INVESTMENT COMPANY INSTITUTE

1401 H Street, NW, Washington, DC 20005-2148, USA
202/326-5800 www.ici.org

November 30, 2020

Ms. Vanessa Countryman
Secretary
US Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549-1090

Re: *Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security (File No. S7-10-20)*

Dear Ms. Countryman:

The Investment Company Institute ("ICI")[1] welcomes the opportunity to share our views on the Securities and Exchange Commission's ("SEC" or "Commission") proposed amendments to the national market system (NMS) plan governing the consolidated audit trail ("CAT") ("Proposal").[2] We appreciate the Commission's commitment to prioritizing CAT data security and confidentiality and, therefore, applaud its efforts to enhance the scope and required standards for CAT data security. On balance, we believe that the proposed amendments would enhance the security and confidentiality of CAT data without undermining the purposes of the CAT. While we express general support for the proposal, we also strongly oppose the continued lack of mandatory breach notification to registered funds.

Our comments also provide several recommendations to the Proposal:

- **Comprehensive Information Security Program**: We support the proposed definition of "comprehensive information security program" (CISP) and its broad application to persons and entities that interact with the CAT. We recommend that a regular review of the CISP

[1] The Investment Company Institute (ICI) is the leading association representing regulated funds globally, including mutual funds, exchange-traded funds (ETFs), closed-end funds, and unit investment trusts (UITs) in the United States, and similar funds offered to investors in jurisdictions worldwide. ICI seeks to encourage adherence to high ethical standards, promote public understanding, and otherwise advance the interests of funds, their shareholders, directors, and advisers. ICI's members manage total assets of US$26.1 trillion in the United States, serving more than 100 million US shareholders, and US$7.7 trillion in assets in other jurisdictions. ICI carries out its international work through ICI Global, with offices in London, Hong Kong, and Washington, DC.

[2] Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security, Release No. 34-89632, 85 Fed. Reg. 65990 (Oct. 16, 2020) ("Proposing Release").

should also specifically examine the permissions and limitations on CAT data access and an assessment of new and ongoing attack threats.

- **Security Working Group**: We strongly recommend that the Operating Committee's Security Working Group also include permanent members that are chief information security officers from advisers to registered funds.

- **Online Targeted Query Tool Download Limit**: We believe that all CAT data should be accessed and analyzed in a Secured Analytical Workspace (SAW) or an approved non-SAW environment, including data obtained via the online targeted query tool. If users are allowed to download CAT data outside of the CAT system, however, then we support limiting the number of downloadable records per query and recommend that the limit be subject to a regular review to ensure that it does not pose data security risks.

- **Customer Breach Notification**: We request that the CAT NMS Plan's breach management policy explicitly require prompt notification to all entities whose trading information may be affected by a CAT data breach, including customers whose data was submitted by another entity to the CAT.

I. Background

ICI continues to support the ongoing regulatory and industry efforts to achieve full CAT implementation. These efforts will provide the Commission and the self-regulatory organizations (SROs) with comprehensive and timely data necessary to conduct effective market oversight and ensure that they operate in a fair, efficient, and orderly manner.[3] Therefore, we appreciate the Commission's amendments to the CAT NMS Plan earlier this year that ensure the transparency of those efforts through mandatory publication of each SRO's CAT implementation plan and quarterly progress reports.[4]

We continue to stress the importance of ensuring robust CAT data security that maintains strict access and limits on the use of CAT data for regulatory purposes only and enforces strong confidentiality provisions. The CAT—which is a vast repository of sensitive position information and trading strategies for all registered funds and other entities active in the U.S. equity and options

[3] We have long supported the CAT, which is a single audit trail that comprises all order and execution information for exchange-listed equities and options. *See, e.g.*, Letter from Karrie McMillan, General Counsel, ICI to Elizabeth M. Murphy, Secretary, Commission (Aug. 9, 2010), *available at* https://www.sec.gov/comments/s7-11-10/s71110-50.pdf.

