December 4, 2020

VIA EMAIL (rule-comments@sec.gov)

Ms. Vanessa Countryman
Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

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

Dear Ms. Countryman:

The Participants of the CAT NMS Plan appreciate the opportunity to provide comments on the Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to enhance data security[1] published by the Securities and Exchange Commission ("SEC" or "Commission") on August 21, 2020.[2] The Participants have implemented robust protections to protect the security and confidentiality of CAT Data, and share the Commission's view that CAT Data reported to and retained in the Central Repository currently is subject to stringent security policies, procedures, standards and controls.[3] The Commission notes that the security of the CAT should remain an ongoing focus,[4] however, the Participants note that the Commission does not explain how the security of the CAT would be materially enhanced by the Proposed amendments. The Participants also believe that, by substantially limiting the ability of the Participants to access CAT Data, the Proposed Amendments will hamper the Participants' ability to perform their self-regulatory responsibilities. Moreover, the Participants believe the Proposed Amendments will significantly increase the cost and extend the timeline for the implementation of the Consolidated Audit Trail ("CAT"), particularly as it relates to the

[1] Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security, Exchange Act Release No. 89632 (Aug. 21, 2020), 85 Fed. Reg. 65991 (Oct. 16, 2020) (the "Proposing Release").

[2] The registered national securities exchanges and national securities association (collectively, the "Participants") formed Consolidated Audit Trail, LLC ("CAT LLC") to implement the requirements of Rule 613, promulgated under the Securities Exchange Act of 1934, as amended ("Exchange Act"). Rule 613 requires the Participants to create the CAT NMS Plan. The Limited Liability Company Agreement of Consolidated Audit Trail, LLC is the CAT NMS Plan. The twenty-five Participants of the CAT NMS Plan are: BOX Exchange LLC ("BOX"); Cboe BYX Exchange, Inc., Cboe BZX Exchange, Inc., Cboe EDGA Exchange, Inc., Cboe EDGX Exchange, Inc., Cboe C2 Exchange, Inc. and Cboe Exchange, Inc. (collectively, "Cboe"); Financial Industry Regulatory Authority, Inc. ("FINRA"); Investors' Exchange LLC ("IEX"); Long-Term Stock Exchange, Inc. ("LTSE"); MEMX LLC ("MEMX"); Miami International Securities Exchange LLC, MIAX Emerald, LLC, MIAX PEARL, LLC (collectively, "MIAX"); NASDAQ BX, Inc., Nasdaq GEMX, LLC, Nasdaq ISE, LLC, Nasdaq MRX, LLC, NASDAQ PHLX LLC, The NASDAQ Stock Market LLC (collectively, "NASDAQ"); and New York Stock Exchange LLC, NYSE American LLC, NYSE Arca, Inc., NYSE Chicago, Inc. and NYSE National, Inc. (collectively, "NYSE"). Unless otherwise noted, capitalized terms are used as defined in Rule 613, in the CAT NMS Plan, or in this letter.

[3] *See* Proposing Release at 65991 ("CAT Data reported to and retained in the Central Repository is thus subject to what the Commission believes are stringent security policies, procedures, standards and controls.").

[4] The Proposing Release notes that, notwithstanding the stringent security policies and procedures, the Commission believes that it can and should take additional steps to further protect the security and confidentiality of CAT Data. *Id.*

implementation of the proposed Secure Analytical Workspace ("SAW"). The Participants also believe that the proposal will raise additional security issues for the CAT.[5]

Specifically, the Proposed Amendments present significant issues that, if adopted, would materially impact the timely development and implementation of a secure CAT System. In particular, and as described herein, the Participants believe:

1. the Commission's estimated costs in the Proposing Release significantly underestimate the likely costs of the Proposed Amendments;

2. the Proposed Amendments could not be reasonably implemented within the time frame set forth in the Proposing Release;

3. the Proposed Amendments would divert the Plan Processor's resources from focusing on the current development and implementation of the CAT, which would materially and adversely affect implementation timelines;

