INVESTMENT COMPANY INSTITUTE

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

July 18, 2016

Brent J. Fields
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549

Re: *Joint Industry Plan; Notice of Filing of the National Market System Plan Governing the Consolidated Audit Trail (File No. 4-698)*

Dear Mr. Fields:

The Investment Company Institute ("ICI")[1] welcomes the opportunity to share our views on how the Securities and Exchange Commission ("SEC" or "Commission") can create a consolidated audit trail ("CAT") that will promote transparency, competition, and efficiency in the listed equities and options markets while also protecting the position information and trading strategies of registered funds and other investors. We write to express our concern that the proposed national market system ("NMS") plan to implement the CAT contains inadequate information security measures that leave registered funds' confidential information vulnerable to a data breach.[2] We offer a number of recommendations to address the deficiencies of this information security program. Incorporating our suggestions would decrease the risk that a cyber attack on the CAT harms investors—including registered funds—and would improve the operations and decision-making process of this NMS plan. We and our members stand ready to help the Commission implement our recommendations.

Our comments address three key aspects of the proposed CAT NMS plan: data security and confidentiality, governance, and the format of data reported to the CAT ("CAT data"). Part I of our letter provides context for our support of the CAT and explains why we remain concerned about the confidential information of registered funds. Parts II and III explain how the data security and

---

[1] ICI is a leading, global association of regulated funds, including mutual funds, exchange-traded funds, closed-end funds, and unit investment trusts 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 U.S. fund members manage total assets of $17.9 trillion and serve more than 90 million U.S. shareholders.

[2] *Joint Industry Plan; Notice of Filing of the National Market System Plan Governing the Consolidated Audit Trail*, Securities Exchange Act Release No. 77724 (April 27, 2016), 81 FR 30614 (May 17, 2016) ("Release").

confidentiality provisions of the CAT pose risks to registered funds and their shareholders and identify certain measures that would improve the safeguards of CAT data and prevent its misuse. In Part IV, we examine the governance of the proposed CAT NMS plan and recommend that the Commission adopt a governance structure that includes representatives from industry participants other than SROs, including advisers to registered funds. In Part V, we suggest that the CAT NMS plan ensure that the plan processor accepts data in a commonly used format to increase the quality of reported data and decrease the cost of reporting to the CAT.

I. ICI Supports the Regulatory Need for the CAT but Remains Concerned about the Confidential Information of Registered Funds

To perform its oversight responsibilities, the SEC currently must attempt to cobble together disparate data from a variety of existing information systems that vary in scope, data elements and format.[3] This fragmented approach to order and transaction reporting hinders the gathering of a complete and accurate audit trail that would enhance market oversight and the ability of the Commission to obtain a complete picture of the markets. For example, in the aftermath of the "flash crash" of May 6, 2010, SEC staff had to compile order and trade data from various sources to analyze the unusual market activity. The data sets available to the staff took five months to analyze and contained only approximately 90% of the trade and order activity for that day.[4]

The Commission adopted Rule 613 of Regulation NMS to address the various shortcomings in the completeness, accuracy, accessibility, and timeliness of existing audit trail systems in the U.S. equity and options markets.[5] Rule 613 requires the self-regulatory organizations ("SROs") to work together to create an NMS plan for the creation and operation of the CAT. The Commission now seeks comment on the SRO's proposed CAT NMS plan.

ICI fully supports the Commission's goal of creating a single audit trail comprising all order and execution information for exchange-listed equities and options.[6] We believe that the CAT will provide the Commission and the SROs with comprehensive and timely data necessary to assist them in overseeing the markets and ensuring their fair, efficient, and orderly operation. The CAT should significantly improve the Commission's ability to reconstruct market events (such as the flash crash or the unusually volatile market activity on August 24, 2015), provide an accurate and timely accounting of these events to the public, and formulate an appropriate regulatory response.

---

[3] *See* Release at 30614-15.

