FINRA CAT™

Shelly Bohlin
President & Chief Operating Officer
FINRA CAT, LLC

December 2, 2020

Ms. Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-0609

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:

This letter is submitted on behalf of FINRA CAT, LLC ("FINRA CAT" or the "Plan Processor")[1] with respect to the Securities and Exchange Commission's ("Commission" or "SEC") proposed amendments to the National Market System Plan governing the Consolidated Audit Trail ("CAT NMS Plan" or the "Plan") to enhance the security of CAT (the "Proposed Amendments").[2] FINRA CAT appreciates the opportunity to comment on the Proposed Amendments.

FINRA CAT shares the Plan Participants' and the Commission's commitment to security and supports the overall objectives of the Proposed Amendments, including augmenting the security of CAT and limiting the amount of sensitive data required to be reported to the CAT. However, as described in more detail below, FINRA CAT is concerned certain aspects of the Proposed Amendments, including expansion of the CAT security perimeter to encompass at least one secure analytical workspace (each, a "SAW")[3] for each Plan Participant, may not fully achieve the desired increased security and may in fact introduce significant unintended risks and other adverse consequences.

---

[1] FINRA CAT entered into an agreement on March 29, 2019, with Consolidated Audit Trail, LLC ("CAT LLC") to become the Plan Processor and perform the functions and duties of the Plan Processor contemplated by the CAT NMS Plan, including the management and operation of CAT. FINRA CAT is a Delaware limited liability company and a subsidiary of the Financial Industry Regulatory Authority, Inc. ("FINRA Parent"). FINRA CAT is only commenting as FINRA CAT and not on behalf of the FINRA Parent.

[2] *See* Securities Exchange Act Release No. 89632 (File No. S7-10-20) (August 21, 2020), 85 FR 65990 (October 16, 2020). All capitalized terms used but not defined herein shall have the meaning ascribed to them in the Plan.

[3] *See supra note 2*, at 85 FR 65995, which defines a SAW as an "analytical 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 the [proposed] section 6.13."

9509 Key West Avenue
Rockville, MD
20850-3329

[redacted]

Specifically, FINRA CAT is concerned that the implementation of the Proposed Amendments would:

- significantly increase the quantity and types of sensitive data, including Sensitive Regulator Data (as defined below), within the CAT security perimeter by requiring all self-regulatory organizations ("SROs") performing automated surveillance using CAT Data to do so within CAT, thereby materially increasing the risk profile of both CAT and the Plan Processor;
- potentially constrain the choice of automated surveillance tools that can be used by each Plan Participant and the SEC (each, a "Regulator" and collectively "Regulators"),[4] as the Plan Processor would need and expect to have full transparency of each Regulator's surveillance systems and software and final control and authority to determine whether such systems, software, and data are consistent with the Plan Processor's and CAT LLC's risk tolerances;
- create an extensive and complex infrastructure and organizational interdependencies that will require significant resources and incur costs considerably higher than those estimated in the Proposed Amendments; and
- jeopardize implementation timeframes for CAT, which is currently in the build phase.

Importantly, FINRA CAT believes that other enhancements to the current SAW approach can achieve security benefits similar to those sought by the Proposed Amendments without these added material risks, complexity, and costs. FINRA CAT includes a description of its proposed approach below.

Finally, FINRA CAT welcomes the opportunity to share its views on several specific questions posed by the SEC in the Proposed Amendments, as identified in Appendix I attached hereto.

I. Adverse Implications of the Proposed Amendments

The CAT currently under development has a clear purpose – as a central data repository for the U.S. securities markets – and is the product of years of discussions, incremental revisions, and exhaustive planning by the SEC, the Plan Participants, Industry Members, and the Plan Processor. The implementation of the Proposed Amendments would represent a substantial redesign and expansion of CAT from a central repository of

[4] FINRA CAT notes that the Proposed Amendments exclude the SEC's use of a SAW from the Plan Processor's oversight and control. As the SEC is not a party to the Plan, and therefore the Plan cannot impose obligations upon the SEC, any expectation by the SEC that the Processor would be responsible for provisioning a SAW environment for the SEC and monitoring the security of the SEC's use of the CAT Data through that environment or otherwise should be made explicit in the rule, including with respect to allocation of costs, the standards for such provisioning and monitoring, and actions to be taken in the event of any identified security issues.

data to a central hub for all automated regulatory surveillance of U.S. securities markets involving CAT Data.

