Elizabeth K. King

Chief Regulatory Officer, ICE.
General Counsel & Corporate Secretary, NYSE

11 Wall Street
New York, NY 10005
[redacted]

December 2, 2020

Via Email

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

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

Dear Ms. Countryman:

NYSE Group, Inc. ("NYSE") respectfully submits this comment letter on behalf of the New York Stock Exchange LLC, NYSE American LLC, NYSE Arca, Inc., NYSE Chicago, Inc., and NYSE National, Inc. (together, the "NYSE Exchanges") in response to the Proposal,[1] which sets forth proposed amendments to the National Market System Plan governing the Consolidated Audit Trail ("CAT NMS Plan").[2]

The NYSE supports strong security for the Consolidated Audit Trail ("CAT") and agrees with the Securities and Exchange Commission (the "Commission") that the CAT NMS Plan must "protect the security and confidentiality of CAT Data."[3] The NYSE does not, however, believe that this problematic Proposal would further that goal.

The most significant problem presented by the Proposal is that it would prevent the CAT from meeting its core purpose: making a consolidated audit trail of U.S. securities market data available to all regulators charged with oversight responsibilities to help them "oversee today's securities

---

1 See Securities Exchange Act Release No. 89632 (August 21, 2020), 85 FR 65990 (October 16, 2020) (File No. S7-10-20). All capitalized terms not otherwise defined are used as defined in the Proposal.

2 See Securities Exchange Act Release No. 79318 (November 15, 2016), 81 FR 84696, (November 23, 2016) (Joint Industry Plan: Order Approving the National Market System Plan Governing the Consolidated Audit Trail) ("CAT NMS Plan Approval Order"). The CAT NMS Plan is Exhibit A to the CAT NMS Plan Approval Order. See id., at 84943–85034. See also Limited Liability Company Agreement of Consolidated Audit Trail, LLC, a Delaware Limited Liability Company (August 29, 2019), at https://www.catnmsplan.com/sites/default/files/2020-07/LLC-Agreement-of-Consolidated-Audit-Trail-LLC-as-of-7.24.20.pdf.

3 Proposal, at 65991. "CAT Data" is defined to mean "data derived from Participant Data, Industry Member Data, SIP Data, and such other data as the Operating Committee may designate as 'CAT Data' from time to time." CAT NMS Plan, at Section 1.1. See also Proposal, at note 4.

markets and fulfill their responsibilities under the federal securities laws."[4] As set forth in Rule 613 of Regulation National Market System ("Rule 613"), the CAT requirements explicitly mandate that all self-regulatory organization ("SRO") participants in the CAT NMS Plan (the "Participants") have unlimited access to CAT Data.[5] Rather than further this goal, the Proposal would work against it, by making it substantially and, for some SROs, prohibitively difficult to access or use CAT Data. CAT Data that was intended to be used for regulatory purposes would become effectively inaccessible to many SROs, curtailing the quality of regulatory oversight of the U.S. securities markets, rather than strengthening it as Rule 613 and the CAT NMS Plan contemplate.[6]

At the same time, contrary to its stated goal of protecting the security and confidentiality of CAT Data, the Proposal would make the CAT structure, and accessing CAT Data, much riskier. By requiring SROs to conduct nearly all surveillances that use CAT Data within CAT environments, the proposed amendments would make it possible for a single data breach to affect every SRO at once—making CAT Data and SRO data *less* secure than they are today. At the same time, it would force SROs to upload large proprietary datasets into CAT environments, a step that would make the CAT an even more attractive target for bad actors. Together, these effects would eliminate the ability of many, if not most, SROs to access CAT Data as a practical matter.

The proposed amendments also exceed the Commission's authority in important ways, including by improperly delegating SRO responsibilities to the Plan Processor and its employees in ways that conflict with Section 11A of the Securities Exchange Act of 1934, as amended (the "Exchange Act"),[7] and Rule 608 of Regulation National Market System ("Rule 608").[8]

Like all government agencies, the Commission must comply with the Administrative Procedure Act ("APA")[9] in pursuing its stated ends. The APA's requirement of reasoned decision making dictates that the Commission must address important aspects of the problem the Proposal seeks to tackle, consider the collateral consequences of its action, reasonably assess the Proposal's costs and benefits, and account for reliance interests stemming from prior agency actions.[10] For the reasons set forth below, the Proposal fails to satisfy those bedrock legal requirements, and should therefore be withdrawn.

In this letter, the NYSE describes many problems with the Proposal that it currently observes. For

---

4 Securities Exchange Act Release No. 67457 (July 18, 2012), 77 FR 45722 (August 1, 2012) (order adopting Rule 613) ("Rule 613 Adoption Release"), at 45726.

5 17 CFR 242.613(e)(2). The national securities exchanges and the Financial Industry Regulatory Authority ("FINRA") are all self-regulatory organizations and Participants in the CAT NMS Plan. See Proposal, at note 1.

6 See, e.g., Rule 613 Adoption Release, supra note 4, at 45730 (enumerating ways in which the CAT, as originally contemplated, was expected to improve the quality of regulatory oversight of the securities markets in the United States, among other things).

7 15 USC 78k-1.

8 17 CFR 242.608.

9 See 5 USC 706(2).

10 See, e.g., *Motor Veh. Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983).

ease of review, the Executive Summary the same numbering in its primary headings as the longer discussion that follows the Table of Contents.

Executive Summary

I. The Proposal Would Undermine the CAT's Core Purposes

A. The Proposed Amendments Would Make CAT and SRO Data Less Secure and Increase the Risk of a Major Data Breach.

Although purportedly designed to increase the security and confidentiality of CAT Data,[11] approval of the Proposal would create significant new security risks for CAT Data, as well as for non-CAT data and regulatory systems.[12] These risks would make it difficult or impossible for the SROs to use CAT Data in support of their regulatory functions, contrary to the CAT's original goal of providing access to a single, cross-market consolidated audit trail for regulatory use.[13] Nonetheless, even as it proposes the requirements that create these new risks, the Proposal does not adequately consider them.

1. The Proposal Would Create a Single, More Valuable Target

A main driver of the Proposal's new risks is the proposed requirement that secure analytical workspaces ("SAWs") created by the Plan Processor be the primary means for SROs to access and analyze CAT Data, as well as the *only* means of accessing and analyzing CAT-related personally identifiable information ("PII").[14] Though not acknowledged by the Commission in its Proposal, these limitations would require the SROs to migrate their proprietary, non-CAT regulatory systems and data into their SAW in order to use CAT Data to perform regulatory functions.[15] SRO regulatory systems and data are currently stored and analyzed in separate, decentralized systems managed by each SRO and subject to Regulation Systems Compliance and Integrity ("Regulation SCI")[16] compliant, but diverse security controls. Under the Proposal, all of those systems and data would be housed under one roof and governed by a single, identical set of security protocols. That transition would greatly expand the scope of data stored within the CAT, making the CAT a more valuable target for bad actors.

Significantly, under the proposed SAW structure, a breach in one SAW could lead to a breach in the entire CAT, significantly increasing the scale of the risk created. If there were a flaw in the SAW or a vulnerability in the infrastructure of the entity hosting the cloud environment, it could affect *all*

---

11 Proposal, at 65991.

12 Part I.A.3-6 below includes a discussion of the risks relating to the proposed identical confidentiality policies regarding the usage of CAT Data ("Proposed Confidentiality Policies"); codification of specific standards and practices into the CAT NMS Plan; new security working group ("SWG"); and requirements relating to the Programmatic CCID Subsystem Access.

13 See, e.g. CAT NMS Plan Approval Order, supra note 2, at 84753.

14 See Proposal, at 65992 and 66099 (proposed Section 6.13(a)(i)).

15 See CAT NMS Plan, Sections 6.7(a)(iv) and 6.10(a).

16 17 CFR 242.1000 et seq.

SROs simultaneously. The entire CAT could be compromised, and the regulation of the securities markets affected—a disastrous outcome that is much less likely under the current decentralized framework.

2. The Proposal Would Force SRO Reliance on, and Disclosure to, the Plan Processor

The Proposal requires the SROs to grant the Plan Processor, which currently is a Financial Industry Regulatory Authority, Inc. ("FINRA") subsidiary, broad access and control over their regulatory environments. Specifically, the Proposal assigns the Plan Processor, the Chief Information Security Officer ("CISO") and Chief Compliance Officer ("CCO") responsibility for creating the SAW environments, controlling access to those environments, and monitoring the SROs' activities in the SAWs, among other critically important tasks.[17]

Such access would create new security and operational risks. The Plan Processor would have access to all proprietary data that the SROs introduce to their SAWs, including surveillance results. The Proposal also requires the Plan Processor to share information regarding each SRO's regulatory program with the Operating Committee, potentially revealing such proprietary data to competitors.[18] These proposed requirements would create additional impediments to the SROs' ability to use CAT Data in their regulatory programs, potentially leading SROs or the Commission to conclude that exchanges' own regulatory programs are insufficient and requiring instead that an SRO pay a third party for the regulatory activities it is required to conduct.

3. Security Requirements Should Apply to Commission and its Staff

Although the Proposal would impose unprecedented new restrictions on SROs, it would not apply these restrictions to Commission staff who access the CAT. Instead, the Proposal states that the Commission will ensure that it has policies and procedures that result in comparable security protections.[19] Notably absent from this vague undertaking is any statement that the Commission staff will be required to use a structure similar to the SAWs or limited in their ability to download CAT data into local systems. It is unclear why such different standards may apply to this subset of CAT Data users—which the NYSE believes will make up the majority of CAT users—and likewise unclear how this inconsistent treatment would serve the goals the Proposal is purportedly designed to achieve.

If Commission users are governed by less rigorous standards than the SROs, any proposed changes would provide no meaningful security benefits. Security frameworks are only as strong as their weakest link, such that a lapse by even a single, less-vigilant regulatory user would render the security efforts of other regulatory users almost meaningless. The Commission should therefore be required to meet the same security- and data-access standards as the SROs or explain which security and access requirements of the CAT NMS Plan with which its staff will not be required to comply, and why not.

---

[17] See Proposal, at 66096-66106 (proposed amendments to Sections 4.12, 6.1, 6.2, 6.5, 6.6, 6.10, and 6.13, and Appendix D, Sections 4.1.1, 4.1.4-4.1.6, 8.1.1, 8.2, 9.1, 9.3, 9.4 and 10.1).

[18] See id., at 66097 (proposed Section 4.2), and 66099 (proposed Section 6.13(d)). The Operating Committee includes representatives of each SRO.

[19] Id., at 66053.

B. The Proposal Would Fundamentally Alter the Cost/Benefit Justification for Developing the CAT.

The Commission determined years ago that the existing CAT security framework is adequate and can be adapted to new needs and circumstances in order to achieve the CAT's goals.[20] If adopted, the Proposal would significantly amend the CAT's security framework without acknowledging these prior conclusions or demonstrating a need for change—in violation of the APA's requirement of reasoned decision making.[21]

From the start, the CAT was designed to be a tool to help the national securities exchanges and other regulators comply with their oversight mandates.[22] Rule 613, which called for the creation of the CAT, was clear: regulators must have access to the CAT and all data reported to it in order to perform their regulatory responsibilities, and that *access shall not be limited.*[23] Nonetheless, the Proposal would put serious limitations on the SROs' ability to access CAT Data—for example by giving the Plan Processor the ability to mandate the form and structure of how the SROs carry out regulatory programs using CAT Data, and by restricting the amount of CAT Data that SROs may extract from the CAT system. Collectively, these limitations could make it impossible as a practical matter for the SROs to use CAT Data for regulatory purposes.

Similarly, the Proposal would impose new costs not contemplated by Rule 613 or the CAT NMS Plan. As of October 15, 2020, the SROs' total unreimbursed costs for development of the CAT were in excess of $221 million.[24] That figure does not include the varied costs incurred by the SROs in reliance on current CAT NMS Plan requirements.[25]

Now the Commission is demanding more. The Proposal would require the SROs to incur substantial additional costs—in technology costs, personnel resources, opportunity costs, and potential liability—to use CAT Data to comply with their obligations. Specifically, the proposed amendments would require SROs to commit monetary, personnel, and technology resources to

---

20 See, e.g. CAT NMS Plan Approval Order, supra note 2, at 84753.

21 See *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 515-14 (2009).

22 The Commission explained the original purpose of the CAT in releases that accompanied the proposal and adoption of Rule 613. See Securities Exchange Act Release No. 62174, 77 FR 32556 (June 8, 2010) (proposing new Rule 613); and Rule 613 Adoption Release, supra note 4.

23 17 CFR 242.613(e)(2).

24 Report by the Chair of the CAT NMS LLC Operating Committee to Plan Participant Operating Committee Members, October 15, 2020.

25 The costs incurred by the SROs, including the NYSE Exchanges, include, among other things, costs for: (a) compensating and training for personnel, including regulatory and reporting compliance, project management, technology development, and legal personnel; (b) technology hardware and software systems to ensure proper CAT reporting by SROs and SRO member firms; (c) hardware and software systems for regulatory use of CAT Data; (d) coordinating implementation of SRO reporting and member firm reporting; and (e) legal resources to implement the CAT requirements. All of this investment and expenditure has been made in reliance on current CAT requirements, including the security requirements that are currently proposed to change.

satisfy a wide range of new mandates.[26] In addition, some of the Proposal's requirements would require significant alteration, or even abandonment, of projects or items for which SROs have already made investments in reliance on the existing, Commission-approved regulatory structure.

The upshot is that the Proposal would fundamentally change the cost/benefit analysis for the CAT. Although the Commission originally justified the CAT's substantial costs by pointing to corresponding benefits in the form of stronger regulatory oversight, many of those benefits would no longer materialize if the Proposal were adopted, and the costs of achieving whatever benefits remain would be considerably higher than originally forecast. The Proposal does not address these dynamics or show that the CAT's costs would continue to be justified if the proposed amendments were adopted and is arbitrary and capricious as a result.