4. the Proposed Amendments would delay the retirement of Participants' existing duplicative rules and systems, thereby imposing on additional costs and a prolonged period of duplicative regulatory reporting on Industry Members;

5. requiring the Participants to bring their own data into the CAT for analysis in the AWS environment provided by the Plan Processor would greatly increase the security risks associated with the CAT;

6. the Proposed Amendments would significantly impact the timing for satisfying the requirements related to the Financial Accountability Milestones for Periods 3 and 4 under the CAT NMS Plan;[6]

7. the Proposed Amendments envision an inappropriate role for the Plan Processor in overseeing the regulatory activities of the Participants; and

8. the current composition and operation of the current Security Working Group, including discretionary consultation of industry representatives, has worked well to protect the security and confidentiality of CAT Data. Adding industry representatives as permanent participants on the Security Working Group would unnecessarily enhance the risks to CAT Data.

The Participants also note that the Plan Processor, FINRA CAT, LLC, has submitted its own, detailed comments concerning these and other issues related to the Proposed Amendments.[7]

---

[5] The comments set forth in this letter represent the consensus of the Participants, but each Participant reserves the right to submit its separate views to the Commission.

[6] *See* CAT NMS Plan, Section 11.6(a)(i)(C), (D).

[7] *See* Letter from Shelly Bohlin, President & Chief Operating Officer, FINRA CAT, LLC, to Vanessa Countryman, Secretary, SEC (Dec. 2, 2020).

I. The Current Security Profile of the CAT is Robust

The Participants believe, and as noted in the Proposing Release, the Commission has concurred that a robust security system has been developed and implemented for the CAT. The Participants, in concert with the Plan Processor, regularly assess the security of the CAT, and actively consider whether and how the security of the CAT can be enhanced on an ongoing basis. Without a clear understanding of how the proposals will materially enhance the current security profile of the CAT, it is difficult to assess them from a cost benefit perspective or in light of the impact they would have on the Participants' ability to complete the scheduled development and implementation of the CAT or to perform their self-regulatory functions. Given the acknowledged stringent security of the CAT, as well as these and other concerns discussed below, the Participants recommend that the SEC not move forward with the proposal.

II. The Commission's Cost Estimates Significantly Underestimate the Cost of Implementing and Operating the Proposed Changes to the CAT

Based on discussions with the Plan Processor, the Participants believe that the Commission has significantly underestimated the costs that would be involved in implementing the proposed SAW environment as well as the impact of the proposal. For example, the Commission's Proposed Amendments would fundamentally change the nature of the CAT in a manner that was not previously contemplated, and this fundamental shift in purpose and function was not factored into the SEC's cost estimates. Proposed Section 6.1(d)(v) of the Plan would require the Plan Processor to provide for each Participant a SAW account that implements all common technical security controls required by the Comprehensive Information Security Program ("CISP").[8] With this new requirement, the Plan Processor would need to create and staff an entirely new line of business to provide infrastructure and security delivery services for the Participants and Commission to conduct their regulatory surveillance activities. The Plan Processor also would be required to build and support multiple, separate SAW environments for each Participant and the Commission (*e.g.*, development, quality assurance, certification test, production, and disaster recovery). Additionally, the Plan Processor would need to provide tools and processes that allow for the development, promotion, and operation of the Participants' and Commission's regulatory software and data across these multiple environments.

The Commission believes it will cost approximately $441,600 in initial costs and $860,200 in ongoing annual costs to develop and implement the SAWs.[9] The Commission notes that these costs must be incurred regardless of whether any Participant chooses to work within SAWs.[10] The Proposing Release also provides cost estimates if all Participants work within SAWs versus working in non-SAW environments that have been granted an exception from the proposed SAW usage requirements pursuant to proposed Section 6.13 of the Plan ("Excepted Environment"). The Commission preliminarily estimates that Participants working within a SAW would incur $61.6 million in total initial costs and $32.8 million in total ongoing annual costs, including base costs.[11] The Commission preliminarily estimates Participants working in