[4] *See Consolidated Audit Trail*, Securities Exchange Act Release No. 67457 (July 18, 2012), 77 FR 45722, 45732-33 (August 1, 2012).

[5] *See* Release at 30615.

[6] *See* Letter from Karrie McMillan, General Counsel, ICI to Elizabeth M. Murphy, Secretary, Commission, dated August 9, 2010, *available at* https://www.ici.org/pdf/24477.pdf.

Although we support the objectives of CAT, we believe the CAT poses new dangers to registered funds and their shareholders that the CAT NMS plan must address. Implementing the CAT will require the creation of a central repository containing a vast amount of information about the U.S. equity and options markets. 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.[7] Essentially, the CAT will contain information concerning position information and trading strategy for all registered funds and other entities active in the U.S. equity and options markets.

This treasure trove of order and execution information has tremendous commercial value, and we are gravely concerned that cyber criminals and others will seek to access and use it for their personal gain to the detriment of funds and their shareholders.[8] Predatory traders or cyber criminals could use CAT data to construct fund position information or reverse engineer fund trading strategies, enabling them to replicate fund portfolios or, in some case, front-run fund trading decisions.[9] Any such misuse of CAT data could undermine certain of the benefits that the Commission hopes the CAT will deliver, including improved investor protection and confidence in the capital markets.[10] If investors perceive that the CAT NMS plan leaves their trading strategies and position information vulnerable to discovery and predatory use, interest in equity investing may decrease to the detriment of liquidity and, ultimately, capital formation.

When the Commission proposed Rule 613 of Regulation NMS, we expressed our view that the Commission would need to limit the use of CAT data to regulatory purposes and adopt strong confidentiality protections to ensure the security of CAT data.[11] As described in more detail below, we believe the CAT NMS plan's proposed approach to the information security and confidentiality of CAT data does not go far enough to address or alleviate those concerns. We strongly recommend that the final CAT NMS plan include more stringent standards than the proposal.

---

[7] The CAT will store, 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.

[8] The repository also may attract foreign state actors that have an interest in obtaining a macro view of the equity holdings of U.S. market participants, including registered funds.

[9] We note that Rule 613 of Regulation NMS requires reporting of order information to the CAT on a T+1 basis. 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, even if the order remains open for more than one day. Any person that learns of a fund's open or partially filled order could use this information to front-run the fund's trading.

[10] *See* Release at 30748.

[11] *See* Letter from Karrie McMillan, General Counsel, ICI to Elizabeth M. Murphy, Secretary, Commission, dated August 9, 2010, *available at* https://www.ici.org/pdf/24477.pdf.

II. The Commission Should Enhance the Data Security Provisions of the Plan

SEC Chair Mary Jo White noted recently that cybersecurity is "one of the greatest risks facing the financial services industry"[12] and that the SEC cannot do enough to improve cybersecurity in the U.S. financial markets.[13] We could not agree more. As currently drafted, however, the CAT NMS plan fails to address adequately the threat of a data breach at the plan processor or central repository. The SEC can and should act to increase the cybersecurity measures of the proposed CAT NMS plan.

Despite the highly sensitive nature of the data captured by the CAT, the proposed CAT NMS plan provides only vague details about the information security provisions for the CAT. Given the importance of protecting CAT data, the CAT NMS plan must ensure that the plan processor has robust cyber policies and procedures tailored to the risks faced by the central repository. We understand that certain details of the plan processor's information security program must remain confidential, but the proposed CAT NMS plan sets too low of a bar for information security. The Commission must improve these anemic standards.