In particular, the Proposed Amendments would require the Plan Processor to provide each Plan Participant separate and distinct SAWs[5] within the CAT security perimeter. The Plan Participants would be required to conduct all automated regulatory surveillance activities that use CAT Data within these SAWs. SEC Rule 613 and the CAT NMS Plan did not specify that regulatory surveillance activities would be conducted within CAT. Further, the negotiations that led to FINRA CAT becoming the Plan Processor did not contemplate that the responsibilities of the Plan Processor would include providing technology operating environments and full security services for effectively all automated surveillance employing CAT Data that may be performed by Regulators.

These fundamental changes to the requirements of the CAT System have several significant implications, which are detailed below.

A. *The Proposed Amendments Would Increase the Amount of Sensitive Data Within CAT and Materially Change the Risk Profile of CAT and the Plan Processor*

First, to effectively conduct all required regulatory surveillance activities mandated by the Proposed Amendments, the Plan Participants would need to bring sensitive non-CAT Data, including personally identifiable information ("PII"),[6] regulatory intelligence, and other confidential and proprietary information (collectively, "Sensitive Regulator Data"), required for their respective regulatory programs into their CAT-provided SAWs, contrary to the significant efforts of the Commission to limit the inclusion of such sensitive data in CAT. In addition to the risk associated with adding Sensitive Regulator Data to CAT, the proposed approach could also introduce non-CAT Data into CAT that would not be reported through a CAT Reporter interface and associated controls. Further, output from Plan Participants' surveillance activities that contains CAT Data would also be stored within CAT, introducing additional sensitive regulatory intelligence into CAT.

FINRA CAT has significant concerns relating to any introduction or retention of Sensitive Regulator Data in CAT given the concomitant increase to the overall risk profile of CAT. As the Proposed Amendments would require the Plan Processor to become the custodian of Sensitive Regulator Data, as well as Regulator intellectual property (*e.g.*, a Regulator's proprietary software and models), the aggregate value of the information stored within CAT would be substantially increased, making the potential impact of a cyber event

[5] While the Proposed Amendments only contemplate one SAW per Regulator, the Plan Processor expects that each Regulator will require multiple SAW environments to support various stages of their software development lifecycle.

[6] As used herein, PII refers to sensitive, personally identifiable information, as is commonly protected by various state privacy laws.

involving CAT, and thus the overall security risk of CAT, commensurately greater.[7] Further, there is the risk of compromise of all aspects of market surveillance if the CAT security perimeter, within which would sit all Regulator SAW accounts, is breached.

The security risk profile of CAT would also be increased by the complexity and interdependencies that the Proposed Amendments would introduce. As described below, if the Plan Processor were required to take on the responsibilities outlined in the Proposed Amendments, it also would require the ability to exercise control over the systems, software and information introduced into the SAW environments. Making the Regulator SAWs part of the CAT (*i.e.*, bringing them within the CAT security perimeter) and subject to the Plan Processor's security requirements creates a complex set of dependencies between the Plan Processor and each of the Regulators. Complexity exacerbates the challenge of maintaining security; hence, FINRA CAT is concerned that this increased complexity could actually result in a CAT that is less secure.

B. *The Proposed Amendments Would Potentially Constrain the Tools Used by Regulators to Conduct Surveillance by Requiring the Plan Processor to Exercise Full Control and Authority over Each SAW*

The Proposed Amendments would require FINRA CAT to provision at least five SAW environments for each Regulator (or corporate family of SROs, depending on what the SROs request) – Development, Test, Certification Test, Production, and Disaster Recovery environments – as well as the tools and processes to effectively manage these environments and allow the Regulators to develop, promote, and operate their regulatory software across these environments.

To effectively incorporate these SAW environments into the single Comprehensive Information Security Program ("CISP") contemplated by the Proposed Amendments,[8] the Plan Processor would need to have ultimate authority (as it does with the Central Repository) as to all systems and software permitted to operate in the SAWs, including any SAW environment(s) established for the SEC. This scope would include the authority to set conditions on activities conducted in the SAWs, including requiring changes to any Regulators' proprietary systems or software prior to their use in the SAW or prohibiting their use in the SAW entirely, if this activity would be inconsistent with FINRA CAT security policies, standards, or risk tolerances.

---

[7] *See* NIST SP 800-30, which describes risk as a function of likelihood and potential impact.