---

8 *See* Proposing Release at 65996.
9 Proposing Release at 66076.
10 *Id.*
11 *Id.*

Excepted Environments would incur $4.9 million in total initial costs and $4.7 million in total ongoing annual costs.[12]

The Commission's estimates summarized above – related to initial and ongoing annual costs to develop and implement the SAWs, as well as initial and ongoing costs to work within the SAWs or Excepted Environments – are much too low. For example, the Plan Processor estimates the labor costs alone to build the proposed SAW would be approximately $26.4 million, an amount more than 60 times greater than the Commission's estimate of $441,600. Similarly, the Plan Processor estimates that the annual cost of operating the proposed SAW would be approximately $34.4 million, an amount more than 40 times greater than the Commission's estimate of $860,200. The Plan Processor believes that these are *conservative* estimates of the cost differential with the Commission's estimates.[13] Importantly, the Proposing Release also does not consider significant costs related to identifying and hiring additional qualified staff, developing and building a new system, and significantly expanding the staffing and capabilities of the Plan Processor's help desk.

The Proposing Release also does not consider the non-labor costs associated with implementing the SAWs. Additional non-labor costs would include, among others, costs related to: (1) Plan Processor software and tools, licenses and subscriptions; (2) SAW delivery services (*e.g.*, development tools, identity/authentication platforms, logging, monitoring, etc.); (3) networking; (4) security services; (5) Plan Processor provided networking equipment, licenses and subscriptions; (6) Plan Processor AWS service fees; (7) insurance (*e.g.*, CAT System and directors and officers liability insurance); and (8) third-party audit and security services (*e.g.*, independent verification and validation testing, penetration testing, Regulation System Compliance and Integrity, and third-party audits).[14] Although the Plan Processor's cost estimates are preliminary due to the open ended nature of the Proposed Amendments, the Participants have significant concerns that the costs to implement the Proposed Amendments far exceed the cost estimates set forth in the Proposing Release.

In addition, the Proposing Release does not consider the costs related to securing the Participants' proprietary software and monitoring the Participants' regulatory programs. With no standardization of the Participants' software, the Plan Processor likely would need to significantly expand its security staff by hiring individuals with the knowledge of Participants' regulatory systems, expertise needed to secure such a wide set of technologies and to satisfy any new service level agreements entered into with the Participants. As noted above, the Plan Processor also would need to establish new operations and help desk services for each

---

12 *Id.*

13 Note, the cost estimates set forth herein are based on the Participants' and Plan Processors' current understanding of the proposal and could materially change as additional facts come to the attention of the Participants or the Plan Processor. As noted, the Participants' comments with respect to costs are based on discussions with the Plan Processor, and the Plan Processor determined its cost estimates based on discussions with its Engineering, Development and Tools, Networking Operations and HelpDesk teams, among others.

14 The Plan Processor believes the non-labor costs will be substantial and cannot be estimated as they are dependent upon factors beyond its control, such as Participant and Commission data types and volumes, compute volumes, and software. Moreover, the Plan Processor currently leverages existing technology and resources from FINRA, the parent company. In the event that the Plan Processor is no longer able to leverage these resources, the costs for implementing the SAW will increase exponentially.

Participant and the SEC across their multiple SAW accounts, each of which will present its own set of security risks and challenges in identifying and hiring qualified staff. The Plan Processor also likely would be required to expand the security of the Participants' tools and existing software.

Finally, the cost analysis does not consider the effect of the increased costs on Industry Members. As the CAT NMS Plan contemplates Industry Members contributing to the costs of the CAT, Industry Members will be required to contribute to the increased CAT costs related to the Proposed Amendments. Given the significant additional costs, the Participant believe that Industry Members will face materially increased CAT fees.