II. The Proposal Does Not Adequately Address Its Effect on Efficiency, Competition, and Capital Formation.

Although the Exchange Act requires the Commission to address the effects of its action on efficiency, competition, and capital formation,[27] the Proposal neglects to discharge that obligation in several important ways. The Proposal does not contemplate the uneven impact it would have on the SROs—most notably by affecting FINRA differently than the other Participants.

Nor does the Proposal address that the fact that, by making it difficult, expensive, and perhaps impossible for exchanges to conduct their own regulation programs using CAT Data, the Proposal would require exchanges to outsource their regulatory programs to FINRA. The Proposal, therefore, substantially increases the likelihood of FINRA's role as a monopoly provider of most or all cross-market regulatory services, decreasing the amount of innovation in, and the diversity of, regulatory approaches. Ultimately, the consolidation would increase the risk of regulatory oversight becoming less effective.

III. The Proposal Overlooks Alternative Approaches to Securing CAT Data.

Rather than adopting the sweeping changes and new structures discussed in the Proposal, the Commission should rely on Regulation SCI—which already governs the CAT system, the SRO systems that would be used to access CAT data,[28] and the Plan Processor[29]—to ensure adequate security. The Proposal fails to address this alternative and more effective means of securing CAT Data and is arbitrary and capricious for that reason as well.[30]

---

26 See CAT NMS Plan Approval Order, supra note 2, at 84799-84897. See also Sections C and D of the CAT NMS Plan for discussion of the costs and benefits associated with the present CAT.

27 15 USC 78c(f).

28 Proposal, at Note 54.

29 See 17 CFR 242.1000 and 242.600(b)(55), and 15 USC 78c(22)(B).

30 See, e.g., *Am. Gas Ass'n v. FERC*, 593 F.3d 14, 19 (D.C. Cir. 2010) (agency must consider all "reasonable alternatives" raised in comments); *Chamber of Commerce v. SEC*, 412 F.3d 133, 145 (D.C. Cir. 2005) (same). Of the Proposal's 116 pages in the Federal Register, fewer than two pages are dedicated to the consideration of alternatives. See Proposal, at 66092-66093.

The Proposal also overlooks two other important alternative approaches. *First*, the Proposal does not explain why the current CAT security framework is insufficient. *Second*, the Proposal bypasses alternative approaches for handling PII and Customer IDs.[31] Existing SRO databases include sensitive data, including PII, and have found reasonable methods to manage the balance between security and usability. Yet rather than explore such options, the Proposal would move from a flexible system that can develop with technology and best practices to a rigid prescriptive standard that cannot evolve or change without a CAT NMS Plan amendment.

IV. The Proposal Exceeds the Commission's Authority.

A. The Proposal Conflicts with Rule 613.

The Proposal's new limitations are inconsistent with Rule 613's direction that the SROs must have access to CAT Data "for the purpose of performing [their] regulatory and oversight responsibilities," and that such access "shall not be limited."[32] The Proposal's mandates would sharply limit SROs' ability to access and utilize CAT Data. Nonetheless, the Proposal would charge the Plan Processor with substantial gatekeeping and monitoring authority.[33]

The Proposal does not squarely confront the ways in which it departs from Rule 613. Indeed, it does not address Rule 613's "shall not be limited" language at all. Nor does the Proposal provide "good reasons" for replacing that open-access guarantee with a new, restrictive regime in which many SROs will be unable to make meaningful use of CAT Data.[34] The Proposal's "failure to come to grips with conflicting [agency] precedent constitutes 'an inexcusable departure from the essential requirement of reasoned decision making.'"[35]

B. The Proposal Unlawfully Delegates Significant Regulatory Authority to the Plan Processor and Its Officials.

Section 11A of the Exchange Act states that the Commission may "authorize or require *self-regulatory organizations* to act jointly with respect to matters as to which they share authority under this chapter in planning, developing, operating, or regulating a national market system."[36] Likewise, Rule 608 assigns the responsibility for "implementing" and "administering" every NMS Plan to the SROs themselves.[37] Each SRO, which is statutorily required to "protect investors and the public

---

31 See letter from Scott W. Bauguess, Clinical Associate Professor of Finance, McCombs School of Business, University of Texas at Austin, to Ms. Vanessa Countryman, Secretary, Commission, dated November 30, 2020 ("Bauguess Letter").

32 17 CFR 242.613(e)(2).

33 See Parts I.A.1 and 2 and Part I.B, below.

34 See *FCC v. Fox Television Stations, Inc.*, supra note 21, at 515.

35 *Ramaprakash v. FCC*, 346 F.3d 1121, 1125 (D.C. Cir. 2003) (quoting *Columbia Broad. Sys. v. FCC*, 454 F.2d 1018, 1027 (D.C. Cir. 1971)).

36 15 USC 78k-1(a)(3)(B) (emphasis added).

37 17 CFR 242.608(a)(3)(iii).

interest,"[38] is also legally obligated to comply with the terms of each NMS Plan of which it is a sponsor or participant and charged with "enforc[ing] compliance with any [NMS] plan by its members and persons associated with its members." [39]

The Plan Processor, by contrast, has no obligations under Rule 608 to administer or implement the CAT Plan or to comply with its terms.[40] In addition, although they owe a fiduciary duty to CAT NMS Plan LLC, the CISO and CCO are Plan Processor employees and, similarly, have no obligations under Rule 608. Nothing in the Exchange Act authorizes the Commission to delegate its regulatory responsibility to entities or persons that, like the Plan Processor, CISO and CCO, have no obligations under Commission rules with respect to NMS Plans such as the CAT Plan. Nonetheless, the Proposal purports to grant significant regulatory authority to the Plan Processor, CISO and CCO, compelling them to perform certain obligations and oversee SRO compliance with the SROs' obligations under Rule 608.[41] If the Proposal were adopted as written, the Plan Processor, CISO, and CCO would be assigned responsibilities that would put them in a position of overseeing the SROs and would effectively give them authority to regulate SRO usage of CAT Data. Even though it is not authorized to do so under Regulation National Market System ("Regulation NMS"),[42] the Plan Processor and its employees would review what data an SRO extracted from the CAT, monitor the SRO's SAW, and determine when and whether the SRO could use any environment outside of a SAW to access CAT Data (a "Non-SAW").[43] In short, the Proposal would cause a limited liability company that is a subsidiary of one of the competing SROs, is not itself an SRO, has no regulatory obligations to implement, administer, or comply with the CAT Plan, or obligation to the SROs or the Commission, to perform the Commission's oversight responsibilities. The NYSE cannot support such an unlawful proposal.

For many of the same reasons, the Proposal violates the Constitution's Appointments Clause, which requires that every "Officer of the United States" must be appointed by the President, the courts, or the head of an executive branch department.[44] Commission regulations, including Rule 613 and the CAT NMS Plan Approval Order, establish the CISO and CCO as continuing offices, and the Proposal would vest those offices with significant governmental authority—for example by granting the CISO and CCO gatekeeping authority with respect to the SROs' use of CAT Data.[45] As a result, the CISO and CCO are "Officers of the United States" subject to the Appointments

---

38 15 USC 78f(b)(5),

39 17 CFR 242.608(c).

40 See Part IV.B, below.

41 See Proposal, at 66096-66101 (proposed amendments to Sections 4.12, 6.2, 6.5 and 6.13, and Appendix D, Sections 4.1.4 and 4.1.6).

42 17 CFR 242.600 et seq.

43 If an SRO met certain specific requirements, it would be allowed to use a non-SAW environment ("Non-SAW"). For a discussion of the risks relating to Non-SAWs, see Part I.B.1, below.

44 *Ass'n of American Railroads v. Dept. of Transportation*, 821 F.3d 19, 36 (D.C. Cir. 2016).

45 See note 41, supra.

Clause's requirements.[46] Because the CISO and CCO are appointed by the Plan Processor, rather than the Commission (or any other proper party under the Appointments Clause), they cannot be lawfully vested with the regulatory powers conferred by the Proposal, and their actions in carrying out the Proposal would be without force. The Commission should remedy this problem by refraining from delegating significant new responsibilities to the CISO and CCO.

V. The Proposed Implementation Periods are Unrealistic.

If adopted, the Proposal would require substantial changes to structures, policies, procedures and environments already created or in development. Based on experience, the NYSE disagrees with the proposed implementation periods set out in the Proposal. The various entities and individuals involved would not have sufficient time to meet the Proposal's demands, and each of the described tasks would be too significant, have too many consequences, and raise too many risks, to rush through.

---

46 *Lucia v. SEC*, 138 S. Ct. 2044, 2051 (2018).

Table of Contents

Discussion

I. The Proposal Would Undermine the CAT's Core Purposes.

The Proposal is arbitrary and capricious because it would prevent the CAT from serving the role it was originally designed to facilitate, while also making CAT and SRO data less secure than it is today—an outcome 180 degrees opposite the Proposal's stated purpose. Together, these effects would fundamentally alter the cost/benefit analysis that justified development of the CAT in the first place by reducing the CAT's benefits and markedly increasing its costs. The Proposal's failure to grapple with these important issues violates the APA's requirement of reasoned decision making and would leave the Proposal vulnerable to a court challenge if adopted.

At the outset, it is worth noting that the NYSE believes that the Commission has not adequately identified the specific problem that it is attempting to solve through the Proposal.[47] The Proposal does not establish that the existing security requirements mandated by Rule 613 and the CAT NMS Plan—both of which the Commission approved—are inadequate to meet the system's security needs. Nor does the Proposal show that the existing framework will be unable to address future security threats. Instead, the Proposal appears to be founded on a desire to "enhance" the CAT's security for security's sake. That rationale cannot suffice given the significant adverse effects the Proposal would have on the CAT and the SROs that rely upon it to carry out their regulatory obligations.

A. The Proposed Amendments Would Make CAT and SRO Data Less Secure and Increase the Risk of a Major Data Breach.

1. The Proposal Would Create an Exponentially More Valuable Target with a Single Point of Failure.

Although purportedly designed to increase the security and confidentiality of CAT Data,[48] the Proposal would in fact create significant new security risks. Many of the security risks would be created as a direct result of the proposed requirements that SROs use SAWs to access and analyze CAT Data, and that SROs be permitted to use Non-SAW environments only in limited circumstances (if at all). More specifically, the proposed amendments would

> require the Plan Processor to create secure analytical workspaces, direct Participants to use such workspaces to access and analyze PII and CAT Data obtained through the user-defined direct query and bulk extract tools described in Section 6.10(c)(i)(B) of the CAT NMS Plan, set forth requirements for the data extraction, security, implementation, and operational controls that will apply to such workspaces, and provide an exception process

---

[47] See Memorandum to Staff of the Rulewriting Divisions and Offices, from RSFI and OGC (March 16, 2012), at note 15, citing Executive Order 12866 (September 30, 1993), 58 FR 51735 (October 4, 1993) ("Each agency shall identify the problem that it intends to address (including, where applicable, the failures of private markets or public institutions that warrant new agency action) as well as assess the significance of that problem").

[48] Proposal, at 65991. The Commission does not make a meaningful case that there is an existing problem that the proposed measures would resolve. See Part I.B, below.

> that will enable Participants to use the user-defined direct query and bulk extract tools in other environments.[49]

These proposed mandates are based on the Commission's belief that requiring the creation and use of SAWs would "minimize the attack surface associated with CAT Data," "maximize security-driven monitoring of CAT Data, both as it is reported to the CAT and as it is accessed and utilized by regulators," and "leverage … security controls and related policies and procedures that are consistent with those that protect the [CAT] Central Repository."[50]

The Proposal does not meaningfully quantify or qualify the benefits that would result from a reduction in attack surface[51] by consolidating all CAT Data and usage into a single security perimeter controlled by the Plan Processor or improvements in monitoring and controls due to the creation of the SAWs, and does not weigh any benefit against the risk from increased exposure of SROs regulatory systems and data. These deficiencies reveal that the Commission has not adequately considered or justified whether the SAWs would address the Proposal's stated goal, or that the SAWs would resolve any specific problems with the current security framework.[52]

The NYSE believes that any hypothetical reduction in security risk to CAT Data resulting from mandatory usage of SAWs would more than be offset by the new security risks created by that approach, which could make it impossible as a practical matter for SROs to use CAT Data in their internal regulatory programs.[53]

These risks arise because, under the Proposal, SAWs would effectively be the only means of accessing and analyzing CAT Data and would be the *only* means of accessing and analyzing CAT-related personally identifiable information ("PII").[54] To comply with their regulatory mandate and the requirements of the CAT NMS Plan,[55] the SROs would have to move their proprietary non-CAT data and regulatory systems from their current, segregated, highly secure, SRO-specific environments, into the SAWs. This migration would require an SRO to move complex, proprietary regulatory systems designed to provide the highest levels of security within the walls of the SRO outside of that environment. Such migration would be unprecedented in terms of risk from change

---

49 Proposal, at 65992.

50 Id., at 65995.

51 "Attack surface" refers to the sum of the points at which an unauthorized user could attempt to enter or extract data—i.e., the extent of the CAT's overall exposure to cyberattacks.

52 The framework is described in the CAT NMS Plan and Rule 613. See CAT NMS Plan Approval Order, supra note 2, and Rule 613 Adoption Release, supra note 4. See also discussion in Part IV.B.4, below.

53 For a discussion of the Proposal's potential impact on the cost/benefit analysis that an SRO would make when determining whether to use CAT Data, see Part I.B, below.

54 SAWs would be the only means of accessing and analyzing Customer and Account Attributes. As proposed, Participants could use an online targeted query tool to extract a limited amount of other CAT Data, primarily transaction data, from the Central Repository outside of a SAW. See Proposal, at 65992 and 66099 (proposed Section 6.13(a)(i)). Extracting data for integration into SROs' systems would be prohibitively limited by the terms of the Proposal. See Part I.B.1, below.