[4] Amendments to the National Market System Plan Governing the Consolidated Audit Trail, Release No. 34-88890, 85 Fed. Reg. 31322 (May 22, 2020).

markets—has significant commercial value and poses risks to funds and their shareholders.[5] For example, predatory traders or cyber criminals would be able to use CAT data to construct fund position information or reverse engineer fund trading strategies, thereby enabling them to replicate fund portfolios or, in some case, front-run fund trading decisions.[6] Therefore, inadequate CAT data security standards would undermine investor protections and market confidence to the detriment of liquidity and capital formation.

In light of the importance of CAT data security to funds and their investors, ICI has recommended that the minimum data security standards should adhere to three key principles.[7] First, the CAT plan processor's data security program must be able to evolve with current practices to parry cyber threats effectively. Second, the CAT plan processor's cyber policies and procedures should minimize the number of points through which unauthorized access to the CAT could occur, including limited access for necessary personnel only and prohibitions on dispersing CAT data. Third, the cyber policies and procedures should guarantee that all CAT data receive the same level of protection regardless of where the Commission or an SRO accesses it.

ICI supports the Proposal, which aligns closely in many respects with these fundamental principles. The proposed amendments would improve CAT data security by enhancing and clarifying secure CAT data handling and access standards and protocols. These requirements are based on current industry data security standards and, therefore, should be achievable by the plan processor—FINRA CAT—and the SRO plan participants. However, we vigorously oppose the exclusion of customers such as registered funds from the proposed mandatory breach notification requirements. We detail our concerns with the Commission's proposed approach and recommend additional ways in which the Commission should amend the plan to fully achieve our three principles outlined above.

---

[5] The CAT stores, among other things, a unique identification code for each party to an equity or option order or transaction, the time of order entry, execution, routing, or cancellation, symbol, size, side, and price information for all orders, special handling instructions for orders, execution timestamps, and information concerning the price and size of an execution. The central repository will include customer and event information across all markets, from the time of order inception through routing, cancellation, modification, or execution in a single consolidated data source.

[6] We note that Rule 613 of Regulation NMS requires reporting of order information to the CAT on a T+1 basis, even if the order remains open for more than one day. Registered funds occasionally submit orders that take multiple days to fill. Rule 613 of Regulation NMS would require reporting of such an order on a T+1 basis. Therefore, any person that learns of a fund's open or partially filled order could use this information to front-run the fund's trading.

[7] Based on these three principles, we previously provided a specific list of recommendations to enhance CAT data security. These recommendations include (i) a requirement that the CAT NMS Plan employ state of the art cybersecurity practices; (ii) tailored data security provisions that reflect the sensitive nature of CAT data; (iii) storage of CAT data in the Central Repository; (iv) a requirement that the plan processor to notify customers if a data breach compromises their order or trade information; and (v) a requirement that plan participants use CAT Data only for regulatory purposes with strict limits on commercial use. Letter from David W. Blass, General Counsel, ICI, to Brent J. Fields, Secretary, Commission (July 18, 2016) ("2016 ICI Letter"), *available at* https://www.sec.gov/comments/4-698/4698-8.pdf.

II. Comprehensive Information Security Program

The Proposal would refine the scope and standards for CAT information security through a definition of "Comprehensive Information Security Program" that clarifies that the CAT NMS Plan processor must apply the SP 800-53 information security controls developed by the National Institute of Standards and Technology ("NIST") on a broad organization level, not just the Central Repository, as is currently required.[8]

We support the proposed CISP definition, which would ensure that CAT data security standards apply to both internal and external personnel and information systems that interact with the CAT system. Although the Central Repository—where CAT data is received and stored—is already subject to a standard that adheres to the NIST SP 800-53 controls, a significant number of other systems and personnel will also have access to and utilize this information, including through downloading of the data via their own hardware and software systems. Therefore, applying a broad standard consistently across all aspects of the CAT system would reinforce existing data security mechanisms and protocols already in place. Further, it would enhance overall CAT data security by mitigating inconsistent approaches or standards that represent potential vulnerabilities.[9] Importantly, we continue to support applying the NIST SP 800-53 controls as the basis for CAT data security. These controls provide a clear, objective, and auditable way to help owners of critical infrastructure combat cyber threats.