We recommend that the Commission consider three key principles in setting the minimum standards for information security. First, the information security program of the CAT plan processor must evolve with current practices to parry cyber threats effectively. No information security program can completely eliminate the threat of data breach, but a dynamic cybersecurity program stands a better chance than a static one. Second, the cyber policies and procedures of the plan processor should reduce the opportunities for breach by minimizing the number of points through which a cyber criminal could access CAT data. In addition, the information security program likely will better protect the data if it limits access to necessary personnel and prohibits dispersal of the data. Third, the cyber policies and procedures should guarantee that all CAT data receive an appropriate level of protection regardless of its location. In other words, CAT data should receive the same level of protection regardless of where the Commission and SROs use it.

In keeping with these principles, we seek four specific changes to the CAT NMS plan that would greatly improve data security as described below.

A. The CAT NMS Plan Should Employ State of the Art Cybersecurity Practices

We strongly urge the Commission and the plan participants to update the proposed CAT NMS plan to account for cybersecurity developments since the Commission adopted Rule 613 of

---

[12] *See* Chair Mary Jo White, Securities and Exchange Commission, *Keynote Address Investment Company Institute 2016 General Meeting – The Future of Investment Company Regulation* (May 20, 2016), *available at* https://www.sec.gov/news/speech/white-speech-keynote-address-ici-052016.html.

[13] *See* Lisa Lambert, "SEC Says Cyber Security Biggest Risk to Financial System," (May 18, 2016), *available at* http://www.reuters.com/article/us-finance-summit-sec-idUSKCN0Y82K4.

Regulation NMS in 2012. Specifically, we recommend that the final CAT NMS plan employ state of the art information security practices, such as the cybersecurity framework developed by the National Institute of Standards and Technology ("NIST") and the cybersecurity assessment tool created by the Federal Financial Institutions Examination Council ("FFIEC"). We also suggest that the final CAT NMS plan require the plan processor to implement an information security program that assesses and responds continually to threats. Implementing these practices should ensure that the information security program that protects CAT data remains current and enables the plan processor to detect and react expediently to any security breach.

The NIST's 2014 cybersecurity framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The NIST framework provides an objective, repeatable, and cost effective way to help owners of critical infrastructure combat cyber threats. It incorporates leading practices from various information security standards and is emerging as a standard in the financial industry.[14] We do not understand why the plan participants appear not to have considered this framework in crafting the data security and confidentiality provisions of the proposed plan, but the final CAT NMS plan should reflect the evolving nature of cyber security standards, including the NIST framework.[15] Although compliance with the NIST cybersecurity framework will not guarantee that the plan processor will operate an effective information security program, it would provide some assurance that the plan processor's information security program rests on a solid foundation.

We further recommend that the CAT NMS plan require the plan processor to evaluate regularly its information security program. We believe that the final plan should require the plan processor to use a cybersecurity assessment tool, such as the one prepared by the FFIEC in 2015, as one component of its information security program review process.[16] Cyber security assessment tools help institutions identify their risks and determine their cybersecurity maturity, and we believe the plan processor could use such a tool to assess its preparedness to respond to cyber threats and ensure that the central repository meets certain minimum, widely recognized cybersecurity thresholds.

Finally, effective information security programs today assess cyber threats proactively and address systems vulnerabilities to reduce the likelihood of a data security breach on a continuous basis. To that end, we recommend that the CAT NMS plan require the plan processor to employ information security measures that ingest information about cyber threats from a variety of forums,

---

[14] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, February 12, 2014, *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[15] We note that Section 6.5(f) of the proposed plan would require the information security program of the CAT NMS plan to employ state of the art technology. We support this requirement, but respectfully request that the Commission also require the plan's information security program to follow state of the art practices to safeguard CAT data.

[16] Federal Financial Institutions Examination Council, Cybersecurity Assessment Tool, June 2015, *available at* https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf.

synthesize the information, and provide actionable information to the operations teams of the plan processor. Similarly, the plan processor's information security program should include capability that regularly scans and tests the plan processor's network and the network of the central repository to identify and remediate security vulnerabilities. The final plan also should require the plan processor to retain an independent third-party to test and audit its information security program. To ensure that the information security program remains current, the plan processor should update all aspects of the program on an annual basis.