III. Timeline and Resources

The Commission proposes to amend the CAT NMS Plan by adding proposed Section 6.1(d)(v), which would require the Plan Processor to provide SAWs to the Participants in accordance with proposed Section 6.13.[15] The Proposed Amendments further provide that the requirements of proposed Section 6.1(d)(v) must be met no later than 120 days from the effective date of the Proposed Amendments.[16] The Commission views this timeframe as sufficient for the Plan Processor to establish the Participants' SAWs, noting that the Plan Processor has been authorized to build similar environments for some of the Participants since November 2019 and, therefore, the Plan Processor will have already achieved interim elements of SAW implementation.[17]

The Participants believe the Commission significantly underestimates the time that will be needed to implement the proposed SAW. The Plan Processor estimates that it will need to hire a significant number of qualified personnel, at least doubling its current staff, to implement the Proposed Amendments and that it will take at least 12 months to hire such staff to address both the SAW and non-SAW requirements of the Proposed Amendments. These personnel would be hired to: (1) build, develop and maintain the AWS platform; (2) run a 24/7 development help desk and AWS-focused operations center; and (3) provide security and compliance functions in support of the CAT Chief Information Security Officer ("CISO") and CAT Chief Compliance Officer ("CCO").[18] From the time that the Plan Processor hires and onboards additional qualified personnel, the Plan Processor estimates that it would take a minimum of 18 months to build and develop both the SAW and non-SAW aspects of the

---

15 *Id.* at 66053.

16 *Id.* at 66053.

17 *Id.*

18 The Participants understand that the Plan Processor's hiring process could take longer if the Plan Processor needs to hire additional personnel to research and understand the Commission's and Participants' unique regulatory needs and related software. In addition, this review process assumes the Participants will be transparent in sharing their "source code" to allow the Plan Processor to determine whether they are free of security defects and to determine what technology is necessary to permit use of Participant software in the SAW. To the extent that the Plan Processor cannot access such source code or other sensitive proprietary information – whether owned directly by a Participant or licensed from a third party (that may have contractual or other legal obligations barring it from sharing such information) – it may not be possible for the Plan Processor to satisfy the requirements of the Proposed Amendments. The Participants note that the Proposed Amendments would not apply to the Commission. Excluding the SEC from CAT security requirements generally may enhance the security risk of the CAT. Accordingly, the Participants believe that it should be clear that neither the Participants nor the Plan Processor are responsible or liable for the SEC's CAT activity.

proposed amendments. The Plan Processor also would need to implement the controls, policies, and procedures consistent with the NIST SP 800-53 based controls, policies, and procedures the Plan Processor has already implemented for the CAT System. This would be a significant endeavor and entail standardization of infrastructure, software development lifecycle, and operational practices, processes and controls by the Participants and the Commission, and could take at least several months of effort to scope and define.

The Participants also will need time to migrate their regulatory programs to this new platform. This would require the Plan Processor to address the following for each Participant: (1) support architectural changes to the Participants' networks; (2) migrate significant amounts of the Participants' data into the Plan Processor's system; (3) migrate the Participants' application portfolios into the Plan Processor's architecture; (4) migrate the Participants' service development lifecycles ("SDLCs") to a common Plan Processor platform, which would include the SDLC security controls as required by the proposed CISP; (5) update all policies and procedures, including policies and procedures related to software selection, integration, and software libraries, and standards that would need to be agreed upon by the Participants and the Commission; (6) establish security monitoring, tooling, threat hunting capabilities based on unique characteristics across arbitrary technologies unique to each Participant and the Commission; and (7) update records management and data protection policies, procedures, and practices. As part of this migration, all of the data that a Participant currently uses in its regulatory and surveillance program will have to be migrated to the new SAW platform, including personally identifiable information ("PII"), which the Commission, Participants and industry have sought to remove from the CAT System.[19]

The Proposed Amendments would be material, significant, and would go far beyond the scope of current requests for similar secure analytical environments ("PP SAW"), necessitating that the Participants and the Plan Processor to negotiate and enter into an entirely new Plan Processor Agreement. The Participants previously authorized the Plan Processor to develop and implement a PP SAW that would give the Participants and the SEC an option to connect a workspace to the Central Repository to analyze CAT Data and run their surveillance protocols. The PP SAW also would provide regulators with another means of accessing and analyzing CAT Data in a secure workspace, but regulators would not be limited to accessing and analyzing CAT Data only in the PP SAW. In addition, unlike the Central Repository, the PP SAW would not be within the sole control of the Plan Processor; each regulator would administer its own PP SAW account, including, the implementation of its own security controls.[20]