[8] *See supra note 2*, at 85 FR 65992, which defines CISP as "the organization-wide and system-specific controls and related policies and procedures required by NIST SP 800-53 that address information security for the information and information systems of the Plan Processor and the CAT System, including those provided or managed by an external organization, contractor, or source." The proposed definition further states that the CISP will also apply to SAWs, new environments within the CAT System to which CAT Data may be downloaded.

The Plan Processor would expect to develop and impose upon all Regulators[9] a common software development lifecycle ("SDLC") and related suite of governance processes and tools. Moreover, the tools and processes that would be imposed on the Plan Participants in their respective SAW environments are numerous, covering for example account creation, virtual private cloud management, networking, authentication systems, identity management, access management, open source software management, software build and deployment automation, infrastructure provisioning, Amazon Web Services ("AWS") service management (*e.g.,* policies, thresholds, limits), software security scanning, and vulnerability scanning. Several of these items would require the AWS account owner (*e.g.,* FINRA CAT as the Plan Processor and proposed owner of the SAWs) to configure and manage such activities as they cannot be delegated to the SAW users (*e.g.,* Regulators), thus requiring FINRA CAT to provide separate development support in addition to providing operational support.

Each Plan Participant has a unique and diverse set of software applications that would require specialized expertise on the part of the FINRA CAT Security team in order to effectively analyze, monitor, and control the security in each SAW environment to support SDLC phases. Therefore, FINRA CAT will need to embark on a concentrated program to identify and recruit staff with the appropriate level of specialized expertise, which would be time-consuming and challenging. The Plan Processor would be required to recruit, hire, and retain experts in the diverse, potentially divergent, and often proprietary systems and software of each of the Plan Participants, as well as of the SEC. Each Regulator would also need to fully disclose intellectual property related to each of these solutions, such as architecture, design documentation, and source code. As described below, undertaking this substantial additional work would significantly jeopardize CAT's current implementation schedule.

In light of these challenges, maintaining adequate expertise at the Plan Processor for the custom solutions of each Regulator may not be practical. Even if the Plan Processor were successful in assembling the broad security team necessary to manage the risks across the numerous SAWs, that staff would be tasked further with reviewing and authorizing changes in accordance with as-yet undefined service level agreements ("SLAs"). These practical challenges counsel against resting this authority and responsibility with the Plan Processor. Rather, Regulators, particularly those using their own custom software solutions, would be best positioned to secure their respective solutions, based on their expertise with the applicable technologies and the architecture and design of their customer solutions.

Further, beyond the challenges of staffing, intellectual property sharing, and service provision, there are technical limitations on the Plan Processor's ability to manage security

[9] Exempting the SEC (or any party) from the common, standardized SDLC and governance processes imposed on the Plan Participants would increase the security risks, complexity, and associated costs; if the Proposed Amendments are adopted as proposed, FINRA CAT strongly cautions against such an exemption.

risks to acceptable levels while still allowing Regulators to use their own software and data to meet their regulatory obligations. In effect, these limitations could constrain the tools used by Regulators to conduct automated surveillance in furtherance of their regulatory obligations. As noted above, the Proposed Amendments appear to require Regulators to provide their proprietary software to the Plan Processor for review and approval prior to introduction to the Regulator's SAW accounts. The Plan Processor would need to establish restrictions regarding permissible software and tools for use in the SAW environment by Regulators. Both the time to complete such reviews (which the Proposed Amendments significantly underestimate) and potential limitations that the Plan Processor determines must be imposed on the use of certain software and tools based on those reviews (*e.g.*, a prohibition on uploading PII or other Sensitive Regulator Data) likely would impair the effectiveness of the Regulators in performing core regulatory functions. FINRA CAT is also concerned that such limitations would place what some Regulators may believe to be unacceptable constraints on regulatory innovation and flexibility (*e.g.*, if the Plan Processor denies upload of an enhancement to a Regulator's SAW account, and as a result, the Regulator is unable to fulfill a regulatory obligation).