B. The Commission and Plan Participants Should Tailor the Information Security Provisions of the Plan to Reflect the Sensitive Nature of CAT Data

The proposed CAT NMS plan appears to classify CAT data in only two ways: data that contains personally identifiable information ("PII") and data that does not contain PII.[17] PII data would receive a higher level of protection than non-PII data. We believe that this dichotomy creates the misimpression that all non-PII data merits less information security protection than PII data. In fact, certain non-PII data, such as the majority of order information, and certain execution information, contains critical information about fund trading strategies that the plan processor must protect zealously. We encourage the Commission to require the CAT NMS plan to include additional levels of data classification to protect adequately commercially sensitive non-PII data.

Providing more granular data classifications would enable the plan processor to implement a risk-based information security program that applies different types of security controls commensurate with the inherent sensitivity of reported data. We believe that the central repository should store CAT data in a segmented manner—on separate networks with security controls that correspond to the sensitivity of the information stored in each segment. Segmenting data in this manner would enable the plan processor to ensure that the most sensitive data receives the highest level of protection. The CAT NMS plan should require the plan processor to work with market participants, including registered funds and their advisers, to determine the sensitivity of data in determining the appropriate classifications.

C. CAT Data Should Remain in the Central Repository

The proposed plan contemplates that plan participants could implement the CAT in a way that would "(1) require regulators to download entire data sets and analyze such data within the regulator or the regulators' cloud or (2) permit regulators to analyze sets of data within the CAT using applications or programs selected by the Commission."[18] We urge the Commission to reconsider the proposal to allow regulators to download CAT data to their own systems.

---

[17] The proposed CAT NMS plan would define PII data to include a social security number or tax identifier number or similar information. *See* Release at Exhibit A, Section 1.1.

[18] Release at 30648 (Question 193).

CAT data should remain in the central repository. Requiring, or even permitting, regulators to download CAT data increases exponentially the risk of a security breach that would expose CAT data, including data regarding registered funds' holdings and trading strategies. If the final CAT NMS plan requires all CAT data to remain in the central repository, plan participants and the plan processor could adopt robust security measures designed to protect CAT data in a single location. Protecting CAT data becomes enormously more difficult if the final plan permits each plan participant and the SEC to download CAT data because a cyber criminal could target CAT data in up to 20 additional locations.[19] Permitting CAT users to download and store CAT data also would complicate efforts to manage a breach of CAT data. If a data breach occurs at the site of a participant, the plan processor would learn of the breach only after the participant goes through its breach management and notification policies and procedures. These processes may result in the plan processor learning of a breach later than if the breach occurred at the central repository, or containing the breach less effectively, which could greatly harm registered funds and other victims of the breach.

Notwithstanding these significant issues, if the Commission determines to permit the final plan to allow users to download CAT data, the data security and confidentiality provisions of the plan should apply to downloaded data. Specifically, the plan should provide 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.

D. The CAT NMS Plan Should Require the Plan Processor to Notify Customers if a Data Breach Compromises Their Order or Trade Information

Currently, the CAT NMS plan does not contain meaningful policies and procedures for responding to a data breach. An appendix to the proposed plan would require the plan processor to "develop policies and procedures governing its responses to systems or data breaches," including a cyber