The Proposed Amendments, however, would introduce new requirements that are fundamentally different than the PP SAW. For example, under the Proposed Amendments, the SAW would be "an analytic environment account that is part of the CAT System, and subject to the Comprehensive Information Security Program, where CAT Data is accessed and analyzed as part of the CAT System pursuant to proposed Section 6.13."[21] In addition, the Plan Processor would be required to provide a SAW account for each Participant that implements all common

---

[19] *See, e.g.*, Exchange Act Release No. 88393 (Mar. 17, 2020), 85 FR 16152 (Mar. 20, 2020).

[20] *See* Letter from Michael Simon, CAT NMS Plan Operating Committee Chair, to Hon. Jay Clayton, Chairman, Commission, at 4-5 (Nov. 27, 2019).

[21] Proposing Release at 65995.

technical security controls required by the CISP.[22] As noted, the Participants believe that these changes are so significant that they would require the negotiation of a new contract with the Plan Processor. Such negotiations would be complex, costly and time consuming. Additionally, the Plan Processor may need to renegotiate existing agreements with various third-party vendors (*e.g.*, leveraged technology and business services, security, development, operations tools and licenses), adding additional complexities.

IV. Adverse Effect on Implementation of the CAT

The Participants believe that the Proposed Amendments would divert the Plan Processor's resources from focusing on the current development and implementation of the CAT. This would materially and adversely affect currently projected implementation timelines. For example, the development of the AWS platform to meet the requirements of the Proposed Amendments would divert senior Plan Processor personnel (*i.e.*, the CISO and CCO, Chief Technology Officer, Chief Operating Officer, and delivery and operations teams (technology and security)) away from their current responsibilities, including focusing on the development of Phases 2c, 2d and Customer and Account Attributes of the CAT build and implementation. As a result, the Proposed Amendments are likely to delay the implementation of final CAT implementation phases, which would delay the availability of certain CAT Data and functionality to regulatory users. Therefore, at a minimum, any commencement of the implementation of the Proposed Amendments ultimately adopted by the Commission should not occur until at least 2022, after the current phasing is complete.

V. Adverse Effect on Retirement of Duplicative Systems

One of the benefits of the CAT is to facilitate the retirement of Participants' existing rules and systems rendered duplicative by the CAT, such as, for example, the Order Audit Trail System ("OATS"). The Proposed Amendments would delay the planned retirement of such duplicative rules and systems. As noted above, the Participants believe that the Commission underestimates the time that would be necessary to build the SAWs required under the Proposed Amendments and for the Participants to customize and access their SAWs. To the extent that the Participants and SEC cannot make use of the CAT until the Proposed Amendments are adopted and fully implemented, the Participants believe that the retirement of current duplicative regulatory rules and systems may be delayed, thereby causing the industry to incur additional costs and comply with duplicative reporting requirements for a longer period.

VI. Enhanced Security Risks

The Participants also are concerned that the Proposed Amendments would add new security risks to the CAT. Pursuant to proposed Section 6.13(a)(i)(A), the CISP must establish policies and procedures that would require Participants to use their SAWs as the only means of accessing and analyzing customer and account data.[23] Further, pursuant to proposed Section 6.13(a)(i)(B), the CISP must establish policies and procedures that would require the Participants

---

22 *Id.* at 65995-96.
23 *Id.* at 65998.

to use their SAWs when accessing and analyzing CAT Data through the user-defined direct query and bulk extract tools, unless an exception is granted pursuant to proposed Section 6.13(d).[24] Thus, any Participant's analysis that involves both CAT Data and its own non-CAT Data required for its regulatory programs, which, as previously discussed, can include PII, would need to occur in the SAW. Since the SAW environments will be part of the CAT System, the CAT System would likely contain not just CAT Data, but non-CAT Data as well, including PII. Indeed, the types of PII would likely extend beyond the types of PII originally included in the CAT prior to efforts to limit the inclusion of PII in the CAT. The introduction of non-CAT Data, including PII, into the CAT will significantly enhance the security risk posed by the CAT, which is the very concern that the Commission, Participants and industry have taken steps to avoid.

