "central to the functioning of the U.S. securities markets."[5] Whereas the second component focuses on those operations that are of a significant impact to the markets as a whole in keeping with the Proposal's discussion above that describes critical operations as those that support the fair and orderly functioning of our markets. Additionally, referring to the securities markets covers any jurisdictional questions by limiting the scope to the U.S. securities markets. This is especially important given that many firms have global, multi-asset class operations and limiting the scope of critical operations to the U.S. securities markets will avoid overlapping requirements.

Including the term "critical operations" in the terms "information" and "information systems" will focus on those systems where disruption would have the biggest impact. FIA PTG recommends updating the definitions of these terms as follows (new text is underlined, deleted text is bracketed):

> Information means any records or data related to the market entity's <u>critical operations</u> [business] residing on the market entity's information systems, including, for example, personal information received, maintained, created, or processed by the market entity.

---

[3] *See* NIST, *Criticality Analysis Process Model Prioritizing Systems and Components* (Apr. 2018), *available* at https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8179.pdf.

[4] *See* Proposal at 88 FR 20233.

[5] *See* 79 FR 72272.

> Information systems means the information resources owned or used by the market entity, including, for example, physical or virtual infrastructure controlled by the information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the covered entity's information to maintain or support the covered entity's critical operations.

By focusing "information" and "information systems" on critical operations, the cyber-related definitions including "cybersecurity incident," "cybersecurity risk," "cybersecurity threat," and "cybersecurity vulnerability" would also be focused on those risks, threats, vulnerabilities and incidents that impact critical operations.

FIA PTG recommends additional modifications to the definition of "significant cybersecurity incident":

> Significant cybersecurity incident means a cybersecurity incident, or a group of related cybersecurity incidents, that:
> (i) Significantly disrupts [or degrades] the ability of the market entity to maintain critical operations; or
> (ii) Leads to the unauthorized access or use of the information or information systems of the market entity, where the unauthorized access or use of such information or information systems results in [or is reasonably likely to result in]:
> (A) Substantial harm to the market entity; or
> [(B) Substantial harm to a customer, counterparty, member, registrant, or user of the market entity, or to any other person that interacts with the market entity.]

Because the term "critical operations" is already part of the definition of "significant cybersecurity incident," no additions are required. However, by eliminating the ambiguous terms "or degrades" and "or is reasonably likely to result in," only incidents where there is an actual impact are included in the definition. FIA PTG also recommends deleting the second prong of the definition that focuses on substantial harm to others. Making such an assessment during an incident may be difficult to ascertain and could distract from doing the forensic analysis required to mitigate and resolve an incident. We note that proposed amendments to Reg S-P and Reg SCI both cover notification and disclosure requirements that impact broker-dealer customers and members of Reg SCI entities.

Take into Account Firm Attributes, Market Structure and Service Provider Due Diligence Mechanisms as part of Reasonably Designed Policies and Procedures

FIA PTG appreciates the Proposal's requirement for reasonably designed policies and procedures based on a firm's attributes but notes that the policies and procedures requirements for non-covered broker-dealers includes the language "taking into account the size, business, and operations of the broker or dealer." We respectfully request that this language be added to the policies and procedures requirement for Covered Entities since the size, business and operations of a firm are relevant to the design of policies and procedures for all firms. Maintaining consistent language for all Market Entities reinforces that policies and procedures should be adapted to a firm's specific

business and these attributes should be taken into account by all firms when conducting risk-assessments and prioritizing resources.

While not discussed in the Proposal, we believe it is important for firms and the Commission to consider the impact of U.S. securities market structure on policies and procedures. Unlike Market Entities that perform initial public offerings or maintain exclusive listings, broker-dealers are not single points of failure. The ubiquity of smart order routing which automates the transfer of order flow from one broker-dealer to another reduces the risk of an overall market disruption. Critical market infrastructure is connected through private lines with executions occurring at secured data centers that have market access controls in place. These elements of our market structure reduce the risk of contagion by isolating the execution process from the public internet and limiting human intervention.