55 See CAT NMS Plan Section 6.7(a)(iv) and 6.10(a).

to these systems and exposure of sensitive and proprietary data. Further, as part of this migration, the SROs would have to transfer PII and proprietary third party data obtained from other sources—such as transaction data not required to be reported to the CAT, proprietary surveillance programs and patterns, surveillance exceptions, investigation records, and a case management system—into the CAT's SAW environments.[56] The end result would be that sensitive and proprietary information, including the granular details of surveillance patterns, code, alerts, and investigations, as well as SRO-specific data needed for surveillance, would move outside of the SRO's security perimeter into the SAW.[57]

Importing all this information would significantly expand the scope of the data stored in the CAT and greatly increase the value of the CAT as a target for bad actors, potentially increasing the frequency and intensity of attempted attacks. Even if the attack surface were reduced through centralization in the SAW, the concentration risk would increase, since, in the event of a security breach in any SAW, not just CAT Data but also any non-CAT data or regulatory system brought into the SAW would also be vulnerable.

It is important to note that the risks created by the SAW structure are not just risks for the SROs. Because of the enriched data made available within a SAW environment, member firm data and data from other sources would also be exposed, as transactional and customer data would by necessity be uploaded into one or more SAWs during the normal course of an investigation, as they are required elements of SROs' regulatory programs. Further, the Commission's proposal to remove most PII from the CAT central repository[58] would become meaningless if the SROs were required to use SAWs to conduct regulatory activities, which would necessitate the addition of non-CAT PII into the CAT in order to perform such activities. A framework that excludes PII in one part of a system but leads to PII being imported elsewhere does not result in net security gains—a fact the Proposal fails to address.

Importantly, a security breach in one SAW could mean a breach in the entire CAT, significantly increasing the scale of the risk the proposed requirements would create. Presently, the central repository of the CAT is hosted in an Amazon Web Services ("AWS") cloud environment.[59] Forcing

---

[56] The PII and other data that the SROs would have to add to their SAWs may include data originating from outside the U.S., which could subject the SAWs to foreign data privacy regulation. The Commission does not consider this potential consequence of the Proposal, which would create additional layers of potentially conflicting regulation, and could ultimately open up the CAT to the scrutiny of foreign regulators or curtail the SROs' regulatory efforts involving certain data.

[57] Given the risks that the SAWs create, an SRO may opt to manage its surveillances, case management, and regulatory records in an environment separate from the SAW. In such a case, the SRO would have two environments, SAW and non-SAW. Having dual tracking systems would introduce other risks. For example, there could be data security risk resulting from staff having to train for, understand, and maintain two environments, or increased operational risks from technology staff being required to manage configurations, settings and different software tools and vendors in two environments.

[58] In March 2020, the Commission granted the SROs' request for an exemption from reporting certain PII to the CAT, conditioned on the SROs meeting enumerated conditions. See Securities Exchange Act Release No. 88393 (March 17, 2020), 85 FR 16152 (March 20, 2020) (order granting exemptive relief). The Proposal would amend the CAT Plan to incorporate the substance of this exemption. See Proposal, at 66084.

[59] Id., at 66075.

all SROs' regulatory programs into a single SAW ecosystem would mean that if there is a flaw in the SAW created by the Plan Processor, such as a misconfiguration that allows broader access than intended, or a vulnerability in the infrastructure of AWS (or any successor), it would affect the CAT and *all* of the SROs' non-CAT regulatory data that had been uploaded into the SAWs. The entire CAT could be compromised, and the regulation of all U.S. national securities exchange markets could be affected through a single intrusion. This significant risk does not exist if each SRO continues to use its own separate analysis environment, as currently contemplated by the CAT NMS Plan.[60] The dependency on a single security format or single third party, such as AWS or the Plan Processor, does not exist under the current CAT NMS Plan than it would be under the Proposal because SROs are not currently obligated to use a particular vendor before interacting with CAT Data.[61]

The Proposal would require all the SAWs be operated and monitored by one entity and would thus increase the insider threat to the CAT and to SROs' proprietary systems that would otherwise be separated from the Plan Processor. The Proposal posits that, by establishing additional administrative clearance to that already required by the CAT NMS Plan and Rule 613, use of a SAW "may reduce the amount of CAT Data exposed to regulators."[62] However, this reasoning does not adequately take into account the increased access to non-CAT data and regulatory systems that would be created by the Proposal, or the correspondingly greater risk of exposure of industry data and trade secrets among competitors. Nor does the Proposal adequately address whether SROs should, or even could, organize their operations and entitlements such that SRO staff who have access to non-CAT data and regulatory systems that are housed within the CAT system would be prevented from having access to CAT Data when, but for their need to access non-CAT

---

60 See CAT NMS Plan, Sections 6.2(b)(vii), 6.5(f)(ii) and (iii), and 6.5(g). The policies are subject to review by the CISO.

61 Mandating that the SROs use SAWs within the same security perimeter as the Plan Processor would force SROs to the same third-party vendor as the Plan Processor (i.e., AWS). It would eliminate any negotiating power an SRO might otherwise have if there were competition for such services, because each SRO would be required to contract with AWS before it could access or use CAT Data. For example, under the Proposal, if AWS were to create conflicting policies, force agreement changes, set prohibitive prices, or be influenced by other customers, the SROs would not easily be able to negotiate a change, much less terminate AWS' services. Moreover, the SROs' inability to move the CAT to another database host provider would prevent them from effectively managing the costs of the CAT system. By contrast, under the current CAT NMS Plan, which allows a diversity of providers, the SROs have more options. The Commission has neglected to sufficiently consider this long-term cost of the Proposal.

62 Proposal, at 66084 (discussing "provisions that establish that access to Customer Identifying Systems are subject to certain restrictions, including requiring that authorization to use Programmatic CAIS Access or Programmatic CCID Subsystem Access be requested and approved by the Commission"). See also id., at 66085 ("The Commission recognizes that a possible indirect cost of the proposed amendments is less overall regulatory use of CAT Data"). Reducing the number of regulators with access to CAT Data is contrary to one of the primary purposes of the CAT. See CAT NMS Plan, Rule 613(e)(2) (providing that "access to and use of such data by each national securities exchange, national securities association, and the Commission for the purpose of performing its regulatory and oversight responsibilities pursuant to the federal securities laws, rules, and regulations shall not be limited"); and CAT NMS Plan Approval Order, supra note 2, at 84830 ("The Commission explained that the Plan would bring audit trail data related to trading on all venues into the Central Repository where it could be accessed by all regulators").See Part I.B, below, for a discussion of the changes to the cost/benefit analysis.

data or regulatory systems, they would not otherwise have access to the CAT. In addition, insider risk would be created under the Proposal by allowing Plan Processor staff to access and oversee a SAW with non-CAT data and SROs' proprietary regulatory systems, including surveillance logic, investigatory records, and other metrics and sensitive information that would affect SROs' ability to regulate effectively.

Currently, an SRO's regulatory systems and data, including transactional and customer data, are not exposed outside of the security perimeter of the SRO.[63] They are secured by the SRO's own security programs, which also secure other aspects of the SRO's business, are subject to Regulation SCI, and receive regulatory scrutiny and oversight from Commission staff. NYSE regulation's security policies and procedures have been certified to be comparable to security policies and procedures of the Plan Processor, as required by the CAT NMS Plan.[64] The Commission has not adequately explained by such policies and procedures are insufficient to secure CAT Data.

If these systems and data were forced into a SAW, a new risk would be created from the moment of transfer: the required migration of data and systems to the SAW would introduce security risk that does not accrue to data and systems that the SROs maintain internally. Modifying controls, security implementations, and security infrastructure to export regulatory data and systems would add a level of risk that the Commission does not adequately consider in the Proposal, even though the risk is foreseeable, and would be created for all the data and systems that would be introduced to the SAW.[65] The Proposal also does not adequately address the implications with respect to maintaining the confidentiality of regulatory data. SROs would not be able to ensure the confidentiality of data that is migrated into an environment that is not in their control, but rather in the control of the Plan Processor.

Finally, the Proposal does not adequately address the issues that the Customer Identifying Systems Workflow ("CISW") would create with respect to the SAW. In the Proposal, the Commission proposes "to define the [CISW] for accessing Customer and Account Attributes, and to establish restrictions governing such access."[66] Accordingly, the SAW would be the only means for SROs to access and analyze Customer and Account Attributes.[67] The security safeguards

---

63 Some data may be provided to FINRA in the course of its regulatory work on behalf of an SRO or utilized in a litigated regulatory action. As these regulatory systems and data, associated operational, network, and security elements, generally are not maintained or exported outside of an SRO's security perimeter, the feasibility, effort, cost, and exposure risk from the migration process is unknown. The Proposal does not address this issue.

64 See CAT NMS Plan, Sections 6.2(b)(vii), 6.5(f)(ii) and (iii), and 6.5(g). See also CAT NMS Plan Approval Order, supra note 2, at 84757-84758.

65 The Proposal introduces a new transition risk due to moving from a known and tested program code base and environment to a new code base and environment, as well as the ongoing risks of concentration of SRO-specific data in the SAW environments and insider threat. Migrating regulatory systems and data currently secured within the SROs environments has the potential to introduce vulnerabilities to not only an SRO's regulatory systems and data, but to the CAT and all SROs regulatory programs housed in the CAT.

66 Proposal, at 66024.

67 Id., at 66099.

implemented in an SRO's SAW would be applied "to protect all access to Customer Identifying Systems, leveraging security controls and related policies and procedures that are consistent with those that protect the Central Repository."[68] Requiring CAT Data access through the SAW would enable the Plan Processor to capture information about CAT usage by SROs, such as the content of queries made to the CAT in the course of surveillance and investigation. As a result, if adopted, the Proposal would again increase insider risk, because the Plan Processor would have access to detailed information about SRO CAT Data usage and activity in SROs' regulatory programs that could be related to ongoing, non-public investigations.

2. The Proposal Would Force SRO Reliance on, and Disclosure to, the Plan Processor.

The Proposal would force the SROs to rely on the Plan Processor, which is currently a FINRA subsidiary, to an unprecedented degree—and would likewise purport to grant the Plan Processor broad access and control over SRO regulatory environments.[69] The Commission's Proposal assigns responsibility to the Plan Processor, which is neither a self-regulatory organization nor a Participant in the CAT NMS Plan, to build, control and monitor the SAWs that the SROs would need to run surveillance programs using CAT Data.[70] In addition, the CISO and CCO, who are Plan Processor employees, would be required to monitor and report on the SROs' activities within their SAWs, either in the CAT or in the SROs' own regulatory programs. As discussed further below, the NYSE does not believe that the Commission can assign obligations under an NMS Plan to persons that are not SROs.[71]

Such access would create new security and operational risks. The Plan Processor would have access to all proprietary data that the SROs introduce to their SAWs, including surveillance results. The Proposal also requires the Plan Processor to share information regarding each SRO's regulatory program with the Operating Committee, potentially revealing such proprietary data to competitors.[72] These proposed requirements would create additional impediments to the SROs' ability to use CAT Data in their regulatory programs, potentially leading SROs or the Commission

---

68 Id.

69 Id., at 66028.

70 If an SRO was approved by the Plan Processor to use a Non-SAW environment, the SRO would still not be out from under Plan Processor control. The CISO and CCO would determine whether a proposed Non-SAW environment were acceptable. To grant the required exception to the SAW requirement the CISO and CCO would "determine, in accordance with policies and procedures developed by the Plan Processor, that the residual risks identified in the security assessment or detailed design specifications provided by the requesting Participant do not exceed the risk tolerance levels set forth in the risk management strategy developed by the Plan Processor for the CAT System pursuant to NIST SP 800–53." Id., at 66055. In other words, employees of the Plan Processor would determine whether and when an SRO could use a system other than the Plan Processor's SAW based on policies and procedures determined by the Plan Processor itself. The Proposal does not seem to recognize the risk of a conflict of interest this would create, nor does it acknowledge that this arrangement essentially presents a false choice that no SRO is likely to pursue. See Part I.B.1, below.

71 See Part IV.B, below.

72 See Proposal, at 66097 (proposed Section 4.2), and 66099 (proposed Section 6.13(d)). The Operating Committee includes representatives of each SRO.

to conclude that exchanges' own regulatory programs are insufficient and requiring instead that an SRO pay a third party for the regulatory activities it is required to conduct.

a. Plan Processor SAW Responsibilities

The Commission's desire for the Plan Processor to monitor the SAWs seems to drive the entire proposed alternative structure of the CAT, despite the fact that it is the SROs, not the Plan Processor, are the participants in the CAT NMS Plan with obligations under the Commission's rules to implement, administer and comply with the CAT NMS Plan.[73] The Proposal sets forth the Commission's logic as follows:

> [t]he Commission preliminarily believes that the alternative of allowing each Participant to build its own SAW would inhibit the Plan Processor's ability to control, manage, operate, and maintain the CAT System, which would include the SAWs. . . .
>
> If each Participant were permitted to build the common security controls for its SAW account without the input or knowledge of the Plan Processor, different Participants might make different (and potentially less secure) decisions about how to implement the information security program or the proposed CISP. These different decisions could, in turn, hamper the Plan Processor's ability to consistently monitor the SAWs, because it would be difficult for the Plan Processor to automate its monitoring protocols or to uniformly monitor SAWs that had been not been [sic] uniformly implemented. A lack of consistent monitoring could endanger the overall security of the CAT, because the Plan Processor could be less likely to identify non-compliance with the CISP or with the SAW design specifications.[74]

In other words, the Commission appears to believe that allowing a variety of regulatory decisions would be dangerous, that the Plan Processor must be able to monitor (and, implicitly, second guess) the security structures employed by the SROs,[75] and that the best way to avoid the first and ensure the second is to force the SROs to use SAWs that are under the Plan Processor's control, since the Plan Processor is the best party to identify non-compliance.