VII. Impact on the Financial Accountability Milestones

The Participants believe that the Proposed Amendments would have a significant adverse effect on the financial viability of the CAT. The SEC has required the Participants to satisfy certain Financial Accountability Milestones in order to recover from Industry Members the full amount of CAT costs allocated to Industry Members and incurred in four distinct periods from June 22, 2020 through December 30, 2022. The Proposed Amendments do not appear to take the Financial Accountability Milestones into consideration and the Participants believe that the Proposed Amendments would make it impractical, or even impossible, to satisfy the Financial Accountability Milestones for Periods 3 and 4. As discussed in detail above, the Participants do not believe that new SAW-related and other requirements set forth in the Proposed Amendments could be completed in the required timeframes. Furthermore, the Participants believe that any attempt to comply with the new requirements in the Proposed Amendments would undermine and delay efforts to timely complete the existing requirements necessary for Periods 3 and 4. Therefore, the Proposed Amendments, if adopted, would unfairly cause the increased CAT costs for these two years to be borne entirely by the Participants.[25]

VIII. Inappropriate Oversight Role for Plan Processor

The Proposed Amendments would inappropriately place oversight responsibility for the Participants' usage of CAT Data to meet their statutory obligations as self-regulatory organizations on the CISO and CCO. In particular, proposed Section 6.13(c)(i) of the Plan would require the Plan Processor to monitor each Participant's SAW in accordance with the detailed design specifications developed pursuant to proposed Section 6.13(b)(i) for compliance with the CISP and to notify a Participant of any identified non-compliance with the CISP or the detailed design specifications.[26] Executing this responsibility would require the CISO and CCO to have oversight and control over the tools and data each Participant proposes to bring into the SAW.

The Plan Processor should not have responsibility for such oversight and control over the Participants' regulatory functions; the Commission retains such oversight authority pursuant to

---

[24] *Id.*

[25] While the Participants could request an exemption to extend the timeline for satisfying the Financial Accountability Milestones for Periods 3 and 4, any such exemption would be subject to Commission approval.

[26] Proposing Release at 66003.

the Exchange Act. By placing these oversight and control responsibilities on the Plan Processor, the Proposed Amendments effectively would inhibit the Participants' ability to satisfy their obligations under the Exchange Act to conduct regulatory surveillance. Such an arrangement also would contravene one of the fundamental purposes of the CAT, which is to "substantially enhance the ability of the [Participants] and the Commission to oversee today's securities markets and fulfill their responsibilities under the federal securities laws."[27] As such, the Participants believe that placing such oversight and control responsibilities on the Plan Processor would be inappropriate and could have a negative impact on the ability of the SROs to protect the integrity of the US securities markets through the use of innovative and dynamic surveillance. Moreover, giving the Plan Processor oversight and control over the Participants' manner of satisfying their self-regulatory responsibilities would significantly impede the Participants' ability to manage their key vendor.

IX. Security Working Group

Among other requirements, proposed Section 4.12(c) would permit the CISO and the Operating Committee to invite external parties to attend specific meetings, including the Security Working Group meetings.[28] These external parties could include, among others, external consultants with expertise in organizational-level or system-specific security and *industry representatives*.[29] The Commission believes these provisions would enable the Security Working Group to obtain a broad spectrum of views and to present such views to the CISO and the Operating Committee on key security issues.[30]

The Participants believe the current structure and operation of the Security Working Group is appropriate and has worked well to protect the security and confidentiality of CAT Data. The Security Working Group currently consists of the CISOs of the Participants, and other senior security personnel and subject matter experts of the Participants, all of whom provide their input related to the security of the CAT.[31] These members of the Security Working Group advise on security-related issues and serve as an additional resource to the CISO. For example, the Security Working Group reviews and makes recommendations to the Operating Committee

---

[27] *See* Securities Exchange Act Release No. 79318 (Nov. 15, 2016), 81 Fed. Reg. 84696, 84698 (Nov. 23, 2016) ("CAT NMS Plan Approval Order").