We also strongly believe that the CISP as a whole should be subject to regular review and evaluation, including an audit on CAT data use.[10] Examining all aspects of the CISP on an ongoing basis will enable the plan processor and plan participants to anticipate and quickly respond to new and evolving cybersecurity threats. Accordingly, we support the amended plan's emphasis on monitoring certain aspects of the CISP, such as requiring the plan Chief Compliance Officer (CCO) and the Chief

---

[8] National Institute of Standards and Technology, Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations* (5th rev, Sept. 2020) ("NIST SP 800-53 Controls"), *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[9] The NIST SP 800-53 controls comprise part of the NIST's cyber security framework, which consists of standards, guidelines and practices to promote critical infrastructure protection. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (rev. Apr. 16, 2018), *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[10] The CAT NMS Plan currently requires the plan CCO to oversee the plan participants' regular written assessment of the plan processor's performance, which must be provided to the Commission at least annually and which must include an evaluation of the existing information security program "to ensure that the program is consistent with the highest industry standards for the protection of data." CAT NMS Plan at Section 6.6(b)(i)(B) (effective July 24, 2020), *available at* https://www.catnmsplan.com/sites/default/files/2020-07/LLC-Agreement-of-Consolidated-Audit-Trail-LLC-as-of-7.24.20.pdf.

Information Security Officer (CISO) to review the quantity and type of CAT data extracted to identify potential security risks and perform any corrective measures.[11] This review, however, should also specifically include an examination of the scope of permissions and limitations on CAT data access and mandatory assessment of new and ongoing attack threats against privileged users. Devoting attention to these areas in a CISP audit would inform the Operating Committee about whether the CISP is effectively minimizing system vulnerabilities and whether it reflects the most current and widely accepted industry standards and practices.

III. Security Working Group

The amended CAT plan would require the Operating Committee to maintain a permanent "Security Working Group" to advise the plan's CISO and the Operating Committee on CAT information security matters.[12] These matters include (i) information technology matters pertaining to the CAT's development; (ii) the development, maintenance, and application of the CISP; (iii) the review and application of confidentiality policies; the review and analysis of third-party risk assessments, and (v) emerging cybersecurity topics. The Operating Committee currently relies on such a working group for data security recommendations, and the Commission believes that this mechanism promotes CAT oversight by allowing the group to offer their expertise and views on key information security issues. The members of this group are currently limited to the plan CISO and each plan participant's CISO, but the amended plan would permit them to invite other individual participants.[13] The Commission, however, seeks comment on whether any other parties should be included in the group, such as members of the CAT Advisory Committee.[14]

We strongly recommend that the Security Working Group also include permanent members that are CISOs from advisers to registered funds. Buy-side CISOs have a foremost responsibility to protect their clients' data and, therefore, have an equal interest in ensuring the security of the CAT system. These CISOs can provide significant data security experience related to the protection of data,

---

[11] *See* proposed Section 6.6(b)(ii)(B)(3) of CAT NMS Plan.

[12] We note that such a group currently exists and makes recommendations to the Operating Committee. *See* CAT Security Overview at 3 (Aug. 28, 2019), *available at* https://www.catnmsplan.com/sites/default/files/2020-01/FINRA-CAT-Security-Approach-Overview_20190828.pdf.

[13] The CAT NMS Plan currently allows other individuals with relevant expertise to participate in the working group. *Id.* at 8. As amended, the CISO specifically could include the deputy CISO. *See* proposed Section 4.12(c) of CAT NMS Plan.