The Proposal's reasoning is incorrect. First, allowing each SRO to build the controls for its own SAW might result in different decisions about how to implement the information security program or proposed CISP, as the Proposal notes, but that outcome would strengthen, rather than undermine, the CAT's security. Each SRO's structure, market position, and regulatory program is distinct, with secured environments carefully tailored to its specific needs and risks. Strict adherence to a generic concept that may become obsolete, as described in the Proposal, would make that SRO's

---

73 See Part IV.B, below.

74 Proposal, at 65996.

75 The Plan Processor would be required to monitor each SRO's SAW for compliance with the CISP and the detailed design specifications developed pursuant to 6.13(b)(i), and notify the SRO of non-compliance. See id., at 66099 (proposed Section 6.13(c)(i)). Indirect consequences may arise: proposed Section 6.13(c)(iii) would allow each SRO to "provide and use its own choice of software, hardware configurations, and additional data within its SAW, so long as such activities otherwise comply with the [CISP]." Id. Given that it is the Plan Processor who would approve and monitor each SRO's SAW for compliance with the CISP, the freedom granted by proposed Section 6.13(c)(iii) would seem to be illusory.

environment weaker. The Commission even acknowledges that, absent the Proposal, certain SROs might have stronger security than what the Proposal would require, but does not adequately explain why that scenario is less desirable.[76] The Proposal would lead to weaker security for those SROs' environments. Having a diversity of security controls would mean that the Operating Committee and the existing security working group ("ESWG") could benefit from testing different approaches to similar issues and the SROs might be inclined to share security best practices. The Proposal ignores all these considerations.

In addition, the Proposal's requirement that SROs interact with CAT Data only within the SAW would create a technology barrier, because SROs would be required to program surveillances to work within that environment. SROs' ability to use their existing surveillances or create innovative new surveillances as market conditions and structures change would be impaired. The time to market would be increased due to SROs' dependence on approvals from, and restrictions imposed by, the Plan Processor, as well as the requirement for programming in an environment that is not within their control.

The reduced access to CAT Data that would result from the restrictions in the Proposal would, thus, fundamentally and seemingly intentionally limit the consolidated audit trail tool that the Commission required be developed and made available to regulators for increased and more efficient market oversight. Fewer regulators analyzing CAT Data would reduce the ability for regulators to rapidly adapt to changes in market conditions and market structure. These impacts would drastically diminish many of the benefits contemplated by the Commission when Rule 613 was adopted and the CAT NMS Plan was approved,[77] as "[t]he utility of the Central Repository is dependent on regulators being able to have access to data for use in market reconstruction, market analysis, surveillance and investigations."[78]

Presently, each proposed environment is subject to review by the CISO, and each of a SRO's security policies and procedures must be certified by the CISO as comparable to the CAT's security policies and procedures.[79] Even if environments differ from each other, under the present CAT NMS Plan a comprehensive review must be conducted to ensure that the controls meet the CAT NMS Plan's security mandates. The Commission has not adequately addressed why this present practice is inadequate.

---

[76] Id., at 66092 ("The Commission recognizes that this variability could also lead to some analytic environments being more secure than they would be under the proposed approach").

[77] The Commission explained that the CAT would, among other things, increase data availability to regulators, improve regulatory oversight of the U.S. securities markets, and improve efficiency of regulation, thereby improving securities markets and lowering costs of capital. The Commission anticipated that availability of accurate data to regulatory staff would reduce "data delays and costly data investments [that] would permit regulators to complete market reconstructions, analyses, and research projects, as well as investigations and examinations, more effectively and efficiently, and would lead to improved productivity in the array of regulatory matters that rely on data, which should lead to improved investor protection." CAT NMS Plan Approval Order, supra note 2, at 84829. See generally id., at 84816-84897.

[78] CAT NMS Plan, at Appendix C, Section 2(b).

[79] See id., at Sections 6.2(b)(vii), 6.5(f)(ii) and (iii), and 6.5(g). See also CAT NMS Plan Approval Order, supra note 2, at 84757-84758.

The Commission has not shown why the current practice is inadequate, or shown that the additional measures contemplated by the Proposal are necessary. The NYSE is not aware of any actual issue that would be addressed with the significant expansion of the role of the Plan Processor. In fact, the current responsibilities and structure of the Operating Committee and Plan Processor, as well as the current security requirements, allow for continued enhancement of the security profile if and when issues arise, as well as when technology and best practices evolve.

The Proposal is predicated on the assumption that the Plan Processor would be able to deliver on the new requirements in a satisfactory manner. The Plan Processor's role would expand to require that it develop, maintain, and make available detailed design specifications for the technical implementation of the access, monitoring, and other controls required for SAWs by the CISP; create, control, and monitor the SAWs themselves; assess and monitor any Non-SAW environments; and conduct myriad other activities.[80] Yet the required design specifications and policies have not been created, giving rise to a risk that the Plan Processor will be unable to create them in a manner that would satisfy the proposed requirements.

If the Plan Processor is unable to meet its new requirements in the timeframes set by the Commission, it is the SROs that would be held accountable, as only they are obligated to comply with the terms of the CAT NMS Plan.[81] The Plan Processor is not responsible under the securities laws. Moreover, the Plan Processor Agreement does not contemplate the proposed requirements and it is unknown whether the Plan Processor would agree to modify the agreement to meet the requirements in the Proposal, what time frame would be required, or what the additional cost to the SROs might be. Finally, the Proposal requires the SROs to enter into an agreement with the Plan Processor to perform the enumerated functions, even though such functions include areas where the NYSE does not believe the Plan Processor has subject-matter expertise.

The Proposal does not establish that the implementation requirements are feasible or propose an alternative if not all the requirements in the Proposal prove feasible. It does not address how long it would take the Plan Processor to engage additional staff with sufficient expertise over every type of data, software, and surveillance that the SROs currently use in their own environments and build additional technology to assist with the oversight described in the Proposal—assuming that these steps are possible in the first place. In addition, the Proposal indicates that the Commission does not realize that multiple parties would have to play a role, including not just the SROs and Plan Processor, but also AWS, third party network providers, and security vendors, to name a few.

Ultimately, the Proposal would create the new risk that not all its requirements could be met—an outcome that likely would result in delays to completion of the CAT system. Such delays could include delays in implementation or approval of the SAWs, which would force SROs to abandon

---

[80] The Plan Processor, as designated by the SROs pursuant to the CAT NMS Plan, is responsible for implementing security for the CAT and for reporting back to the Operating Committee to ensure compliance with the security requirements in Rule 613 and the CAT NMS Plan. See CAT NMS Plan, Appendix D, Section 4. The Plan Processor is subject to obligations defined by the agreement between the Plan Processor and CAT NMS LLC (the "Plan Processor Agreement") and is subject to termination according to its terms. The Plan Processor does not have independent oversight responsibilities outside of those defined by the Plan Processor Agreement and the CAT NMS Plan. For the requirements for the Plan Processor under the proposed changes to the CAT NMS Plan, see note 17, supra and Part I.B.1.a, infra.

[81] 17 CFR 242.608(c).

their use of CAT Data, software, or surveillance programs that the Plan Processor could not properly assess or monitor. Potentially, the SROs would have to cease using the current Plan Processor if it could not satisfactorily assure the SROs of its ability to meet all requirements in a timely manner.[82] The Proposal is arbitrary and capricious because it fails to address these important aspects of the problem.

b. CISO and CCO Monitoring Responsibilities

Even as the Proposal suggests making the CISO and CCO the gatekeeper to, and monitor of, the SAWs and use of CAT Data, the Proposal does not adequately consider the risk it is creating for the regulatory programs of the SROs, much less the risk of bias in favor of FINRA.

The CISO and CCO are employees of the Plan Processor, which is an affiliate of one of the SROs. At the same time, the CCO and CISO are officers of, and owe fiduciary duties to, CAT NMS Plan LLC, the company through which the SROs conduct the activities of the CAT.[83] The Proposal would charge the CISO and CCO with significant responsibilities,[84] including monitoring and reporting on the SROs' activities within their SAWs.

The Proposal does not adequately address the risk created by the requirement to report on confidential regulatory activity to an Operating Committee comprised of competitors. In addition, CAT NMS Plan LLC has no employees, so it is realistic to expect that the CISO and CCO will use their employer, the Plan Processor, and potentially even seconded employees from its parent, FINRA, to carry out the monitoring, at least in part. Given that the CAT NMS Plan will be in place for an indefinite period, it is realistic to consider the risk that an individual CISO or CCO could align with his or her employer and its parent FINRA more than with the CAT, and be unduly influenced in decision making regarding regulatory need and security risk. In such a case, the Proposal gives the CISO and CCO, or an employee of the Plan Processor acting on their behalf, opportunity to compromise the SROs' regulatory programs and data.

Under proposed Section 6.6(b)(ii)(B)(3), the CCO and CISO would be required to conduct periodic reviews of the "quantity and type of CAT Data extracted from the CAT System to assess the security risk of permitting such CAT Data to be extracted and identify any appropriate corrective measures…"[85] The granularity of such review is boundless. The decisions on what and how to monitor would not be in the hands of the SROs' regulator, the Commission, but in the hands of the CISO and CCO. With information regarding the quantity and type of CAT Data searched or reviewed by an SRO, the CCO and CISO or a Plan Processor employee could see the quantity and type of CAT Data extracted by an SRO and could extrapolate the underlying queries, surveillance logic, or other confidential information. Sensitive or proprietary SRO information,

---

82 As an example, to effectively review regulatory systems put into a SAW, the CISO and CCO likely would need access to the source code. However, many of those regulatory systems would be licensed from third parties, who would not necessarily provide the Plan Processor with access to their source code, leading to each of the enumerated risks.

83 See Proposal, at notes 3, 28 and 71.

84 See note 41, supra.

85 See Proposal, at 66098-66099.

including specific investigatory targets and methods, likely would be placed at increased risk by the required monitoring by employees of an SRO's competitor.

3. Requirements for Confidentiality Policies Would Decrease the Effectiveness of the SROs' Security Measures.

The Proposal would require SROs to create and maintain identical Proposed Confidentiality Policies.[86] A review of the requirements set forth in proposed Section 6.5(g)(i) shows that the requirement for identical Proposed Confidentiality Policies likely would decrease the effectiveness of the SROs' security measures.

SROs come in different shapes and sizes: some are subsidiaries of multinational entities subject to numerous regulators and legal regimes, while others are smaller domestic entities with one primary regulator. As a practical matter, like any common policy, the Proposed Confidentiality Policy would be highly unlikely to be responsive to their varied institutional concerns.

Accordingly, the Proposal would mean that many, if not all, SROs would need to have two confidentiality policies: one internal that applies specifically to that SRO and its organization, and one common one for the CAT that only addresses the requirements in the CAT NMS Plan. The former would be responsive to the specific needs of the SRO, and the latter would be to comply with proposed Section 6.5(g)(i). Because the terms of the Proposed Confidentiality Policy would by necessity trump any internal policy, an SRO is likely to need to revise its internal policies to comply with the terms of the Proposed Confidentiality Policy, irrespective of whether the changes improve its current policies. Further, having such dual policies increases the costs and complexity of administering security requirements, and increases the likelihood of the misapplication of the wrong policy. Consequently, these proposed requirements would increase the risk to the security and confidentiality of CAT Data that the Proposal purports to decrease, while also creating risks for non-CAT data and systems. The Commission has not adequately considered these risks introduced by requiring a uniform policy across SROs.

One potential result of the Proposal would be that the SROs establish a shared Proposed Confidentiality Policy that is sufficiently general to be almost meaningless.[87] For example, proposed Section 6.5(g)(i)(G) would require the Proposed Confidentiality Policy to "define the individual roles and regulatory activities of specific users" of CAT Data.[88] But as the Proposal itself recognizes, not every SRO is organized in the same way. Moreover, pre-determining the regulatory activities of specific users would limit their flexibility and access to CAT Data, one of the benefits identified in the Commission's release adopting the CAT NMS Plan.[89] As a result, it would be difficult to define individual roles and regulatory activities of specific users that could fit all the SROs and all possible circumstances. A policy that did so would likely have to be very broad and

---

86 See id., at 66037 and 66098.

87 If an SRO opted to only have one policy, it would have to be the Proposed Confidentiality Policy. That would leave the SRO open to the risk that its policy did not cover confidentiality issues specific to that SRO's institution.

88 Id., at 66098.

89 See CAT NMS Plan Approval Order, supra note 2, at 84829.

therefore almost meaningless—making the creation of a second, more accurate internal SRO confidentiality policy that much more likely.

Given all of the above, the Commission has failed adequately to consider the security impact from having a single, identical Confidentiality Policy that replaces the well-designed individual policies in place under the CAT NMS Plan,[90] much less identified a problem with the current practice.[91] In fact, the NYSE believes that the current practice is stronger than the one proposed. Each SRO is in the best position to determine its specific needs and oversee the implementation of its policies and related procedures, consistent with SROs' obligations under Regulation SCI. If the Commission believes there are inadequacies in the SROs' current confidentiality policies and procedures, it should consider whether it is appropriate to make changes to Regulation SCI. It does not seem that the Commission seriously considered this option or other options that may resolve the undefined issue that the Commission purports to seek to resolve.