[28] *Id.* at 65994. Additionally, request for comment five asks:

> Should any other parties be included as required members of the Security Working Group? If so, please identify these parties and explain why it would be appropriate to include them. For example, should representatives from the Advisory Committee established by Section 4.13 of the CAT NMS Plan be added as required members to the Security Working Group? Should any limitations be placed on the kinds of parties the CISO and the Operating Committee may invite? For example, should the CISO and the Operating Committee be limited to inviting personnel employed by the Participants, because such personnel would already be subject to the confidentiality obligations set forth in Section 9.6 of the CAT NMS Plan for Representatives? If not, should external parties invited by the CISO and the Operating Committee be explicitly required by proposed Section 4.12(c) to sign a non-disclosure agreement or to comply with any other kind of security protocol in order to prevent the disclosure of confidential information regarding the security of the CAT System. Proposing Release at 65995.

[29] *Id.*

[30] The Commission believes the CISO and the Operating Committee should consider requiring non-member invitees to sign a non-disclosure agreement or to abide by some other protocol designed to prevent the release of confidential information regarding the security of the CAT System. *Id.* at 65993.

[31] SEC staff observers also are invited to attend Security Working Group meetings.

regarding the CAT System Security Plan, security policies and procedures, penetration testing and security audits, among other security related topics. The Participants have met with industry representatives on an ad hoc basis to discuss security matters, which has allowed the Participants to obtain the industry's views on security issues when necessary and appropriate. For example, the Participants engaged the industry to solicit their input on the development of the strategy for CAT Customer ID. The Participants believe that this flexibility and the current structure and operation of the Security Working Group functions extremely well without introducing unnecessary security risk to the CAT by expanding the Security Working Group beyond representatives of regulated entities.[32]

The Proposing Release asks whether other parties should be included as required members of the Security Working Group. The Participants believe that permitting industry representatives or other public participants to become required members of the Security Working Group, and therefore become privy to confidential security measures related to the CAT System, would raise significant security risks. The topics discussed during the Security Working Group meetings are highly confidential and sensitive in nature (*e.g.*, specific security plans, and surveillance models). The fundamental risks associated with making this type of information available to non-regulators simply cannot be mitigated through the use of a non-disclosure agreement or similar measure. Any leakage of such sensitive information would be detrimental to the investing public as well as to the successful development, implementation and maintenance of a fully functional and secure CAT System.

[32] Additionally, the Participants have hosted various industry events regarding the security of the CAT that were open to the industry and the public, and will look for opportunities to host similar events in the future. The Participants believe these industry and public events are the appropriate forum for external parties to provide their input and raise any questions about CAT security.

* * *

Thank you for your attention to this matter. Please contact me at [redacted] if you have any questions or comments.

Respectfully submitted,

Michael Simon
CAT NMS Plan Operating Committee Chair

cc: The Hon. Jay Clayton, Chairman
The Hon. Caroline A. Crenshaw, Commissioner
The Hon. Allison Herren Lee, Commissioner
The Hon. Hester M. Peirce, Commissioner
The Hon. Elad L. Roisman, Commissioner
Mr. Brett Redfearn, Director, Division of Trading and Markets
Mr. David S. Shillman, Associate Director, Division of Trading and Markets
Mr. David Hsu, Assistant Director, Division of Trading and Markets
Mr. Mark Donohue, Senior Policy Advisor, Division of Trading and Markets
Ms. Manisha Kimmel, Senior Policy Advisor, Regulatory Reporting to Chairman Clayton
CAT NMS Plan Participants