[14] Proposing Release at 65995 (Question 5). The CAT Advisory Committee, which advises plan participants on matters related to the Central Repository, consists of various types of broker-dealers and other market participants, including three institutional investors trading on behalf of an investment company or group of investment companies registered pursuant to the Investment Company Act of 1940. CAT NMS Plan at Section 4.13(b)(i)-(xii).

trading strategies and other confidential information for hundreds of thousands of clients.[15] Additionally, they also offer a unique and meaningful perspective on data security matters and, therefore, would further diversify views on key issues in a way that enhances the group's value to the Operating Committee. Earlier this year, several of our members' CISOs had fruitful and productive discussions with the current working group on CAT data security. Based on that experience, we strongly believe that adding buy-side CISOs will ensure more efficient and consistent communication among relevant stakeholders to help the CISP evolve its practices to meet novel cybersecurity threats.[16]

IV. Secure Analytical Workspaces

The Proposal would require the plan processor to create a "Secure Analytical Workspace" that is a CISP-governed "analytic environment account" that plan participants must use (i) to access and analyze customer and account attributes; and (ii) download transaction data via user-defined direct query and bulk extraction tools.[17] The plan processor would provide each participant with a SAW account that implements common technical security controls required by the NIST SP 800-53 controls, unless it is not technologically or organizationally possible.[18] Within each SAW account, each plan participant could provide and use its own CISP-compliant software, hardware configurations, and additional data, but the plan processor would be required to evaluate monitor each plan participant's SAW to ensure that it complies with detailed design specifications.

The amended plan would also permit the plan processor to grant an exception to a plan participant to use a non-SAW environment based on an independent, third-party assessment. The

---

[15] That experience, for example, would allow buy-side CISOs to offer its own perspective on relevant threat scenarios, *e.g.*, potential targeted attacks against privileged individuals or threats of misuse of CAT data for frontrunning or competitive purposes..

[16] Participation on the Security Working Group could be tailored to focus on matters related to protection of CAT data and would not need to address sensitive business matters, such as a detailed review of plan processor policies and procedures or vendor retention. We would be comfortable with the Commission's recommendation that participants sign non-disclosure agreements or comply with protocols designed to prevent the release of confidential information regarding CAT data security matters, or otherwise be subject to a provision in the CAT NMS Plan that imposes confidentiality requirements. Proposing Release at 65993 n.30.

[17] The user-defined direct query and bulk extract tools enable the Participants to download larger sets of data from the Central Repository. CAT NMS Plan at Section 6.10(c)(i)(B) and Appendix D, Section 8.2.

[18] Common security controls, policies, and procedures would be required for at least the following NIST SP 800-53 control families: audit and accountability, security assessment and authorization, configuration management, incident response, system and communications protection, and system and information integrity. Proposed Section 6.13(a)(ii)(A) of CAT NMS Plan. Where it is not possible for the plan processor to implement common security controls, policies, and procedures that align with the Central Repository, *e.g.*, the SAWs may have different functional and technical requirements and may require tailored implementation of controls, each participant may implement those controls in a way particular to their SAW that is consistent with the NIST controls adopted by the plan processor.

participant would be required to show that the non-SAW environment complies with the NIST SP 800-53 controls and associated CISP policies and procedures and has specific requirements to show that the participant's security and privacy controls mitigate the risks associated with extracting CAT data. The plan CISO and the CCO may jointly grant an exception if they determine that the residual risks identified do not exceed risk tolerance levels set forth in the risk management strategy developed by the plan processor pursuant to NIST SP 800-53 controls. Nevertheless, the data that may be accessed in such a non-SAW environment would be limited to transaction data and not customer or account attributes. The Commission believes that an exception is appropriate to afford flexibility to plan participants in how they access CAT data to reduce burdensome costs and/or operational complexity.

We support the mandatory use of a plan processor-developed SAW and SAW accounts to access sensitive customer and account information as well as to use user-defined direct query and bulk extract tools that enable downloading of large data sets. This centralized approach alleviates concerns about the security risks of downloading data by ensuring that more data is accessed and analyzed within the CAT system and subject to CISP policies and procedures.[19] Rather than have plan participants access CAT data in environments with varying degrees of data security, the proposed approach instead promotes greater consistency with common security controls and ensures that downloads and other bulk extraction are subject to security standards equal to those of the Central Repository.