4. The Proposal Would Compromise the CAT NMS Plan's Adaptability.

Standards change over time. Prescriptively imbedding a security practice in the CAT NMS Plan would make it more difficult for the CAT NMS Plan to keep up with best practices or implement the latest standards, since any time an adjustment is merited, the NMS Plan would have to be amended. Overall, such an NMS Plan would become more rigid, less adaptable, and ultimately less secure. To avoid such rigidity leading to less security, Regulation SCI does not prescriptively establish practices, but rather states that policies and procedures "shall be deemed to be reasonably designed if they are consistent with current SCI industry standards."[92] Indeed, when approving the CAT NMS Plan, the Commission noted "the Participants' recognition that regulators should have flexibility in designing . . . surveillance systems, including the ability to access and transfer data where necessary and consistent with appropriate data security safeguards." [93]

By contrast, the Proposal would reduce the CAT NMS Plan's flexibility by specifying standards and practices in the CAT NMS Plan. As a result, unlike now, the Operating Committee would not be able to implement future best security practices or otherwise incorporate any more effective or secure controls that may emerge as technology evolves—or may be necessary as markets change—without amending the NMS Plan, a process that requires extensive negotiation between

---

90 See CAT NMS Plan at Section 6.5(g).

91 The SROs' current security policies are reviewed by the CISO for comparability with the security policies of the Plan Processor and in compliance with a policy established in consultation with the existing security working group ("ESWG") and approved by the Operating Committee. See id., at Sections 1.1 and 6.2(b)(vii). See also Proposal, at 65993.

92 17 CFR 242.1001(a)(4). The section goes even further, noting that compliance with SCI industry standards is not the exclusive way to comply with the requirements set forth therein. Id.

93 CAT NMS Plan Approval Order, supra note 2, at 84757. In the same release, the Commission stated "that Rule 613 provided the SROs with 'flexibility in how they [chose] to meet the requirements of the adopted Rule,' allowing the SROs to consider a number of different approaches in developing the CAT NMS Plan." Id., at 84699. See also CAT NMS Plan Section 6.2(b)(v)(G) (requiring that the policies, procedures and control structures in place to deal with data security issues with the Central Repository include industry standards); Section 6.6(b)(ii)(B)(3) (requiring that the policies, procedures and control structures are assessed on a yearly basis for consistency with the highest industry standards); and Appendix D, Section 4.2 (setting forth a non-exclusive list of examples of industry standards).

parties to obtain consensus and agreeable terms, and approval by the Commission. Similarly, the implementation of better or less expensive technology could be prohibited by codification of older standards and practices. The Proposal does not consider the regulatory delays and costs that amending the CAT NMS Plan would entail. By creating centralized, rigid structures and obligations, the CAT would not be able to keep up with current best practices without a plan amendment, and regulators could be forced to work in a static, constrained environment in the meantime.[94] It is not clear from the Proposal what benefit the Commission believes such rigidity would preserve regarding evolving security best practices.

Below are some examples of where the proposed provisions would add prescriptive requirements to the CAT NMS Plan, illustrating how the Proposal would lead to a CAT NMS Plan that is more rigid and, ultimately, less able to maintain the security and confidentiality of the CAT Data. The Commission has not adequately considered this important problem that the Proposal would create.

a. NIST Cyber Security Framework

The NIST Cyber Security Framework ("NIST Framework") is a current industry standard.[95] If the Proposal were adopted, it would incorporate the NIST Framework into the CAT NMS Plan without recognition that the standard may change.[96] Use of the NIST Framework is not new: the present CAT NMS Plan already refers to the NIST Framework, including it on a non-exclusive list of industry standards that must be followed.[97] Importantly, that list does not require adherence to the listed industry standards for all time. Rather, it explicitly acknowledges that the standards could change, and "may be replaced by successor publications, or modified, amended, or supplemented."[98] The current Plan thus gives the Operating Committee the discretion to approve changes when security interests warrant.

Without clearly identifying a problem with the current practice, the Proposal would sacrifice this flexibility by mandating the use of NIST SP 800–53 (Security and Privacy Controls for Federal

---

94 In addition, the security requirements proposed to be imbedded in the CAT NMS Plan could make it impossible for SROs to comply with both Rule 608(c), which requires SROs to comply with the terms of an NMS Plan, and Regulation SCI, under which the SROs are required to have policies and procedures for their SCI systems, which includes the CAT system, consistent with current SCI industry standards. See 17 CFR 242.608 and 17 CFR 242.1001(a)(1).

95 The Proposal seems to consider the NIST Framework as more helpful than it may be. The NIST Framework is just that, a framework, and not a set of requirements. It provides guidelines to be considered, not clear statements. This could lead to confusion in policy implementation and reviews. While the Proposal gives the appearance of providing a consistent standard, in reality it just shifts the burden from review of the controls implemented to the analysis of how the applicable NIST Framework controls were chosen. There is not a single definition of "required by NIST SP 800–53." See "Security and Privacy Controls for Information Systems and Organizations," NIST Special Publication 800-53 Revision 5 (September 2020), available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

96 For example, NIST 800-53 was initially released in February 2005, and had its fifth revision published in September 2020.

97 See note 93, supra.

98 Appendix D, Section 4.2 of the CAT NMS Plan. The Proposal does not suggest amending the cited text.

Information Systems and Organizations) in several cases. For example, the expanded Comprehensive Information Security Program ("CISP") required by proposed Section 6.12 would be defined to explicitly include "organization-wide and system-specific controls and related policies and procedures required by NIST SP 800–53."[99] As the Proposal states, this would make the NIST SP 800–53 information security program specifically applicable in various areas:

> the proposed amendments, by referencing NIST SP800–53 in the definition of the CISP, would amend Section 6.12 of the CAT NMS Plan to explicitly require the information security program to apply broadly at an organizational level—that is, to address specific organizational mission and/or business needs and risk tolerances for all of the information and information systems that support the operations of the Plan Processor and the CAT System, including Secure Analytical Workspaces. The proposed amendments would also explicitly require the information security program to be applied to information systems within the CAT System that are managed or provided by external organizations, contractors, or other sources that the Plan Processor or the Participants may determine that it is necessary to engage to perform functions related to the implementation, operation, or maintenance of the CAT. . . . The proposed amendments would . . .. explicitly require that external parties be subject to the CISP if they are providing or managing information or information systems that are within the CAT System. Finally, the proposed amendments would explicitly state that the CISP includes the controls, policies, and procedures required by NIST SP 800– 53, including organizational-level controls.[100]

The Commission appears to be unaware of the fundamental difference between the existing CAT NMS Plan and the proposed provisions. The Proposal describes the existing reference to the NIST Framework as requiring "that NIST SP 800–53 must be followed as part of a comprehensive security plan applying to all components of the CAT System implemented by the Plan Processor."[101] This description fails to recognize that the relevant section of the CAT NMS Plan explicitly allows for flexibility.[102]

The proposal to incorporate the specific requirement for NIST SP-800-53 into the CAT NMS Plan[103] reflects an assumption that the NIST SP-800-53 will always exist and will always be applicable in this context. The Commission fails to recognize that, over time, standards change and, in some cases, disappear. Unlike the reference to the NIST Framework in the current CAT NMS Plan, the proposed amendments would not allow the Operating Committee to call on its experience and expertise, or the experience and expertise of the CISO or CCO, to determine how the SROs should comply with the requirements to which they are subject. Rather, the Commission

---

99 Proposal, at 65992; see also id., at 66096.

100 Id., at 65992-65993. The term "NIST SP 800–53" appears 68 times in the Proposal, indicating the level of specificity it enters into.

101 Id., at 65993.

102 See Appendix D, Section 4.2 of the CAT NMS Plan.

103 See Proposal, at 66096 (proposed definition of "Comprehensive Information Security Program") and 66099-66100 (proposed Section 6.13(a) and (d)).

proposes to freeze the current standards in place, irrespective of whatever issues or risk that step creates.

It is worth noting that the introduction of NIST SP-800-53 requirements could impact which subcontractors and providers SROs or the Plan Processor may use. The current NIST SP-800-53 requirement for the Plan Processor includes Control Family "SA" (System and Services Acquisition) ("SA"). The Proposal would override that by requiring NIST SP-800-53 for vendors. Effectively, it would replace a control family with a single, prescriptive approach. As a result, vendors, including potentially the Plan Processor, would not be available if they would be well covered by SA but are not willing to meet the requirements of NIST SP-800-53. Similarly, an existing vendor may seek to evolve security beyond the prescribed NIST standards, but the Plan Processor and the SROs would not be able to allow a change, at least not without seeking approval by the Commission of a Plan amendment. Accordingly, this proposed requirement could force the Plan Processor to use a less effective vendor, pay more for services, or abandon an existing vendor.

The NIST SP-800-53 information security program would be required "to be applied to information systems within the CAT System that are managed or provided by external organizations, contractors, or other sources that the Plan Processor or the SROs may determine" are necessary.[104] The Proposal suggests that NIST SP 800–53 apply to personnel and information systems that support the CAT System:

> The CAT NMS Plan's inclusion of NIST SP 800–53 as a relevant industry standard that must be followed to manage data security for information systems therefore requires that the Plan Processor apply its information security program at an organizational level, and not just to the Central Repository. The Commission preliminarily believes the proposed amendments to define the CISP and other corresponding changes should therefore clearly require the information security program to apply to personnel and information systems that support the CAT System.[105]

As noted above, the central repository of the CAT is currently hosted in an AWS cloud environment. The Amazon staff operating the data centers housing CAT systems or monitoring networks used by CAT could be considered "personnel . . . that support the CAT system," in which case the provision would apply to them. It is not clear whether the requirement would extend to, for example, HVAC, fire suppression, and other data center maintenance personnel. Thus, the Proposal on its face would prohibit the use of AWS if it refused to apply NIST SP 800–53 to such personnel. Alternatively, the cost of the AWS services might increase, especially if no other host were willing to apply the standard. It is not clear that the Commission understands the impact that the change from allowing a more flexible security framework to prescriptive standards would bring.[106]

---

104 Id., at 65993.

105 Id., at 65992.

106 The Commission seems to have ignored the use of FedRAMP guidance and authorization for cloud service providers such as AWS, adding complication on how to properly apply NIST SP 800-53. See FedRAMP "moderate" controls at https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Controls_Baseline.xlsx.

b. Role Based Access Control

The Proposal would mandate the use of Role Based Access Control ("RBAC"), which is "a mechanism for authentication in which users are assigned to one or many roles, and each role is assigned a defined set of permissions."[107] RBAC is already covered in relevant policies and applied in practice. Moreover, mandating its use through codifying it in the CAT NMS Plan would not allow for the implementation of the more effective or secure controls that might emerge as technology and best practices evolve. In particular, the Proposal would limit the use of complementary, hybrid, or alternative controls such as access control lists, attribute-based control lists, mandatory access controls, or discretionary access controls. Not only would the Commission's proposed RBAC requirement be redundant with NIST SP 800-53 control AC-3(7), but it would not allow for improvement if NIST SP 800-53 controls for access control or other practices evolved over time and in fact could become inconsistent with NIST SP 800-53.[108] The Commission has not explained why the current requirements are no longer sufficient

c. Private Lines

Another example of the Commission's imbedding a specific practice in the CAT NMS Plan is the proposal that SROs only connect to CAT infrastructure using private lines. The Proposal states that

> [t]he Commission preliminarily believes that this practice is warranted because public lines are shared with other users, including non-Participants, and usage of public lines could result in increased cybersecurity risks because traffic could be intercepted or monitored by other users. Private lines, managed by Participants themselves, could provide more robust and reliable connectivity to CAT infrastructure because such lines would not be shared with other users and could be tailored to bandwidth and stability requirements appropriate for connecting to CAT infrastructure.[109]

Despite its surface appeal, this approach ignores that private lines are not the only options that would address the Commission's stated goals. Connectivity standards such as TLS 1.2 and later are secure from a monitoring and interception standpoint, as evidenced by their use in e-commerce transactions, individual transactions via banking portals, and by the Commission itself, in accepting EDGAR submissions.[110] Private lines carry a high cost and encrypted data sent over non-private lines provide industry-standard security. The Proposal does not seem to have considered this or other options, or even identified a problem with the current structure.

In fact, the private line argument is based in part on false assumptions and would add needless complexity. A limited number of private lines could actually provide less reliable connectivity, due to

---

[107] Appendix C to the CAT NMS Plan, at note 249.

[108] **In addition, the Proposal would revise the already detailed requirements for implementation of the system to** create Customer-IDs and add the requirements for the Programmatic CCID Subsystem. See Proposal, at 66018-66020 and 66104-66105.

[109] Proposal, at 66048. See also id., at 66100 (proposed Section 4.1.1).

[110] See *EDGAR Release 20.1 Software Upgrade* (January 24, 2020), available at https://www.sec.gov/oit/edgar-release-201-software-upgrade.

the reduced ability to reroute traffic around issues in a secure fashion.[111] The existing CAT NMS Plan makes it clear that the SROs and Industry Members are responsible for ensuring submissions are made in a timely manner and to make technical arrangements to meet their obligations.[112] The NYSE believes that it makes more sense to continue to allow the SROs to determine how to meet their obligations while complying with existing security standards than to codify a particular connectivity method, especially one that may be flawed or may in the future be considered less secure.

Similarly, the Proposal suggests relying on private lines for machine-to-machine interfaces, which interfaces the NYSE expects most SROs will need to conduct surveillance. The Proposal states that the Commission "preliminarily believes that all machine-to-machine interfaces, which facilitate the automated transfer of potentially large amounts of data, should only occur on private lines instead of public lines, and that it is only appropriate for public lines to be used for manual web-based submissions on an encrypted Virtual Private Network."[113] In so stating, the Proposal does not adequately consider that the key consideration in securing the CAT from a confidentiality perspective is not machine-to-machine vs. manual, but whether or not an interface supports entering data vs. retrieving it. The Proposal apparently ignores that virtual private network ("VPN") connections offer a similar level of confidentiality and integrity to private lines, while potentially offering greater availability due to the ability to securely use a diversity of routes.