---

[19] The proposed CAT NMS plan has 19 participants (although the final plan likely will have 20 participants, due to the Commission's approval of IEX as a national security exchange). If the final plan permits participants and the SEC to download CAT data, a cybercriminal might seek to access CAT data by targeting any of 21 locations: the 19 participants, the SEC, or the central repository. By contrast, if the final CAT NMS plan requires participants and the SEC to use CAT data in the CAT, a cyber criminal would have only one place to access CAT data—the central repository. Although we do not have specific concerns about the information security program in place at any participant, we note that recent high-profile cyber attacks on financial market participants emphasize the need for all market participants to adopt strong information security programs. We also note that two recent reports have uncovered weaknesses with the SEC's own information security policies. *See* U.S. Securities and Exchange Commission, Office of Inspector General, *Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2015* (June 2, 2016), summary *available at* https://www.sec.gov/oig/reportspubs/Audit-of-the-SECs-Compliance-with-the-Federal-Information-Security-Modernization-Act-for-Fiscal-Year-2015.pdf (finding that the SEC's information security program contained a number of weaknesses, including outdated policies and procedures); United States Government Accountability Office, *Information Security: Opportunities Exist for SEC to Improve Its Controls over Financial Systems and Data* (April 2016), *available at* http://www.gao.gov/assets/680/676876.pdf.

incident response plan, which the operating committee of the CAT NMS plan must approve.[20] The proposed plan does not require the plan processor to notify customers of cyber incidents that compromise their data. We recommend that the final plan provide a clear mechanism for promptly notifying all victims of a CAT data breach.

Registered funds (and their advisers) and other customers have a right to know if a cyber incident affects the security of their data, so that they can take necessary steps to protect their interests and the interests of fund shareholders. For example, if a registered fund learns that a cyber incident has exposed details about recent trade data, 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. Moreover, ensuring that customers learn of data breaches will incent the plan processor and plan participants to adopt robust data security and confidentiality protections to avoid the embarrassment and reputational damage that could accompany a data security lapse.

III. The Commission Must Ensure That Plan Participants Use CAT Data Only for Regulatory Purposes and Limit Strictly Commercial Use of Raw Data

The CAT will enable the Commission and plan participants to view trade and order information for registered funds and other end users of securities. Because of the sensitive nature of this information, the Commission must limit its use to regulatory purposes. We therefore support the provision of the proposed plan that would permit individuals to use data stored in the central repository only for regulatory and surveillance purposes.[21] We ask the Commission to confirm that this requirement also would apply to plan participants.[22] No individual or entity should have any right to access, repackage and sell CAT data to others or to exploit it commercially in any other fashion. We urge the Commission to examine regularly plan participants for compliance with this requirement and to address immediately any violations.

To reduce the possibility of an authorized person misusing CAT data, we suggest that the CAT NMS plan contain the following three elements.

- Controlling Access to the Central Repository: The plan processor and central repository should impose tight controls on access to CAT data. At a minimum, the plan processor should know the identity of each individual CAT user and should have the capacity to restrict a user's ability to view and manipulate data. To affect this

[20] *See* Release at Appendix D, Section 4.1.5.

[21] *See* Release at Exhibit A, Section 6.5(f).

[22] Rule 613(e)(4)(i)(A) of Regulation NMS applies to plan sponsors as well as to their employees. In relevant part, the rule provides that "[a]ll plan sponsors and their employees…agree not to use [data reported to the central repository] for any purpose other than surveillance and regulatory purposes."

standard, we recommend that the final CAT NMS plan require the plan processor to implement identity and access management capabilities that enable the plan processor to manage the provisioning, auditing and recertification of access by users.

- Requiring Information Security Training for Users: The CAT NMS plan should require the plan processor, plan participants, and the Commission to train all employees and contractors with access to CAT data on how to maintain the security and confidentiality of the data.[23] The proposed CAT NMS plan would require the CAT to support a minimum of 3,000 regulatory users—an extraordinary number—that will have access to view and analyze CAT data.[24] Each of these access points represents a potential security risk.[25] The Commission and plan participants would reduce the likelihood of a data breach due to human error by training all CAT users to protect CAT data prior to granting access to the CAT and at least yearly thereafter. To ensure that CAT users understand their information security obligations, we recommend that the training program require all users to pass a test demonstrating their knowledge of, and attest that they will comply with, applicable policies and procedures. The Commission, plan participants, and plan processor should have the authority and obligation to revoke the access privileges of any user that fails to complete required training or otherwise puts CAT data at risk.