While we agree that there may be cost and operational benefits to allowing non-SAW environments in certain circumstances, we also agree with the Commission's view that the SAW environment still affords the highest level of data protection. Therefore, we support the proposed robust requirements and limitations on the use of non-SAW environments, including an independent third-party assessment and CISO and CCO joint approval,[20] demonstrated compliance with NIST SP 800-53 controls and relevant CISP policies and procedures, restrictions on the scope of accessible data, and an annual review process.

V. Online Targeted Query Tool Download Limit

The Proposal would explicitly limit the amount of CAT data that a regulator could download outside of the SAW via the online targeted query tool[21] to 200,000 records per request. The

---

[19] We previously expressed concerns about the security risks of downloading data and recommended that a user may download CAT data only if the information security measures that would protect the data at the user's site equal or exceed those protecting the data at the central repository. *See* 2016 ICI Comment Letter at 6-7.

[20] However, we request that the Commission clarify how the plan would resolve situations in which the plan CISO and CCO are not able to jointly agree on approving a request to use a non-SAW environment.

[21] The online targeted query tool allows users to carry out focused, narrowly defined queries. *See* CAT NMS Plan at Section 6.10(c)(1)(A).

Commission believes that this limit—intended to prevent large-scale CAT data downloads outside of the SAW—is still sufficiently large to facilitate focused queries in investigations of trading activity.[22] To download and analyze result sets that exceed 200,000 records, regulators would be required to do so within the SAW or an approved non-SAW environment. Further, the amended plan would require the targeted online query tool to log information related to the extraction of CAT data;[23] this information would be included in the plan processor's monthly reports to the Operating Committee, plan participants and the Commission on query performance and data usage. The SEC believes that the proposed limits will still accommodate the targeted searches for which the online targeted query tool was designed, while preventing large-scale downloading outside of the SAW or approved non-SAW environment. The Commission, however, seeks comment on whether plan participants should instead be required to use SAWs when accessing and analyzing CAT data retrieved through the online targeted query tool.[24]

We believe that all CAT data should be accessed and analyzed in a SAW or an approved non-SAW environment, including data retrieved via the online targeted query tool. Adopting such a requirement ensures the same level of protection for all CAT data by promoting a more consistent and controlled approach to CAT data security. However, if the Commission determines to permit users to download CAT data outside of the CAT system, then we strongly support restrictions on the amount of CAT data that can be extracted in such instances. Therefore, we appreciate a proposed limit on the number of records that a user can download to a non-SAW environment. Establishing a limit is consistent with our longstanding view that downloads of CAT data can significantly increase the risks of a CAT security breach. Therefore, we support a requirement that ensures that larger-scale data queries will be subject to NIST SP 800-53 controls under the CISP.

While we acknowledge that the proposed a 200,000-records limit is based on the Commission's goal to facilitate investigatory queries, we also believe that this limit should specifically be subject to an ongoing review to ensure that it achieves the right balance between the goals of maintaining flexibility to conduct focused queries and promoting CAT data security. A 200,000-records limit still creates significant-sized attack surfaces outside of the CAT system that may be vulnerable to breach. As part of the CCO and CISO's ongoing review of CAT data extraction, we strongly urge the plan to enact a

---

[22] The Commission states that based on its experience, a 200,000-record download limit would not prevent regulators from performing many investigations, such as investigations into manipulation schemes in over-the-counter stocks or investigations based on shorter-term trading activity. Proposing Release at 66014.

[23] We note that the CAT NMS plan already requires the targeted online query tool to log submitted queries, query parameters, the user ID of the submitter, the date and time of the submission, and the delivery of results. CAT NMS Plan at Appendix D, Section 8.1.1.