Once again, the NYSE believes that it is would be better for the SROs to determine how best to meet their obligations in compliance with the security requirements of the current CAT NMS Plan, than to codify a particular connectivity method. In following the latter path, the Proposal runs the danger of creating a CAT NMS Plan that is more rigid and, ultimately, less able to maintain the security and confidentiality of the CAT Data as technology evolves and security best practices change.

d. Geographic Limitations

In another example of prescriptive requirements without considering the resulting risks, the Proposal would create geographic limitations on connecting to CAT infrastructure. Specifically, the Proposal would amend the CAT NMS Plan to

> require that for all connections to CAT infrastructure, the Plan Processor must implement capabilities to allow access (*i.e.*, "allow list") only to those countries where CAT reporting or regulatory use is both necessary and expected. In addition, proposed Appendix D, Section 4.1.1 would require, where possible, more granular "allow listing" to be implemented (e.g., by IP address). Lastly, the Plan Processor would be required to establish policies and procedures to allow access if the source location for a particular instance of access cannot be determined technologically. The Commission preliminarily believes that while this control

---

111 Any failure that occurs on a private line prevents all data traffic along that line from re-routing because it is a point-to-point connection. An entity could re-route traffic down a secondary private line or backup to an encrypted non-private line connection. Either would help ameliorate any issue, and the Commission should evaluate the costs of each option and how each could impact the benefits derived from the system.

112 See CAT NMS Plan, Section 6.5(d)(ii), and Appendix C, p. C-21.

113 Proposal, at 66048.

> will not eliminate threats pertaining to potential unauthorized access to the CAT system, this proposed requirement would enhance the security of CAT infrastructure and connections to the CAT infrastructure.[114]

The proposed change would create practical and logistical problems for the SROs, given not just that many of the SROs are part of multinational entities, but also that their employees must sometimes travel. An SRO might need emergency support from a staff member that is temporarily in a different country that does not meet the "necessary and expected" criteria. If a staff member's non-emergency support is needed unexpectedly, whether or not the SRO may access that support might depend on where the staff member is located. The Proposal does not seem to have considered these issues or identified a problem with the current structure. Further, the Commission's Proposal does not evidence having considered alternative approaches for addressing the problem the Commission is attempting to resolve with this restriction.

5. The Required Security Working Group Would Not Improve Security.

Though not specifically required under the CAT NMS Plan, the Operating Committee has established a security working group that is involved in implementing the current CAT system requirements—the ESWG.[115] The ESWG provides recommendations to the Operating Committee, which has the overall responsibility for the security of the CAT.[116] The Proposal would mandate that the Operating Committee establish and maintain a new security working group meeting specific requirements (the "SWG").[117] The Proposal does not adequately address why the Commission proposes requirements for the SWG that are different from the ESWG, why designated personnel of the SROs would be required members of the SWG, or the risks that the requirement would create. Further, the Proposal does not adequately address why the ESWG is inadequate, or why the CAT NMS Plan should require the SWG instead of the ESWG or some other model. Finally, for the reasons set forth below, the NYSE believes that replacing the ESWG with the SWG would result in a net loss in security.

Unlike now, the proposed amendments would mandate whom the SROs may appoint as members of the SWG. Rather than rely on the SROs' expertise to determine who is most appropriate to monitor security, the Proposal would require the SWG consist of each SRO CISO or the SRO's deputy chief information security officer. As a result, several contributing members to the ESWG may not be able to continue as members of the SWG, and new members who have not been significantly involved with the CAT previously could be required to participate on the SWG. The

---

[114] Id. The Proposal also states that, because it may not always be possible to detect the location of a CAT Reporter or Regulatory Staff, "there is a potential for malicious spoofing of location or IP addresses." Id., at 66049. The NYSE believes that with respect to the CAT the "malicious spoofing of location or IP addresses" is so trivial that even a low cost of implementation does not meet a cost-benefit threshold.

[115] Id., at 65994.

[116] The SROs participate in the Operating Committee, which is responsible for, among other things, designating individuals and entities to ensure compliance with Rule 613 and the CAT NMS Plan. See CAT NMS Plan, Sections 4.1 and 4.2.

[117] Proposal, at 65993.

likely net result would be to undermine the effectiveness of the proposed SWG and the Operating Committee.

The Proposal posits that the SWG should be made up of the SRO CISOs or their deputies because they "are the parties that are most likely to have general expertise with assessing organizational-level security issues for complex information systems."[118] In the NYSE Exchanges' experience, this is both incorrect and the wrong criteria to apply. A review of the proposed purpose of the SWG reinforces that conclusion.[119] Simply put, the SRO CISOs and their deputies are too senior to be the best people to appoint to the proposed SWG.

Staff authorized by the SRO Operating Committee members to participate in the ESWG have historically engaged at a level that allows them to effectively monitor and provide advice regarding the security of the CAT. They have the availability and detailed knowledge required to evaluate potential risks to the CAT, assess security design, review new and emerging challenges in the security industry, and bring perspective from their own organization's experiences to bear. They have been involved in lengthy, detailed reviews of all aspects of the CAT's security, from control reviews and threat assessments to technology implementations, and have responded to myriad requests and questions from Commission staff, well beyond typical security implementations. When the ESWG needs input from individuals with more general expertise in order to meet its obligations, it requests outside input from industry CISOs, technology experts, and others. The expertise of system architects and risk and audit staff that also deal with organizational-level security issues for complex information systems for their SROs have augmented the ESWG in critical ways.

By contrast, an SRO CISO is likely to have a large purview that includes all the systems, processes, and practices at the relevant SRO, not just regulatory systems and the CAT, and his or her deputy's responsibilities are likely to be similar. These individuals may be responsible not just for the SRO, but also for entire conglomerates made up of domestic and international entities, with all their diverse security requirements. Such individuals would not have the availability or specific technical knowledge required to meet the purpose of the SWG, much less comply with obligations such as reviewing the application materials of an SRO seeking an exemption from the SAW usage requirements.[120] Requiring that they be the SWG members would significantly undermine the security of the CAT, as it would reduce the variety of opinion and feedback that SRO security staff currently provide and potentially reduce the level of engagement SROs are currently providing. The members of the SWG would presumably be able to bring in more technical personnel to advise them, including the individuals currently on the ESWG. But getting advice from them would not be the same as making the individuals with the technical knowledge the decisionmakers.

---

[118] Id., at 65994.

[119] Id., at 65993-65994 ("The proposed amendments would specify that the purpose of the Security Working Group shall be to advise the CISO and the Operating Committee, including with respect to issues involving: (1) Information technology matters that pertain to the development of the CAT System; (2) the development, maintenance, and application of the CISP; (3) the review and application of the confidentiality policies required by proposed Section 6.5(g); (4) the review and analysis of third party risk assessments conducted pursuant to Section 5.3 of Appendix D, including the review and analysis of results and corrective actions arising from such assessments; and (5) emerging cybersecurity topics.").

[120] Id., at note 38.

Ultimately, if adopted, the Proposal would create the risk that the SWG would lose the people with the most relevant managerial and security expertise, CAT context, and ability to keep up with frequent demands of the group, increasing the risk that the SWG would not be effective in its important role. The Commission has not adequately considered this issue, nor has it sufficiently explained why other alternatives are inadequate to achieve its goals. The current structure of the ESWG, which allows each SRO to appoint the individuals with the requisite expertise, understanding of CAT, and familiarity with the CAT project irrespective of their titles, is an alternative that the Proposal does not adequately assess. It is not clear why the Commission is seeking to change the current structure.

As proposed, the SWG would be made up of senior representatives of all the SROs—companies that compete with one another in several markets. Moreover, the CISO would be required "to apprise the Security Working Group of relevant developments and to provide the Security Working Group with all information and materials necessary to fulfill its purpose."[121] Such information could include competitively sensitive information, such as reviewing reports of a particular SRO's security vulnerabilities that have not been remediated. The Proposal would reduce the SWG's ability to limit the audience for highly sensitive discussions, as it does not adequately consider the need for subcommittees or other smaller-audience structures within the SWG for sensitive discussions.[122] In other words, the Proposal mandates that the entire SWG, and so representatives of every competitor, receives all materials, irrespective of their sensitivity or competitive impact.

6. The Proposed Programmatic Access Would Increase the Potential Consequences of Access to the CCID.

The Proposal would establish in the CAT NMS Plan the circumstances and requirements for Programmatic CCID Subsystem Access. Such access "would allow Regulatory Staff to submit multiple ITIN(s)/SSN(s)/EIN(s) of a Customer(s) of interest identified through regulatory efforts outside of CAT to obtain Customer-ID(s) in order to query CAT Data regarding such Customer(s)."[123] The Plan Processor would be required to provide Programmatic CCID Subsystem Access, and Performance Requirements for the conversion of ITIN(s)/SSN(s)/EIN(s) to Customer-ID(s) would be required to be consistent with the criteria set out in Appendix D of the proposed CAT NMS Plan.[124] The Proposal states why the Commission believes such access is merited:

> [t]he Commission believes that it is appropriate to provide for Programmatic CCID Subsystem Access because such access would facilitate the ability of Regulatory Staff, who may be in possession of the ITIN(s)/SSN(s)/EIN(s) of multiple Customers as a result of their regulatory efforts outside of the CAT, to obtain the Customer-IDs of such Customers and

---

121 Id., at 65994.

122 In addition, in the NYSE Exchanges' experience, smaller groups would also increase the efficiency of the SWG as reviews, advisement, and decisions often occur quicker in smaller, more focused groups.

123 Id., at note 195. This aspect of the Proposal would allow SROs to further enrich data stored in the SAWs, which would at the same time increase the attractiveness of data in the SAWs to bad actors.

124 Id., at 66036.

> query CAT Data, including Customer and Account Attributes and CAT transactional data using an application that accommodates the input of multiple ITIN(s)/SSN(s)/ EIN(s). [125]

The Proposal does not recognize the risk such a requirement would create. Briefly put, the proposed programmatic access would greatly increase the capability of anyone that gains access to the CCID to query large quantities of ITIN(s)/SSN(s)/EIN(s) to create a mapping of ITIN(s)/SSN(s)/EIN(s) to CCIDs. In this manner, the Proposal has the potential to greatly reduce the security of the Customer and Account Information System by providing a means for the creation of cross-references in order to make it easier for regulators to use.[126]

It is not clear why the Commission has elected to change the system of maintaining separate databases with personal identities separate from transactional data to one in which a single data set would be created within the CAT perimeter that houses transactional data with data that could reveal the identities of individual account holders. NYSE believes this is fundamentally contrary to the Proposal's stated goal of increasing security of information in the CAT and inconsistent with its exemption from reporting certain PII to the CAT, which the Commission proposes to incorporate as an amendment to the CAT NMS Plan.[127]

7. Security Requirements Should Apply to Commission and its Staff.

The Proposal spans 116 pages of the Federal Register. Of that material, only one page is dedicated to the application of the Proposal to Commission staff.[128] That page states that, because the Commission is not a party to the CAT NMS Plan, regulates the SROs, and oversees and enforces their compliance with the CAT NMS Plan,

> [t]o impose obligations on the Commission under the CAT NMS Plan would invert this structure, raising questions about the Participants monitoring their own regulator's compliance with the CAT NMS Plan. Accordingly, the Commission does not believe that it is appropriate for its security and confidentiality obligations, or those of its personnel, to be reflected through CAT NMS Plan provisions.[129]

The Commission instead asserts that it "will ensure that its policies and procedures impose protections upon itself and its personnel that are comparable to those required under the proposed

---

125 Id., at 66036.

126 The proposed requirements for the Programmatic CCID Subsystem are another example of the Proposal introducing a level of specificity into the CAT NMS Plan that creates rigidity. The Proposal does not adequately address why the current requirements, which would leave the specifics to the ESWG and Operating Committee, is inadequate. Additionally, the Proposal does not sufficiently consider several design concerns that it would introduce. The addition of a high-speed API potentially changes design assumptions about the ability to create a mapping of ITIN(s)/SSN(s)/EIN(s) to CCIDs, but the Proposal does not require a fresh review of the design.

127 See 85 FR 16152, supra note 58. The Proposal would amend the CAT Plan to incorporate the substance of this exemption. See Proposal, at 66084.

128 Id., at 66053-66054.

129 Id., at 66053. The Proposal does not recognize the irony of it mandating the Plan Processor, a vendor hired by the SROs, to monitor the same regulated entities' compliance with the CAT NMS Plan.

provisions in the CAT NMS Plan from which the Commission and its personnel are excluded, which includes reviewing and updating, as necessary, existing confidentiality and data use policies and procedures."[130]

Notably absent from this vague promise is any statement that the Commission staff will be subject to using a structure similar to the SAW described in the Proposal, or that Commission staff will be subject to limitations on their ability to download CAT data into local systems.[131] It is unclear why such different standards may apply to this subset of CAT Data users and likewise unclear how this inconsistent treatment would serve the goals the Proposal is purportedly designed to achieve.

If Commission users are governed by less rigorous standards than the SROs, any proposed changes would provide no meaningful security benefits. Security frameworks are only as strong as their weakest link, such that a lapse by even a single, less-vigilant regulatory user would render the security efforts of other regulatory users almost meaningless. The Commission cannot justify the imposition of significant costs on the SROs to purportedly improve the security of information in the CAT, while at the same time creating a gap that would render those changes pointless by exempting the Commission staff from its requirements. Concerns about risks related to proliferation of CAT Data, local security, and bad actors having access to CAT Data would persist, yet the Commission has failed to explain why it believes its arrangement would achieve its goal of increasing CAT Data security or would help to address the problem that the Commission is seeking to resolve. The Commission should therefore be required to meet the same security- and data-access standards as the SROs or explain which security and access requirements of the CAT NMS Plan with which its staff will not be required to comply, and why not.