The Proposed Amendments would place the primary oversight and responsibility for each Plan Participant's use of CAT Data not only on the Plan Processor generally, but on the Plan Processor's Chief Compliance Officer ("CCO") and Chief Information Security Officer ("CISO") specifically, which would create significant conflicts for these individuals. Under the Plan, the CCO and CISO, although employees of the Plan Processor, are deemed officers of CAT LLC, and are required to report directly to the Plan Participants (in the form of the Operating Committee).[10] The Operating Committee must approve the Plan Processor's selection of the CCO and CISO, approve their salaries, and evaluate the annual performance of these officers.[11] The Plan further requires that CAT LLC require in a written agreement with the Plan Processor that the CCO and CISO owe fiduciary duties to CAT LLC, which duties shall control in the event they conflict with any duty of these officers to their employer, the Plan Processor.[12]

Despite the breadth of control over these two individuals that the CAT NMS Plan vests in the Plan Participants, the Proposed Amendments would turn this structure on its head by expecting the CCO and CISO to exercise significant decision-making authority over these same Plan Participants and their use of CAT Data, and further expecting these individuals to exercise this authority independently. In particular, the CCO and CISO would be required to make decisions on Plan Participants' conduct within the SAWs, decisions that will go to the very heart of their regulatory activities, including their ability to pursue regulatory innovation. While the Proposed Amendments provide an exception process enabling Regulators to access CAT from non-SAW environments, the granting of such exceptions is similarly left to the sole authority of the CCO and CISO, who would

[10] *See* CAT NMS Plan, Section 4.6(a).
[11] *See id.* at Sections 4.6(a), 6.2(a)(iv), and 6.2(b)(iv).
[12] *See id.* at Section 4.6(a).

require a similar level of transparency into a Regulator's systems, including intellectual property inherent to the "detailed design specifications for [the Regulators'] non-SAW environment," in order to judge whether the "risks associated with extracting CAT Data to the non-SAW environment" have been sufficiently mitigated.[13]

In the case of both SAW and non-SAW environments, the Proposed Amendments would effectively make the CCO and CISO – neither of whom are regulators or privy to the vast regulatory intelligence and expertise available to the Plan Participants – surveillance gatekeepers of the U.S. securities markets. This outcome could materially restrict the ability of Plan Participants to employ their expertise to surveil dynamically and proactively for conduct harmful to investors. We believe it is inappropriate to require the CCO and CISO of the Plan Processor to exercise such broad authority over how SROs can use the CAT Data, particularly given the potential conflicts such a requirement would create.

C. *The Proposed Amendments Do Not Account for the Complexity of Implementing and Maintaining the Proposed SAW Design and the Associated Costs*

The Proposed Amendments appear to present the implementation of the proposed SAW design as straightforward. After significant review, FINRA CAT believes that implementation of the proposed structure would be highly complex and costly. In preparing these comments, FINRA CAT reviewed the Proposed Amendments with its Engineering, Development and Tools, Networking, Operations, and HelpDesk teams, and then created bottom-up estimates based on preliminary assessments of implementation requirements and related considerations. For the reasons identified below, FINRA CAT has concluded that the Proposed Amendments' estimates of complexity, costs, and timing fall far short of the actual complexity, costs, and timing necessary to develop and operate the proposed CAT security structure.

i. FINRA CAT Would Become a Managed Infrastructure Service Provider

Today, FINRA CAT acts as a data services provider. The Proposed Amendments, however, would require FINRA CAT to morph into a managed infrastructure services provider in order to implement the proposed SAW structure, a substantially different business with substantially different requirements in terms of staffing, processes, technology, and contracting.

The new Plan Processor activities necessitated by the Proposed Amendments to remain consistent with NIST SP 800-53[14] would be extensive, requiring FINRA CAT to perform the following for each Regulator's SAWs: (a) support architectural changes to

[13] *See supra note 2*, at 85 FR 66005.
[14] As required by CAT NMS Plan, Section 4.2

their networks and move significant amounts of Sensitive Regulator Data into Plan Processor-owned accounts; (b) support the migration of each Plan Participant's regulatory application portfolios into the Plan Processor architecture; (c) support migration of the Plan Participants and the SEC from their current SDLC to the standardized Plan Processor platform and workflow, which would include amending required SDLC security controls under the CISP; and (d) negotiate and establish a uniform set of policies, procedures, and standards for software selection, integration, security configuration, software libraries, and other functions that are both consistent with the standards set forth by the Plan and acceptable to all Plan Participants and the SEC. The Plan Participants and the SEC, in turn, would be required to make changes to their regulatory systems to align with the imposed standards, establish security monitoring, tooling, and threat-hunting capabilities based on unique characteristics across technologies unique to each Plan Participant and the SEC, and update records management and data protection policies, procedures, and practices.