[24] Proposing Release at 65999 (Question 18).

process to regularly evaluate that limit based on download and usage patterns data over time.[25] In addition to using information from the monthly reports, we recommend that the Security Working Group observe these patterns via regular statistical analyses to identify baseline download and usage trends, as well as deviations in the frequency and/or amount of CAT data being downloaded. By tracking the levels and patterns of CAT data usage outside of the CAT system, the Commission and plan processor can determine whether the threshold is appropriate, as well as identify instances of increased risks to CAT data security that would warrant a reduction to the download limit.[26]

VI. Breach Notification

The Proposal would require the plan processor to take (i) corrective action against a data breach that, at a minimum, mitigates potential harm to investors and market integrity; and (ii) devotes adequate resources to remedy the breach as soon as reasonably practicable. The plan processor would be required to notify CAT reporting parties that it reasonably estimates may have been affected by the breach, as well as plan participants and the Commission. However, this notification would need to occur after the processor has a reasonable basis to conclude that a breach has happened. The plan processor, however, could delay such notification if it determines that doing so would likely compromise CAT security or an investigation of the breach. Further, the plan processor would not need to provide notification if it reasonably estimates that the breach would have no impact or de minimis impact on the processor's operations or on market participants.

We request that the CAT NMS Plan's breach management policy explicitly require prompt notification to all entities whose trading information may be affected by a CAT data breach, including customers whose data was submitted by another entity to the CAT. The plan processor should provide such notification or alternatively require that CAT reporting parties notify their respective customers promptly upon notification from the plan processor.[27] As a matter of public interest, customers such as registered funds (and their advisers) and other customers have a right to know if a cyber incident affects the security of their data. We are greatly concerned, however, that the plan as amended still fails to

---

[25] We specifically agree with the Commission that this review should not be limited to CAT data extracted from the SAWs, but also any CAT data extracted via other methods as well, *i.e.*, the online targeted query tool. Proposing Release at 65999 n.74.

[26] For example, if it appears over time that the trends reflect downloads of less than 200,000 records, then the Commission should consider lowering the threshold to ensure that more CAT data is accessed and used within the SAW or an approved non-SAW environment.

[27] A fund's trading data is typically submitted to the CAT by a CAT reporting party, *i.e.*, the broker-dealer executing the fund's trades, and such data may be subject to compromise due to a CAT breach. We note that the Commission previously proposed a notification requirement that would apply to broker-dealers in the case of a data breach involving individuals' sensitive personal information. *See* Regulation S–P: Privacy of Consumer Financial Information and Safeguarding Personal Information, Release No. 34-57427, 73 Fed. Reg. 13692 (Mar. 13, 2008).

explicitly mandate notification to the principal victims of a cyber incident.[28] In fact, the proposed amendments specify other parties that must be notified, including plan participants, CAT reporting parties, and the Commission.[29] As a primary source of CAT data and the party likely to suffer the greatest impact from a data breach, we are troubled by the fact that customers such as registered funds are not entitled to that right as well. Further, this approach appears to be wholly inconsistent with the Commission's previous position, which we support, that the plan processor must notify customers of a CAT breach.[30]

A fund's information about its trading activity and positions are among its most valuable intellectual property; therefore, fund advisors carry out vigorous efforts to protect that data and mitigate threats of exposure from a data breach. While the amended plan would require the plan processor to take corrective action on behalf of investors, we believe that providing prompt notification to registered funds may be an equally effective step to mitigating potential harm. If notified, funds would be able to take their own necessary steps to protect their interests and the interests of fund shareholders. For example, if a fund adviser learns that a cyber incident has exposed details about recent trade data, then the fund could adjust its trading strategies to attempt to protect itself and its shareholders from predatory traders that might have material information about the fund's intentions. Absent such early notification, however, funds and their shareholders would assuredly incur additional significant economic harm that otherwise could have been avoided.

We also note that mandatory breach notification for registered funds would be consistent with NIST SP 800-53 controls and guidance that address incident response and reporting. First, NIST SP 800-53 incident response controls specify that organizations should "address[] the sharing of incident information" and "provide incident information to the provider of the product . . . involved in the

---

[28] The plan currently states that the plan's "cyber incident response plan *may* include . . . [c]ustomer notifications." CAT NMS Plan at Appendix D, Section 4.1.5. The current plan processor also states that it will "notify other parties of unauthorized access to CAT Data where required by law and as it otherwise deems appropriate." FINRA CAT LLC, *Frequently Asked Questions* (updated Mar. 12, 2020), https://www.catnmsplan.com/faq.