Additionally, with respect to service providers, FIA PTG recommends leveraging multiple mechanisms for service provider oversight. Today, service provider due diligence is performed by many means including conducting surveys and reviewing certifications (e.g., SOC, FedRamp). These methodologies allow broker-dealers the opportunity to collect and analyze information about a service provider's business experience, financial condition, regulatory compliance, risk management and controls, information security, and operational resilience all of which are important elements of service provider oversight. Rather than requiring the repapering of service provider agreements which will be costly and time-consuming both for the implementation of the rule and an ongoing basis, FIA PTG recommends removing this requirement and replacing it with a principles-based requirement requiring that firms have policies and procedures to address service provider cybersecurity risk commensurate with the importance of the service provider in maintaining a firm's critical operations.

Leverage the Financial Services Information Sharing and Analysis Center (FS-ISAC) for Incident Reporting and Threat Analysis

FIA PTG agrees with the Commission that the immediate notification requirement would "allow the Commission and other regulators (if applicable) to begin taking steps to assess the significant cybersecurity incident at that early stage."[6]

However, in discussing the objective of the notice and reporting requirements, the Proposal also states that the notification and reporting requirements:

> "could be used to understand better how significant cybersecurity incidents materialize and, therefore, how Covered Entities can better protect themselves from them and, when they occur, how Covered Entities can better mitigate their impacts and recover more quickly from them. Over time, this database of information could provide useful insights into how to minimize the harm more broadly that is caused by significant cybersecurity incidents, which have the potential to cause broader disruptions to the U.S. securities markets and undermine financial stability."[7]

[6] *See* Proposal at 88 FR 20305.
[7] *See* Proposal at 88 FR 20305.

Given the current and evolving role of the Cybersecurity and Infrastructure Security Agency (CISA) and FS-ISAC in cybersecurity incident reporting, information sharing and threat analysis, FIA PTG questions the need for the SEC to also take on the role of analyzing cybersecurity incidents and providing insights back to the financial services community.

While the Proposal acknowledges the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA),[8] it suggests that the scope of Covered Entities may be different thus justifying the need for the reporting requirements of the Proposal. Given that the CIRCIA rulemaking process is still in progress, FIA PTG recommends that the SEC work with CISA to develop a definition of "covered entity" that is consistent with the Commission's goals for significant cybersecurity incident reporting. CIRCIA also acknowledges the role of Information Sharing and Analysis organizations, like FS-ISAC in incident reporting.[9] Unlike the reporting requirements of the Proposal, FS-ISAC information sharing is two-way. Without such a two-way communication mechanism, we think it is unlikely for Covered Entities to benefit from Rule 10 reporting of other firms impacted by a significant cybersecurity incident caused by the same threat actor.

If the Commission feels that duplicative reporting to the SEC is required, we recommend aligning with CIRCIA and extending the reporting timeframe to 72 hours or provide additional flexibility to firms and apply the "promptly" standard used in Reg SCI. We believe a firm's first priority should be mitigating the incident.

Eliminate Public Disclosure Requirements and associated risk in favor of Reg S-P Customer Notifications

The SEC states that the objective of significant cybersecurity incident public disclosure is to help those doing business with Covered Entities to "assess the effectiveness of Covered Entities' cybersecurity preparations and the cybersecurity risks of doing business with any one of them."[10] FIA PTG questions the ability of the disclosures to achieve those objectives and is concerned that these disclosures will do more harm than good.

In order to avoid garnering attention from threat actors, we believe firms will need to exercise extreme caution in providing cybersecurity risk details to the general public. The proposal anticipates exposing cybersecurity risks that:

> "(1) could disrupt or degrade the Covered Entity's ability to maintain critical operations; (2) could adversely affect the confidentiality, integrity, or availability of information residing on the Covered Entity's

[8] *See* Proposal, 88 FR at note 132.

[9] Not only does CIRCIA acknowledge the role of FS-ISAC, SEC staff has also recognized the importance of this group with respect to achieving greater cyber resiliency. *See* Office of Compliance Inspections and Examinations, Cybersecurity and Resiliency Observations (Jan. 27, 2020) ("In addition to receiving CISA Cyber Alerts, many organizations participate in information sharing groups through industry associations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC, www.fsisac.com). Participation in these information sharing groups provides a mechanism for collaborating across industry and government— providing access to sector specific information about cyber best practices and early warning indicators related to cyber threats. Through such information sharing arrangements, OCIE believes that organizations are able to achieve greater cybersecurity resiliency.")