The Plan Processor would also need to support each Plan Participant's and the SEC's technical teams for infrastructure, development, and operations in their multiple SAW accounts. Additionally, each Plan Participant and the SEC likely have varying levels of software complexity and cloud-based development practices that FINRA CAT would need to access and understand in developing each SAW account. And as noted above, FINRA CAT would need to provide new development and operations support. All of this would increase the complexity and effort across all aspects of the program, including security, operations, development services, networking, disaster recovery, and Regulation SCI compliance. Additionally, FINRA CAT would need to establish and maintain new levels of client relationship management for the Plan Participants and the SEC.

These changes and the others required by the Proposed Amendments would require reconsidering the existing contractual arrangements in place among FINRA CAT (as the Plan Processor), CAT LLC, and the Plan Participants, particularly in terms of risk allocation. Terms related to data security and service level obligations, disclaimers and warranties, and indemnities and insurance would require review, and the availability, cost, and level of insurance coverage would also need to be reevaluated in light of the greatly increased amount of sensitive data that may be included within CAT. In addition, FINRA CAT would also need to re-negotiate service contracts with existing critical vendors, or potentially establish and negotiate new vendor arrangements, in order to address the increased scope and expanded risk profile reflective of its new role as a managed services provider. For example, it is unclear whether the proposed CISP is intended to impose additional requirements on external vendors which, if so, could impact existing contracts or future negotiations. Finally, a number of other security, development, and operation tool licenses and subscriptions would require review and potential renegotiation as well.

ii. The Proposed Amendments Create an Extensive and Complex Infrastructure that Will Require Significant Resources and Incur Costs Considerably Higher than Estimated

FINRA CAT believes that the proposal significantly underestimates the costs of its requirements. For example, in estimating the labor costs to implement the program required by the Proposed Amendments, the SEC's estimates do not reflect the full measure of necessary work. For SAW-related work, FINRA CAT estimates the labor portion to deliver the required services to be more than, possibly substantially more than, 60 times greater than the SEC's estimate of $441,600.[15] FINRA CAT further estimates the labor portion to operate the numerous SAWs to be more than, again possibly substantially more than, 40 times greater than the SEC's estimate of $860,200 annually.

With regard to the non-SAW scope (*e.g.*, security architecture governance, compliance, CISP, OTQT logging, programmatic access to customer, and account information), FINRA CAT estimates the labor portion to deliver the required services to be more than 10 times greater than the SEC's estimate of $812,300. FINRA CAT further estimates the labor portion to operate the non-SAW scope to be more than 5 times greater than the SEC's estimate of $869,200 annually.

It is not possible for FINRA CAT to estimate non-labor costs, which will be substantial, as they are dependent upon the Plan Participants' and SEC's data (types and volume) and the software each Regulator brings into the SAW, which are at present unknown to FINRA CAT. However, FINRA CAT would note that these costs do not appear to be fully accounted for in the SEC's economic analysis. FINRA CAT believes these costs to include, at a minimum, the following items: (i) software and tool licenses and subscriptions; (ii) Plan Processor-provided networking infrastructure, licenses, and subscriptions (*e.g.*, firewalls, gateways, routers, domain name system, certificates); (iii) AWS service fees for provisioning and maintaining the SAWs and related infrastructure (*e.g.*, identify and access management, Direct Connect, compute and storage for FINRA CAT-provided tools, automation, and reporting); (iv) insurance (*e.g.*, Cyber and Director & Officer); and (v) third-party audits and security services (*e.g.*, IV&V, PenTest, external Reg SCI audits).

Given the scope and nature of the Proposed Amendments, the foregoing estimated costs are strictly the "floor" estimate (*i.e.*, "no less than") and are likely to be substantially higher, depending on the final version of the Proposed Amendments and details from the Regulators on their respective data and software portfolios.

D. *The Proposed Amendments Would Put the Current Implementation Timelines at Risk*

[15] FINRA CAT is providing these cost estimates solely in response to the SEC's request for comment on the Proposed Amendments. Cost estimates do not represent and should not be construed as a proposal, offer, bid or commitment from FINRA CAT. FINRA CAT is not making and expressly disclaims any representation about these cost estimates, including, without limitation, any representation that these cost estimates are complete, accurate or final. Cost estimates have a high degree of uncertainty and will be substantially impacted by the final form of the Proposed Amendments and subsequent interpretations and requirements.