[29] In addition to requesting mandatory breach notification, we also request that the Commission set forth clear standards or guidelines in the plan that specify the circumstances or bases upon which a plan processor can exercise discretion to delay or withhold breach notification from market participants.

[30] We note that the Commission previously expected the plan processor to adopt a stronger breach notification requirement when it first approved the CAT NMS Plan. The Commission specifically stated that the plan processor is "responsible for CAT Data, and it will develop a breach protocol and cyber incident response plan that will include notification of breach victims such as Customers, insurance coverage and liability, and details about the distribution of costs." Joint Industry Plan; Order Approving the National Market System Plan Governing the Consolidated Audit Trail, Release No. 34-79318, 81 Fed. Reg. 84696, 84875 (Nov. 23, 2016). The Commission further noted that the plan "explicitly requires customer notifications," though the language as adopted provides flexibility to the plan processor to do so. *Id.* at 84761.

supply chain . . . for systems or system components related to the incident."[31] In this context, registered funds should be viewed as a "supplier" to the CAT of data that should be notified of relevant cyber incidents. Second, NIST SP 800-53 controls specify that an organization's incident response policy should be "consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines."[32] In that light, we observe that most, if not all, states maintain and enforce cybersecurity laws that mandate customer notification where a data breach has occurred.[33] Therefore, we believe that mandatory breach notification to customers such as registered funds would align with standard cybersecurity practices in other areas and, more importantly, with the Commission's primary objective of ensuring investor protection.

VII. CAT NMS Plan Governance

We further recommend that the Commission amend the CAT NMS Plan to include representatives of registered funds and other non-SRO participants to the plan's Operating Committee. As we have previously noted, the actions of the operating committee could profoundly affect trading and order management practices of funds as well as their confidence in the equity markets. Therefore, they have a strong interest in ensuring that the plan processor and central repository adequately protect CAT data in a manner consistent with the interests of long-term investors. Registered fund representation on the Operating Committee not only would ensure that their expertise in protecting trade and order information helps to further enhance CAT data security policy, but it would also complement the value of including buy-side CISOs in the Security Working Group.

* * *

We appreciate the opportunity to provide our views on the Proposal. If you have any questions, please feel free to contact me at (202) 326-5869 or Nhan Nguyen, Counsel, at (202) 326-5810.

---

[31] NIST SP 800-53 Controls, Incident Response Control at Section 3.8, IR-8 (Incident Response Plan). Supply chain incidents include "compromises or breaches that involve information technology products, system components, development processes or personnel, distribution processes, or warehousing facilities." *Id.* at Section 3.8, IR-4 (Incident Handling). NIST further specifies that "[o]rganizations determine the appropriate information to share and consider the value gained from informing external organizations about supply chain incidents, including the ability to improve processes or to identify the root cause of an incident." *Id.*

[32] *Id.* at Section 3.8, IR-1 (Policy and Procedures).

[33] *See, e.g.*, Ca. Civ. Code § 1798.82 (2019). California, for example, requires that an entity that maintains computerized "personal information" that it does not own to provide breach notification to the owner of the personal information "immediately following discovery." Ca. Civ. Code at § 1798.82.

Sincerely,

/s/ Peter G. Salmon

Peter G. Salmon
Senior Director, Technology & Cybersecurity

cc: The Honorable Jay Clayton
The Honorable Hester M. Peirce
The Honorable Elad L. Roisman
The Honorable Allison Herren Lee
The Honorable Caroline Crenshaw

Brett Redfearn, Director, Division of Trading and Markets
Elizabeth Baird, Deputy Director, Division of Trading and Markets
Christian Sabella, Deputy Director, Division of Trading and Markets
David Shillman, Associate Director, Division of Trading and Markets
John Roeser, Associate Director, Division of Trading and Markets