B. The Proposal Would Fundamentally Alter the Cost/Benefit Justification for Developing the CAT.

1. The Proposed Changes Would Make It Difficult or Impossible for SROs to Use the CAT Internally to Carry Out Their Regulatory Functions.

Every national securities exchange is a regulator. Indeed, requiring that every national securities exchange regulate its members is a fundamental building block of the U.S. securities markets. As set forth in the Exchange Act, each national securities market must have the capacity to "enforce compliance by its members and persons associated with its members, with the provisions of [the Act], the rules and regulations thereunder, and the rules of the exchange."[132] In addition, each exchange must enforce compliance with such provisions by its members and persons associated with its members.[133] The Exchange Act does not dictate how the national securities markets must comply with these regulatory obligations. Instead, Commission staff conduct inspections and

---

130 Id., at 66053.

131 The NYSE notes that the existing requirement for the API to meet the Appendix D performance criteria of one million queries in three hours coupled with the Commission being broadly exempted from the limits placed on the SROs indicates that the security in the subsystem's use of an HSM may be diluted by a large number of ITIN(s)/SSN(s)/EIN(s) to CCID mappings existing in Commission systems.

132 15 USC 78f(b)(1).

133 15 USC 78s.

investigations of the national securities exchanges to help ensure that they fulfill the cited obligations under the Exchange Act and related regulatory obligations.

From the start, the CAT was designed to be a tool to help the national securities exchanges and other regulators comply with their mandate to oversee their markets. Originally created pursuant to Rule 613, the CAT's purpose with respect to regulation is clear: regulators must have access to the CAT and all data reported to it in order to perform their regulatory responsibilities. As Rule 613 requires,

> [e]ach national securities exchange, national securities association, and the Commission shall have access to the central repository, including all systems operated by the central repository, and access to and use of the data reported to and consolidated by the central repository under paragraph (c) of this section, for the purpose of performing its respective regulatory and oversight responsibilities pursuant to the federal securities laws, rules, and regulations.[134]

Pursuant to Rule 613, not only does the CAT NMS Plan have to allow the SROs access to the data, but that *access shall not be limited.*

> The national market system plan submitted pursuant to this section shall provide that such access to and use of such data by each national securities exchange, national securities association, and the Commission for the purpose of performing its regulatory and oversight responsibilities pursuant to the federal securities laws, rules, and regulations shall not be limited.[135]

Consistent with Rule 613, the current CAT NMS Plan requires that the SROs use the CAT. Further, it requires that the SROs ensure they have the tools to make use of the CAT, as each SRO must "develop and implement a surveillance system, or enhance existing surveillance systems, reasonably designed to make use of the consolidated information contained in the Central Repository.[136]

In the Proposal the Commission gives a nod to Rule 613,[137] but then goes on to ignore its requirements while proposing restrictions contrary to the purpose of the CAT and Rule 613.[138] That issue is clearly reflected in the Proposal's statement that "[t]he Commission continues to believe that regulators must be permitted to access and extract CAT Data when such access and extraction is for surveillance and regulatory purposes, *but only as long as such access and*

---

134 17 CFR 242.613(e)(2).

135 Id.

136 CAT NMS Plan, Section 6.10(a). See also id., at Section 6.7.

137 See Proposal, at 65991 (noting that the goal of Rule 613 "was to create a modernized audit trail system that would provide regulators with more timely access to a sufficiently comprehensive set of trading data, thus enabling regulators to more efficiently and effectively reconstruct market events, monitor market behavior, and investigate misconduct.").

138 See CAT NMS Plan Approval Order, supra note 2, at 84829. See generally id., at 84816-84897.

extraction does not compromise the security of CAT Data."[139] The italicized text is not grounded in Rule 613 or the Exchange Act. As with the Proposal as a whole, this clause would introduce new limitations on the SROs' ability to access CAT Data and use it for regulatory purposes—limitations that are contrary to Rule 613's mandate that the SROs' ability to use CAT data "shall not be limited."[140] The Proposal would thus materially alter the benefits generated by the CAT. The Commission has not adequately explained its rationale for implementing this change.

In its original order approving the CAT NMS Plan, the Commission stated that data available to regulators would benefit from, among other things, completeness, accuracy, accessibility, and timeliness.[141] Regulators' ability to conduct surveillance, investigations, examinations, analysis and reconstruction of market events, and analysis in support of rulemaking initiatives all benefit from the improved data quality as part of CAT.[142] As detailed below, each of these benefits is undermined by the Proposal's added restrictions. The Commission has not adequately analyzed those effects, evaluated whether the new requirements are necessary, or studied how they would affect the goals originally outlined when the Commission proposed and then adopted Rule 613.[143]

The Proposal acknowledges that "Participants are likely to see reductions in the efficiency with which they perform their regulatory duties…."[144] Yet the Commission does not reasonably consider that the Proposal would put serious limitations on the SROs' ability to access CAT Data and use it to regulate—limitations that are inconsistent with the requirements of the Exchange Act and Rule 613, and undermine the very purpose of developing the CAT in the first place.[145] In short, the Proposal would fundamentally shift the purpose, utility, and cost of the CAT with the purported goal of improving security, but without adequately identifying specific security problems that could not be addressed within the existing CAT security framework and requirements of the CAT NMS Plan.

Based on the NYSE Exchanges' experience insourcing a substantial portion of their regulatory program in recent years, being closer to the markets results in more effective and efficient regulation. The Proposal could significantly impair the NYSE Exchanges' ability to further evolve regulatory oversight of its member firms.

---

139 Proposal, at 65997-65998 (emphasis added).

140 17 CFR 242.613(e)(2). The NYSE notes that Rule 613 does not provide that (a) access to the CAT may be unequal among regulators, (b) third parties, like the Plan Processor, may be used to determine SROs' access and monitor use, or (c) the Plan Processor, because of the requirements described in the Proposal, should mandate that SROs must use its hosting platforms to conduct non-CAT surveillance and analyses.

141 See CAT NMS Plan Approval Order, supra note 2, at 84727. See also Rule 613 Adoption Release, supra note 4, at 45777-45780.

142 See CAT NMS Plan Approval Order, supra note 2, at note 586.

143 See Rule 613 Adoption Release, supra note 4, and 77 FR 32556, supra note 22.

144 Proposal, at 66092.

145 See CAT NMS Plan, at Appendix C, Section 2(b) ("The utility of the Central Repository is dependent on regulators being able to have access to data for use in market reconstruction, market analysis, surveillance and investigations").

The below delineates the specific ways in which the Proposal would make it difficult or impossible for SROs to use the CAT to carry out their regulatory functions.

a. Mandated Use of SAWs

Proposed Section 6.13 would require SROs to use SAWs established by the Plan Processor as the "only means of accessing and analyzing customer and account data."[146] No matter what their preference, if the Proposal were approved, SROs would have to use a SAW built, controlled and monitored by the Plan Processor in order to comply with their regulatory obligations.[147] In addition to leading to the various risks discussed in Part I.A above, the mandate to use SAWs and the impediments to accessing CAT Data that the SAWs would introduce would have a significant impact on the SROs' ability to use CAT Data in their regulatory programs as required by Rule 613. Investigations and disciplinary matters would be delayed.

The SAW requirement would diminish an SRO's ability to efficiently and appropriately refer matters to other SROs for further investigation. Particularly in complex manipulation matters, curtailed or impeded access to CAT Data would make it more difficult to identify problematic cross-market trading and determine whether it does or does not implicate a particular SRO.

In addition to the impact on SROs, the SAW requirement would indirectly increase the regulatory obligations faced by industry members by decreasing the effectiveness and efficiency of certain surveillances used to monitor practices like wash trading on the NYSE Exchanges. CAT Data could be used to systematically identify false positive alerts and obviate the need for an SRO to follow up with industry members to obtain additional information about them. However, the SAW requirement would frustrate those efforts, leaving firms to respond to information requests that might have been avoided if CAT Data were more easily accessible. The net result would be contrary to one of the original benefits of CAT that the Commission identified when it adopted Rule 613, to reduce regulatory obligations and burdens for industry members.[148]

One example of a strong regulatory structure would be to initiate an inquiry in a SAW but export data to apply surveillance logic and review alerts and supporting data to a separate regulatory environment for investigation. With that structure, a regulator would be able to capitalize on the existing, tailored surveillance program and the in-house expertise in working with it, but still draw on the resources that the CAT could provide.[149] The Proposal, however, would not permit this

---

146 Proposal, at 65998.

147 Because of the limitations and costs associated with using the SAWS, NYSE believes that the Proposal would effectively force SROs to contract out their regulatory programs. The Commission has not analyzed or considered this goal. See Part IV, below.

148 See Rule 613 Adoption Release, supra note 4, at 45756 (Explaining that data made available to regulators in CAT would "make regulatory inquiries and investigations more efficient by eliminating delays resulting from the current need to send information requests to individual market participants in search of key information, as well as reducing the burden on regulators and market participants of such requests").

149 Using the SAW as imagined in the Proposal would require more regulators in the SAW and many more person-hours spent in the SAW than if surveillance output and supporting data could be more easily exported into another secure environment.

option as a practical matter because of the Proposal's requirements for Non-SAW environments and limitations on exporting CAT Data.[150]

The Commission may point to the possibility for an SRO to use a Non-SAW environment as an alternative. However, the requirements that an SRO must meet before being granted permission to use a Non-SAW environment raise their own additional security risks and impose burdens that mean that an SRO that took its security obligations seriously, including its obligations to maintain confidentiality for its security program, would almost certainly conclude that using its own environment, i.e., a Non-SAW environment, is not a realistically viable option due to the Proposal's requirements. Ultimately, because of the risks and costs associated with an SRO using a Non-SAW environment, it is unlikely that any SRO would elect to conduct regulatory programs using CAT Data outside of a Plan Processor designed SAW. The choice that the Commission is presenting between a SAW and Non-SAW is accordingly a false one. To the extent that the SRO wished to maintain an in-house regulatory program to oversee its markets, an SRO would effectively be forced to use the Plan Processor-provided SAW to avoid the serious security and competitive risks created by the proposed Section 6.13(d) provisions, and would have to subject itself to oversight by its vendor the Plan Processor within the SAW environment.

The requirements giving rise to the risks and costs are discussed in turn below.

First, in order to apply for an exception, an SRO would be required to divulge sensitive security program design and operational information not just to the Commission, but also to the CISO, the CCO, and the members of the SWG and their designees.[151] The information would include detailed discussion of security and privacy controls and design specifications:

> A security assessment of the non-SAW environment . . . by a named, independent third party security assessor, that: (a) demonstrates the extent to which the non-SAW environment complies with the NIST SP 800–53 security controls and associated policies and procedures . . . ., (b) explains whether and how the Participant's security and privacy controls mitigate the risks associated with extracting CAT Data to the non-SAW environment through user-defined direct query or bulk extract tools . . . and . . . Detailed design specifications for the non-SAW environment demonstrating: (a) the extent to which the non-SAW environment's design specifications adhere to the design specifications developed by the Plan Processor for SAWs pursuant to Section 6.13(b)(i), and (b) that the design specifications will enable the operational requirements set forth for non-SAW environments in Section 6.13(d)(iii).[152]

No reasonable entity that worked with data and data systems would be willing to disclose such detailed security standards, systems, or policies and procedures to third parties other than their regulator, because doing so would potentially expose it to breach vulnerabilities. Any entity, including SROs applying for a SAW environment exemption, would assess the increased security risks, including the risks of breach, exposure, and insider threat, created by such disclosure, and

---

150 For further discussion of possible alternatives, including reliance on existing requirements, see Part III, below.

151 See Proposal, at 66099 (proposed Section 6.13(d)(i)(A)).

152 Id.

would be unlikely to pursue the exemption because of the risk created by the disclosure of internal security systems.

Second, if the CISO and CCO granted an exception after their review of the materials, the SRO would have to provide the same group with updated information annually, and notify them of any material change to the security controls.[153] To do so would mean that every year, or whenever it made material changes to its own system or security policies and procedures, the SRO would have to expose itself anew to the security risk created by its initial application for an exception. As a result, using a Non-SAW environment would not be a realistic option for SROs who do not wish to reveal such proprietary and confidential information to a third party.

The Proposal would go even further, requiring that an SRO open its own security perimeter in an unprecedented manner to allow the Plan Processor to monitor the Non-SAW environment for compliance with the vendor-created design specifications.[154] Proposed Section 6.13(d) would require that the Plan Processor and third party security assessor have access to detailed system design specifications, security protocols, and other information required by the Plan Processor to review any proposed Non-SAW environment.[155] That section also would require the Plan Processor to monitor the Non-SAW, and does not limit the scope or granularity of that within-SRO monitoring or review by the Plan Processor.[156] Nor does proposed Section 6.13(d) adequately contemplate whether the monitoring is even feasible, a valid question given that generally an SRO's regulatory system has customized, often proprietary monitoring systems. It is unlikely that an SRO would allow any vendor to monitor an environment within the SRO itself, much less a vendor that is a subsidiary of a competitor and not itself subject to the CAT NMS Plan, given the risks associated with allowing third parties access to security protocols and systems.

Third, many SROs are part of larger, sometimes multinational enterprises. Such entities are likely to have enterprise-wide risk management policies already in place, a fact that the Proposal does not take into account. As a practical matter, an SRO cannot supersede enterprise-wide risk policies for the comfort or efficiency of one technology vendor. Having portions of the organization subject to the security protocols of its parent company, while others have different, CAT NMS Plan-mandated standards creates risks and increases costs by introducing duplicative, overlapping, and possibly conflicting security policies and procedures within the organization.

b. Responsibility of the Plan Processor

The Proposal would purport to charge the Plan Processor with substantial new responsibilities and authority.[157] Not only does the Commission propose to require the Plan Processor to develop and maintain "detailed design specifications for the technical implementation of the access, monitoring,

---

153 See id., at 66099 (proposed Section 6.13(d)(ii)(A)); and 66100 (proposed Section 6.13(d)(iii)(C)). The NYSE Exchanges do not provide such granular detail to any party other than the Commission, let alone to other SROs or to technology vendors providing a service.