FINRA CAT believes that the Proposed Amendments' required changes cannot be implemented in parallel with the remaining build of CAT, given their breadth and complexity. The timeline of 120 days set forth in the Proposed Amendments does not reflect the enormity of the required changes. Thus, adoption of the Proposed Amendments in their current form would substantially delay the current CAT implementation schedule.

FINRA CAT estimates that it will take at least several months of concentrated effort to scope and define the standard practices, processes, and controls with the Regulators prior to implementation. FINRA CAT further estimates that hiring enough qualified staff to address the SAW and non-SAW requirements in the Proposed Amendments will take at least 12 months. Once adequate staff is hired and trained, FINRA CAT estimates the duration of implementation of the Proposed Amendments will extend 18 months at the very least. Time would also be needed to negotiate new or amended vendor agreements, as well as amendments to the existing agreement between FINRA CAT and CAT LLC. Such negotiations are likely to be very complex and time-consuming as the parties seek to address the myriad issues raised by the proposed redesign and expansion of the CAT System.

The demands on FINRA CAT staff at all levels of seniority to implement the proposals would hamper the ongoing and substantial efforts to meet the current Master Plan and Financial and Accountability Milestones ("F&AM") and place these milestones at risk. As such, unless the F&AM deadlines are substantially revised, implementation of the Proposed Amendments, should they be adopted, could not be scheduled to begin earlier than 2022, after the core set of F&AM are completed (and assuming best case scenario and availability of resources from all relevant parties).

II. Alternative SAW Proposal for Consideration

FINRA CAT believes that the security objectives set forth in the Proposed Amendments can be substantially achieved, with less risk, much lower cost, and a faster timeframe, by enhancing and codifying in the Plan the controls and monitoring regimes applicable under the current SAW model (where each Regulator is responsible for creating its own SAW account) that FINRA CAT has already implemented in 2020.

In place of the Proposed Amendments, FINRA CAT requests that the Plan be amended to provide increased monitoring authority to the Plan Processor over the Regulator-owned SAW environments. The hallmarks of this monitoring authority would be enhanced controls, policies, and procedures applicable to the Regulator-owned and operated SAWs, making the SAW owners accountable for the security of their SAW accounts while still maintaining the Regulators' requisite ability to run their regulatory programs.

This enhanced SAW model would impose four oversight responsibilities with the Plan Processor. First, there could be additional monitoring by the Plan Processor of

infrastructure and software in the Regulator-owned SAW accounts, with more extensive security standards and security guidelines. Second, the Plan Processor could implement vulnerability scanning of infrastructure and deployed software in the Regulator-owned SAWs. Third, the Plan Processor could require periodic penetration testing and code reviews of the Regulator-owned SAWs by independent third parties, with reporting back to the Plan Processor of discovered vulnerabilities and risks by those independent third parties and a commitment to address the risks in accordance with the Plan Processor's risk management policy. Finally, the Plan Processor could require intrusion detection monitoring of the Regulator-owned SAWs.

Together, these four elements of the enhanced security monitoring program would enable the Plan Processor to ensure an appropriate level of monitoring of the Regulator-owned SAWs, avoid the introduction into the CAT perimeter of Sensitive Regulator Data, including PII, that would otherwise occur if Regulators were forced to run their regulatory programs in a Plan Processor-owned SAW, avoid creating unworkable conflicts for the CISO and CCO, and empower innovation by the Regulators while protecting their proprietary systems and data. The Plan Processor welcomes the opportunity to work with the Plan Participants and the SEC to refine this alternative approach.

III. Conclusion

FINRA CAT appreciates the opportunity to comment on the Proposed Amendments. As discussed above, FINRA CAT agrees with the underlying objectives of the Proposed Amendments relating to enhanced data security, but respectfully believes that FINRA CAT's alternative proposal of substantially enhancing the monitoring program under the existing SAW structure could achieve these objectives without the very substantial risks associated with the structure envisaged in the Proposed Amendments. Further, FINRA CAT's alternative proposal could be deployed at a fraction of the cost and time necessitated by the new proposed SAW model.

Should you have any questions or wish to further discuss FINRA CAT's perspective relating to the Proposed Amendments, please contact Shelly Bohlin, FINRA CAT, at [redacted]).