[10] *See* Proposal at 88 FR 20308.

> information systems, including whether the information is personal, confidential, or proprietary information; and/or (3) could harm the Covered Entity or its customers, counterparties, members, registrants, users, or other persons."[11]

We do not believe it is possible to provide meaningful disclosure about cybersecurity risks that would not also aid threat actors in targeting firms. Cybersecurity risks are kept confidential by firms in order to protect firms and their customers. Neither publicly revealing this information nor providing a generic summary of risks achieves the Commission's objectives with respect to disclosure.

Beyond the risk disclosure, we also have concerns about the public disclosure of details related to significant cybersecurity incidents that might give threat actors, including those responsible for the current incident, valuable information regarding the scope and corrective action taken. We also question why disclosure is focused on significant cybersecurity incidents as opposed to a violation of Rule 10. Even the best prepared firm can be the victim of a Day 0 attack. Rather than disclose incidents, FIA PTG recommends including violations of Rule 10 as part of BrokerCheck disciplinary actions. BrokerCheck is already an established part of an investor's review and violations of the rule itself are a better indication of cyber preparedness.

Given the Commission's desire to protect customers and prospects of broker-dealers, FIA PTG recommends relying on Reg S-P's notifications to impacted customers and BrokerCheck to include violations of Rule 10. If Reg S-P's notification requirement is not timely enough, consider modifying Reg S-P rather than promulgating overlapping and inconsistent requirements as part of this Proposal.

Address Implementation Concerns in Adopting Release

FIA PTG believes an overly broad approach to the scope of this rule is not consistent with cybersecurity risk management best practices that stress the importance of prioritization. Additionally, the more expansive and rigid the proposal, the more implementation time that will be required. If the rule stands as is, we believe firms will need 24 months to implement, with risk assessments, repapering service provider contracts and classifying all information systems taking much of the time. Focusing just on critical operations and offering flexibility with respect to service provider due diligence would bring implementation time down by at least six months. Furthermore, if the rule stands as-is, it will create unnecessary and costly duplication of efforts, compared to the other, more well-established mechanisms mentioned above.

Address Enforcement Concerns in the Adopting Release

Unlike the proposed amendments and adopting release of Reg SCI, the Proposal does not discuss enforcement of the rule or safe harbors. We recommend the adopting release of the Proposal specifically address the enforcement of Rule 10 and mirror Reg SCI in acknowledging that while a significant cybersecurity incident may be probative as to the reasonableness of a Covered Entity's

[11] *See* Proposal at 88 FR 20255.

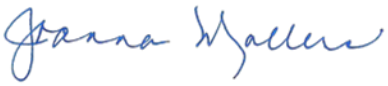
policies and procedures, it is not determinative. Reasonably designed policies and procedures and the other elements of the Proposal can only seek to reduce risk and mitigate the consequences of a breach, enforcement of proposed Rule 10 needs to be clearly articulated as part of the adopting release such that a firm that is a victim of a cyber incident is not automatically in violation of proposed Rule 10. If a firm can demonstrate that it has reasonable policies and procedures, and adheres to the other elements of the Proposal, then post-facto discipline is not appropriate.

*****

FIA PTG encourages the SEC to consider our recommendations intended to focus the Proposal on critical operations and minimize the impact of cybersecurity incidents on the U.S. securities markets. Our recommendations seek to reduce cyber risk and manage the implementation burden of the Proposal. FIA PTG appreciates the SEC's consideration of this comment letter. If you have any questions, please do not hesitate to contact Joanna Mallers at jmallers@fia.org.

Respectfully,

FIA Principal Traders Group



Joanna Mallers
Secretary

cc: Gary Gensler, Chair
Hester M. Peirce, Commissioner
Caroline A. Crenshaw, Commissioner
Mark T. Uyeda, Commissioner
Jaime Lizárraga, Commissioner