- Informing the Commission of Misuse of CAT Data: To ensure that the Commission learns promptly of any unauthorized use of CAT data, the Commission should modify Section 6.5(f)(iii) of the proposed plan to require the plan processor and each plan participant to report to the Commission any breach of the data confidentiality or security provisions of the CAT.[26]

---

[23] This recommendation would strengthen the requirement in Section 6.1(m) of the proposed plan, which would require the plan processor to implement a training program that "will be made available to all individuals who have access" to the central repository. Making a training program "available" to individuals will not protect CAT data nearly as well as requiring every CAT user to complete the training program.

[24] *See* Release at Appendix D, Section 8.1.

[25] For example, a CAT user could leave data open on a computer screen or connect a laptop containing CAT data to a public wireless network.

[26] Section 6.5(f)(iii) of the proposed plan would require each participant and the Commission to report any breach of the security of the CAT to the chief compliance officer of the plan processor within 24 hours of becoming aware of such breach. The proposed plan does not provide a mechanism for ensuring that the Commission also receives notification of any breach of CAT security. We favor requiring the party at the source of the breach to inform the Commission to ensure that the Commission learns of the breach as quickly as possible. Alternatively, the final plan could require the chief compliance officer of the plan processor to report details concerning any breach of the security of the CAT to the Commission within 24 hours of becoming aware of the breach.

For data that plan participants report to the CAT, the proposed CAT NMS plan would provide participants with more flexibility. Specifically, the proposed plan would permit a participant to commercialize the "raw data" that it reports, provided that applicable law does not forbid this use.[27] We understand this provision aims to preserve the ability of plan participants to generate revenue from selling information about the trades and orders that occur on their markets.

We recommend two modifications designed to ensure that plan participants do not use the CAT NMS plan to enlarge the scope of data that they commercialize.[28] First, the final plan should specify that no participant may commercialize customer identifying information, regardless of whether applicable law expressly prohibits its commercialization.[29] The commercialization or public dissemination of customer identifying information would destroy investor confidence by broadcasting the trading strategies of registered funds and other investors to predatory traders and others who would seek to profit from this information. The CAT NMS plan should prohibit commercialization of this data. Second, the CAT NMS plan should limit the scope of data subject to commercialization by narrowing the definition of "raw data" to include only data that a participant must report under Rule 613 of Regulation NMS or the CAT NMS plan. The proposed definition of "raw data" could include any information that a participant reports on behalf of another CAT reporter—such as another exchange or a broker-dealer—which would expand inappropriately the scope of information subject to commercialization by plan participants.

IV. The Plan's Proposed Governance Structure Is Deeply Flawed

As with other NMS plans, the CAT NMS plan will have a significant effect on all market participants.[30] Regrettably, the governance structure of the proposed CAT NMS plan, similar to other NMS plans, deprives a broad range of market participants, including registered funds and their advisers, of any meaningful voice in plan operations by limiting the membership of the plan's operating

---

[27] *See* Release at Exhibit A, Section 6.5(h). "Raw data" would include the data that CAT reporters deliver to the CAT before the CAT system has validated or otherwise checked the data.

[28] ICI members have deep concerns about plan participants' sale of market data, the fees charged for this information, and the rates at which these fees have increased in recent years. We believe the Commission can and should act to provide market participants with access to relevant market data on fair and reasonable terms, but the Commission should assess market data separately from the CAT. We strongly oppose any effort to use the CAT NMS plan as a mechanism to expand the scope of data eligible for commercialization by exchanges. Further, we ask the SEC to clarify that exchanges enjoy no immunity from lawsuits relating to security breaches of commercialized data. When an exchange sells its market data it does so as a commercial participant, not as a regulator.

[29] We note, for example, that "raw data" would include a participant-designated ID for each customer. *See* Release at Exhibit A, Section 1.1.