Sincerely,

/s/ Shelly Bohlin
President & Chief Operating Officer
FINRA CAT, LLC

Appendix I: Responses to Select Questions in the Proposed Amendment

Dedicated Hosts:

Question 164: Should the Commission require that the CAT System use dedicated cloud hosts that are physically isolated from a hardware perspective?

Question 165: Should all development/production be done on a separate dedicated host or should only Customer Identifying Systems development and/or production be done in a dedicated host?

FINRA CAT Response: No. The use of dedicated cloud hosts does not offer any improvement in security over the standard cloud model. In fact, dedicated hosts are contrary to cloud-based designs for resiliency, fault tolerance, scalability, and disaster recovery. Instead, it is possible to employ the same security best practices on shared/multi-tenant servers in AWS, including using the following: micro segmentation to define segments and controls at a granular level; least privilege access to grant users only the permissions required for their jobs; monitoring, alerting and logging of all actions and changes to the environment; application of security at all layers and resources (computer, storage, network, databases); automation of security best practices through development-security-operations/infrastructure as code templates; encryption and tokenization of data at rest and in transit wherever appropriate; minimizing human access to data; and the isolation of development/production accounts/Customer identifying systems using all of the above controls.

Additionally, a requirement to use dedicated hosts does not take into account the benefits obtained through the use of secure cloud services such as serverless services (Lambda, Athena, etc.) and event driven message-based processing systems (SQS, SNS, etc.), which are currently used within the CAT. Nor does such a requirement account for the benefits obtained through the use of secure managed storage systems like S3, Glacier, and Deep Archive. In addition, using dedicated hosts limits compute and storage options which makes the architecture more brittle, increases risks of not processing new peak market volumes, and increases costs. Further, requiring dedicated hosts would require the Plan Processor to provision for forecasted peak rather than scale up and down to meet fluctuating demand, which will significantly increase cost. Finally, using dedicated cloud hosts would always require a full disaster recovery environment for compute and storage to be provisioned and maintained, rather than launching the compute when needed in the case of a multi-region disaster recovery event, which decreases flexibility and substantially increases costs.

Connectivity

Question 158: Should the current secure connectivity practices in place for the Participants to connect to the CAT infrastructure *using only private lines* be codified in the CAT NMS Plan?

Question 159: Is it appropriate to clarify when private line and Virtual Private Network connections should be used?

FINRA CAT Response: No. The CAT NMS Plan specifies various secure connectivity methods. Narrowly defining acceptable methods of secure connectivity, such as VPNs, may preclude the ability to take advantage of innovations in secure connectivity in the future. Currently, Industry Members have three secure options to connect to CAT: Managed Network Service Provider via BT Radianz and Lumen; AWS PrivateLink; or the Secure Reporting Gateway, which establishes a secure TLS connection over the public Internet to a zero-trust gateway using two-factor authentication. It should be noted that the AWS PrivateLink and Secure Reporting Gateway technologies were not available at the time the CAT NMS Plan was approved.

Restrictions to U.S. Citizens

Question 157: Should additional restrictions be required to enhance security, such as imposing U.S. citizenship requirements on all administrators or other staff with access to the CAT System and/or the Central Repository? Please explain the impact on the implementation and security of the CAT including costs and benefits. Should the Commission only apply these additional access restrictions to access the Customer Identifying Systems and associated data?

FINRA CAT Response: No. Plan Processor employees and contractors with access to CAT must submit to FBI fingerprint-based background checks, complete extensive security awareness training, and execute a safeguard of information affidavit. Regardless of their country of citizenship, all administrators are US domiciled and are closely monitored under an insider risk program and in accordance with an approved Insider Risk Policy. Other continuous monitoring, including monitoring designed to detect anomalous activity that could indicate misuse or abuse of access, is in place and agnostic to the citizenship status of the individual being monitored. Restricting staff to only U.S. citizens would require FINRA CAT and its contractors with access to CAT Data to replace any staff with Green Card, visa or dual citizenship and would put the Master Plan and Financial & Accountability Milestones in jeopardy. Reconfiguring staff would put the current CAT implementation timelines, as well as the Proposed Amendments' timelines, at risk due to the time and effort it would take to recruit and on-board new employees. In addition, it

would likely cause a reassessment of fees, especially due to the likely substantial increase in the costs of recruiting and retaining labor due to a smaller talent pool.