[30] *See* Letter from Paul Schott Stevens, President & CEO, ICI, to Mary Jo White, Chair, SEC, dated November 30, 2015, *available at* https://www.ici.org/pdf/29517.pdf.

committee to SROs.[31] The proposed plan charges the operating committee with managing the plan, acting on behalf of the plan, and "mak[ing] all decisions and authoriz[ing] or otherwise approv[ing] all actions" taken by the plan.[32] The proposed plan would provide non-SRO representatives with seats on an advisory committee, but this committee would have "no right to vote on any matter" considered by the operating committee.[33] We vigorously object to the proposed governance framework because (as with other NMS plan governance frameworks) it fails to take any account of the interests of non-SROs and the potential contributions non-SROs could make to plan operations.[34]

We recommend that the Commission add representatives of registered funds and other non-SRO participants to the operating committee of the CAT NMS plan. No legal authority requires SROs to monopolize the operating committee of the CAT NMS plan, and we urge the Commission not to permit this single class of market participants to control all trade and order information for the U.S. equity and options markets. The perspective of other market participants— particularly given that the central repository will house their sensitive information—would help in the development and maintenance of the CAT. If the Commission declines to grant non-SRO market participants seats on the operating committee, we believe it should—at a minimum—enhance greatly the role of the plan's advisory committee to provide non-SROs a more meaningful voice in operating the CAT.

A. The Commission Should Modify the Governance Structure of the Proposed Plan to Reduce Conflicts of Interest and Improve Data Security and Confidentiality

We believe that the work of the CAT NMS plan's operating committee would be far better informed if it included representatives from a broad range of market participants, including registered funds and their advisers. Unlike SROs, registered funds buy and hold securities to deliver long-term returns to shareholders. The actions of the operating committee could affect profoundly trading and order management practices of registered funds and affect registered funds' confidence in the equity markets. Moreover, any breach of CAT data likely will compromise registered fund position information and trading strategies to the detriment of fund shareholders. Registered funds today fiercely protect this critical information and adding registered fund representation to the operating committee of the CAT NMS plan would ensure that their expertise in protecting trade and order information helps formulate the data security policy of the central repository and the plan processor. As fiduciaries, advisers of registered funds have a unique interest in making sure that that the plan processor and central repository protect adequately the data reported to the CAT. This perspective could improve CAT operations for all equity market stakeholders by ensuring that the CAT operates in a manner consistent with the interests of long-term investors.

---

[31] *See* Release at Exhibit A, Section 4.2.

[32] *See* Release at Exhibit A, Section 4.1.

[33] *See* Release at Exhibit A, Section 4.13(d).

[34] *See* Release at Exhibit A, Article IV.

Expanding operating committee representation to include non-SROs also could improve the security and confidentiality of CAT data by mitigating potential conflicts of interest inherent in the proposed governance framework. The proposed CAT NMS plan contemplates that SROs will control the operating committee for the plan, use CAT data for regulatory purposes and, potentially, commercialize the information that they report to the CAT. These roles may, at times, present conflicting incentives for SROs. Adding a broader range of market participants to the operating committee of the plan would ensure that not all operating committee members have such conflicts of interest. Registered funds, for example, would have no use—regulatory or otherwise—for CAT data, but they would have a deep interest in ensuring the security, confidentiality and appropriate use of all data reported to the CAT. If the CAT NMS plan included registered fund representatives on its operating committee, those representatives would have greater incentives to ensure data security and confidentiality. This focus therefore would provide a balance to SRO incentives for greater marketability of, and accessibility to, the data.

B. The Commission Should Increase the Role of the Plan's Advisory Committee

If, despite every reason to the contrary, the Commission excludes all non-SROs from the governance structure, it at a minimum should require the CAT NMS plan to include a stronger advisory committee. The proposed plan would require that the advisory committee consist of at least one representative from twelve different categories of market participants, including various types of broker-dealers.[35] The plan would provide that the advisory committee have at least two representatives of institutional investors, one that trades "on behalf of a public entity or entities" and one that trades "on behalf of a private entity or entities."[36] Members of the advisory committee would have the right to attend meetings of the operating committee and receive information concerning the operation of the central repository—except for executive sessions—but would have no right to vote on any matter considered by the operating committee, as noted above.

Although distinctly less preferable than representation on the operating committee, every NMS plan—including the CAT NMS plan—at least should include an advisory committee comprising a broad range of industry participants that lack operating committee representation. The Commission could enhance the utility of the advisory committee for the proposed CAT NMS plan by requiring this committee to include more investor representation, including representation from registered funds. We also believe that the Commission should clarify that the vague reference in the proposed CAT NMS plan to institutional investors that invest on behalf of "public" or "private" entities includes advisers to registered funds.

---

[35] *See* Release at Exhibit A, Section 4.13(b).

[36] *See* Release at Exhibit A, Section 4.13(b).

To ensure that the operating committee thoroughly considers views of the advisory committee, we recommend that the CAT NMS plan include a requirement for the operating committee to respond in writing to any recommendations of the advisory committee and to provide a written rationale—to the advisory committee and to the Commission—for not accepting advisory committee recommendations. To ensure that advisory committee members remain informed of pertinent information, the advisory committee should receive all documents prepared for or submitted to the operating committee by the plan processor or central repository. If the operating committee wishes to withhold a document from the advisory committee, the plan should require that: (1) a majority of the operating committee votes to deem the document confidential; and (2) the operating committee provide the title of the document to the advisory committee along with a justification of the operating committee's confidentiality determination. We also believe that the advisory committee should participate fully in all operating committee discussions concerning data security or confidentiality and should, without exception, receive the same reports from the plan processor's chief compliance officer and chief information security officer that the operating committee receives.

V. The CAT NMS Plan Should Specify that the CAT Will Leverage Existing Data Formats to Reduce Costs to Market Participants

The proposed CAT NMS plan does not require CAT reporters to provide data to the central repository in any particular format. The proposal instead contemplates that the plan processor—when selected—will determine the electronic format for reported data.[37] The proposed plan would require CAT reporters to report data to the central repository in a format or formats specified by the plan processor, approved by the operating committee, and compliant with Rule 613 of Regulation NMS.[38] We generally support the proposal to permit the plan processor to determine the electronic format of reported data, but we recommend that the final plan require the plan processor to choose an electronic format widely used by industry participants, such as FIX or SWIFT. Requiring the plan processor to accept reports in a format already prevalent in the financial industry should reduce costs associated with implementing the CAT NMS plan and provide regulators with more consistent and higher quality data in the near term.

* * *

We appreciate the opportunity to provide our views on the proposed CAT NMS plan. We share the Commission's view that cyber security represents one of the greatest challenges facing the financial industry, and we encourage the Commission to act now to improve the data security and confidentiality provisions of the proposed plan. We also urge the Commission to reconsider the governance provisions of the proposed plan to provide meaningful voice to funds and other market participants and to provide a richer perspective to the operating committee. Finally, we recommend

---

[37] *See* Release at Exhibit A, Sections 6.3 and 6.4.

[38] *See* Release at Exhibit A, Sections 6.3 and 6.4.

that the Commission ensure that the plan processor accepts data in widely used industry formats to improve the quality of reported data and reduce costs associated with reporting to the CAT. If you have any questions on our comment letter, please feel free to contact me at [redacted], Jennifer Choi, Associate General Counsel, at [redacted], or George Gilbert, Counsel, at [redacted].

Sincerely,

/s/ David W. Blass

David W. Blass
General Counsel

cc: The Honorable Mary Jo White
The Honorable Kara M. Stein
The Honorable Michael S. Piwowar

Stephen Luparello, Director, Division of Trading and Markets
Gary Goldsholle, Deputy Director, Division of Trading and Markets
David Shillman, Associate Director, Division of Trading and Markets