154 See id., at 66099 (proposed Section 6.13(d)(iii)(B)).

155 See id. (proposed Section 6.13(d)(i)(A)).

156 See id., at 66100 (proposed Section 6.13(d)(iii)(B)).

157 For the proposed requirements for the Plan Processor, see note 17, supra, and Part I.B.1.a, infra.

and other controls required for SAWs by the Comprehensive Information Security Program controls,"[158] but the Plan Processor would also be the gatekeeper to determine whether an SRO has met the proposed requirements to use the CAT.[159] In addition, the Plan Processor would monitor each SAW for compliance with the CISP and design specifications, notifying the SRO of any identified non-compliance.[160] As a result, the Proposal places the Plan Processor—a vendor to the SROs—in a position to essentially dictate the form and structure of how the SROs meet their regulatory requirements under the Exchange Act, including the context and terms under which they could access CAT Data and, through their migration to the CAT, other data and regulatory surveillances.

The Commission does not adequately identify why a vendor like the Plan Processor would be the best entity to conduct regulatory assessments and monitoring, and likewise fails to establish that the Plan Processor is better situated than each SRO to determine the SRO's compliance by monitoring its analytic environments or the regulatory systems that the Proposal requires be brought into the SAWs.

Further, the Proposal does not adequately consider whether the Plan Processor could meet the new requirements described in the Proposal, whether the Plan Processor would agree to revising the Plan Processor Agreement to perform and accept the potential risk associated with the new responsibilities, or what the regulatory oversight mechanism might be to ensure that the Plan Processor adheres to the requirements. At a minimum, the Proposal will require a renegotiation of the Plan Processor Agreement with the current Plan Processor, or a search for a new Plan Processor if the current Plan Processor is unable or unwilling to perform the proposed functions and accept the proposed responsibilities.

In fact, the Commission has not considered whether there is any vendor able to perform the proposed requirements and, if not, that it would impossible for the SROs to meet their obligations under Commission rules.[161] Given the scope of these proposed new functions and responsibilities, the costs borne by the SROs to retain a Plan Processor will be much greater than those currently today.[162]

One justification the Commission gives for purporting to vest oversight authority and responsibility in the Plan Processor is that it believes "the Plan Processor would have the most information regarding the security requirements that are applicable to SAWs."[163] This misunderstands how the SAWs would work. Once an SRO's data and proprietary systems are added to its SAW, the Plan Processor would not have as much information as the SRO itself regarding the SAW's security. Moreover, the Plan Processor is unlikely to have the relevant information about all the tools that an SRO would need to use in its SAW, particularly bespoke tools.

---

158 Proposal, at 66099 (proposed Section 6.13(b)(i)).

159 Id. (proposed Section 6.13(b)(ii)).

160 Id. (proposed Section 6.13(c)(i)).

161 17 CFR 242.608(c). See also Part IV.B, below.

162 See discussion regarding costs in Part I.B.2, above.

163 Proposal, at 66001-66002.

Further, SROs are obligated under Regulation SCI to establish, maintain, and enforce policies reasonably designed to ensure its SCI systems—which would include the SAWs and systems in the SAWS—"have levels of capacity, integrity, resiliency, availability, and security, adequate to maintain" the SRO's "operational capability and promote fair and orderly markets."[164] Thus, the SROs cannot relinquish control of the SAWs to a technology vendor. Unfortunately, the Commission has not considered the conflicts between its Proposal and the SROs' obligations under Regulation SCI.

c. Restrictions on Extracting Data

The Proposal recognizes that despite the proposed mandate to use SAWs,

> it may sometimes be necessary for the Participants to extract CAT Data . . . to external systems or environments, including those beyond the Participants' control. For example, the Participants might need to extract CAT Data to respond to a court order or to some other regulatory or statutory mandate, to submit a matter to a disciplinary action committee, to file a complaint against a broker-dealer, or to refer an investigation or examination to other regulators like the Commission. The Commission does not wish to unnecessarily constrain the Participants in situations like these, where only a targeted, small amount of CAT Data is needed to achieve a specific surveillance or regulatory purpose.[165]

Accordingly, proposed Section 6.13(a) would create a maximum and a minimum threshold for the amount of data that can be extracted from SAWs, as well as mandate a method for doing so.

As discussed below, the limitations imposed by the Proposal would frustrate an SRO's ability to conduct routine cross-market surveillance with CAT Data, because it would place significant limitations on the SRO's abilities to access that data and reasonably query it. More specifically, the constraints introduced by the Proposal, including its inflexible and arbitrary limitations on the size of queries and the permitted size and method of CAT Data export, would make it prohibitively difficult for an SRO to incorporate CAT Data into a comprehensive, systematic surveillance platform. Instead, CAT Data would likely become a bespoke tool relegated for use in one-off queries and investigations, contrary to the Commission's original intent. As a result, any SRO that plans to use unique methods and approaches to conduct surveillance for manipulative and fraudulent trading across multiple markets would be severely limited, and efforts to monitor for misconduct in the US markets would be significantly diminished.

Under the existing CAT NMS Plan, subject to Operating Committee review, the Plan Processor must design an online query tool and define the maximum number of records that can be downloaded via the online-targeted query tool, but if a user has a result set too large to be downloaded via the online-targeted query tool, the Plan Processor must notify the user that it could obtain the full data set using user-defined direct queries ("UDDQ") and bulk extracts.[166] The first

---

[164] 17 CFR 242.1001(a)(1).

[165] Proposal, at 65998.

[166] See NMS CAT Plan, Appendix D, Sections 8.1 and 8.1.1. The effective download limit for the online-targeted query tool is dictated by what is technologically feasible based on the Plan Processor's design. The effective limit may evolve as the technology evolves, but the Plan Processor may not limit the number of records available to a regulator.

proposed constraint would replace this flexible and non-restrictive approach to queries, which is designed to facilitate and support regulatory users' access to CAT data, by limiting the maximum number of records that can be downloaded via the online targeted query tool to 200,000 records per query request and removing the ability to use UDDQ and bulk extracts outside of a SAW or Non-SAW environment.[167] The Proposal does not adequately provide a reasoned explanation for why 200,000 was chosen, as opposed to any other figure, or as opposed to continuing to rely on a case by case judgment—and likewise fails to explain why a limit is required in any case, or how limiting query results would impact the CAT system's ability to achieve its goals, including the goal that the CAT improve regulatory analysis of the U.S. securities markets.[168] Instead, NYSE believes the current security requirements are a sufficient alternative to this proposed limit on record extraction.

Based on NYSE regulatory experience, 200,000 records is wholly inadequate. Some background on the scale of the CAT Data helps to frame the issue. In September 2020, an average of 279 billion records were added to the CAT per day, with a peak of 389 billion records per day that month. On a recent day, 200,000 records represented less than 30 seconds of equity orders on just one exchange. In that context, it is unclear how the small number of 200,000 records could be justified. Almost any market activity or event that required analysis across many securities and many market centers, would require an SRO conducting its regulatory activities to access a significant portion of the relevant day's data. Even assuming that the regulator required just 1% of the day's CAT data in order to begin its analysis, an ability to export 200,000 records when 3 billion are perhaps required would effectively render the CAT system unavailable.

Any absolute number set into stone by including it in the CAT NMS Plan would inevitably become a smaller and smaller portion of CAT Data as the CAT grows, further limiting an SRO's ability to utilize the CAT to regulate effectively. Thus, over time, the net result of this limitation would be to prevent the SROs from extracting CAT Data in any meaningful way.

In a second constraint, proposed Rule 6.13(a) would require that the only mechanism to extract CAT Data from the SAWs would be secure file sharing capability provided by the Plan Processor.[169] The mandated use of only one file transfer protocol would limit an SRO's ability to integrate surveillance and other regulatory output from the SRO's SAW with the SRO's other regulatory systems, despite their comparability to the Plan Processor's security policies and procedures and required compliance with Reg SCI. It is not clear what benefit the Commission believes would be achieved by mandating a single method for data extraction, especially given the Commission's oversight authority over the SROs and ability to request information from them at any time in connection with its oversight. Thus, NYSE does not believe that any marginal benefits of tracking the size and recipients of files through secure file sharing would outweigh the negative impact on regulators' ability to use the CAT effectively.

---

[167] Proposal, at 65999 (proposed section 6.13(a)(i)(B)).

[168] For a discussion of the expected regulatory improvements with a CAT, see Rule 613 Adoption Release, supra note 4, at 45730-45733.

[169] Proposal, at 65998. If the file transfer protocol referred to here is like the one used before the online query tool was available, each output file would be attached to an email and must be retrieved and unlocked via password before it could be used in an SRO's system. That system required manual intervention. It would be inefficient for anything but a handful of files.

Finally, in a third constraint, the Proposal would only permit SROs to extract the minimum amount of CAT Data necessary to achieve a specific surveillance or regulatory purpose.[170] The proposed "requirement would apply to all CAT Data, including transactional data and Customer and Account Attributes, as well as means of access to CAT Data, such as the online targeted query tool or Manual and Programmatic CAIS and/or CCID Subsystem Access."[171] As stated in the Proposal,

> [t]he Commission preliminarily does not believe that such a requirement would impede Participant ability to perform surveillance, investigate potential violations, and bring enforcement cases, because Participant Regulatory Staff can view and analyze CAT Data without extraction, such as through the proposed SAW environments or in the online targeted query tool, and to the extent that any CAT Data must be downloaded this proposed provision would not limit a Participant's ability to download the minimum amount of CAT Data necessary to achieve surveillance or regulatory purposes.[172]

Underlying this statement is an assumption that, "in situations like these, . . . only a targeted, small amount of CAT Data is needed to achieve a specific surveillance or regulatory purpose."[173] Not only does the NYSE disagree with this assumption, the Proposal is silent as to how SROs could show they are extracting only the minimum amount for their regulatory needs. Moreover, the NYSE does not believe that its regulatory obligations should be performed at the minimum level, nor does it believe that an SRO's statutory obligations are conditioned on such moderation and restraint.

Ultimately, the Proposal provides no evidence that the SROs have serious security issues or that SROs security perimeters are lacking. The NYSE believes that the proposed limitations on extracting data would impede regulation without additional benefit for security.

d. Regulatory and Commercial Purposes

If adopted, the Proposal would amend Section 8.1 of Appendix D to provide that the Plan Processor must provide the SROs' regulatory staff with access to CAT Data "only for surveillance and regulatory purposes …."[174] Further, proposed Section 8.1 would provide that SRO regulatory staff accessing the CAT Data

> may not use CAT Data in such cases where use of CAT Data may serve both a surveillance or regulatory purpose, and a commercial purpose. In any case where use of CAT Data may serve both a surveillance or regulatory purpose, and a commercial purpose (e.g., economic analyses or market structure analyses in support of rule filings submitted to the Commission pursuant to Section 19(b) of the Exchange Act), use of CAT Data is not permitted.[175]

---

170 Id., at 65998 and 66040.

171 Id.

172 Id.

173 Id., at 65998.

174 Id., at 66103.

175 Id.

The Commission posits that the proposed limitations "would be consistent with the existing requirement in Rule 613 [of] the CAT NMS Plan that CAT Data must be used for solely regulatory and surveillance purposes."[176]

The NYSE disagrees. Under the current CAT NMS Plan, a regulator could access CAT Data that has both regulatory and commercial uses, so long as the regulator uses the data for regulatory and surveillance purposes. This makes sense: what matters is the actual use of the data, not a theoretical one. As drafted, under the proposed rule, a regulator would not be able to access the same CAT Data, simply because it *could* be used in more than one way, *even if the regulator had no plans to use it for commercial purposes*. Compliance with the proposed rule would be virtually impossible, since the individual regulator may not even be aware that the CAT Data they are accessing could have an additional, commercial purpose.

Ultimately, proposed Section 8.1 would have a substantial effect on the SROs' ability to regulate, since it would needlessly limit regulators' access to CAT Data, even inside a SAW environment, and would reduce the benefits of Rule 613 and the CAT NMS Plan originally contemplated by the Commission.[177] The reality is that almost any CAT Data could be used for a market purpose.[178]

The Proposal points to SRO ownership and competition to support its position:

> Today, nearly all exchange SROs are part of publicly-traded exchange groups that are not owned by the SRO members, and, among other things, compete with broker-dealers and each other for market share and order flow. . .. The Commission believes that SROs may want to use CAT Data for legitimate surveillance and regulatory purposes in conjunction with an SRO rule filing, but many exchange SRO rule filings have at least some commercial component. For example, CAT Data could be used to determine whether or not a particular order type is working as intended or if changes would be beneficial to market participants—however, exchange SROs compete for order flow by offering different types and variations of order types, therefore potential SRO rule filings in this context would not be solely related to surveillance or regulation. Prohibiting the use of CAT Data for such a rule change is consistent with the existing requirement that CAT Data must be used for solely regulatory and surveillance purposes, and the proposed amendments make clear that this restriction on the usage of CAT Data applies to SRO rule filings that do not have solely regulatory or surveillance purposes.[179]

However, this explanation does not adequately examine or describe the Commission's reasons for this new requirement, which effectively eliminates the Commission's prior goal of having SROs use CAT Data to analyze market structure, market events, and to conduct "analysis of their rules and

---

[176] Id., at 66045. See 17 CFR 242.613(e)(4)(i)(A); CAT NMS Plan, Sections 6.4(f)(i)(A), 6.5(c) and 6.5(g); and Appendix C, Section 4(b).

[177] See, e.g., CAT NMS Plan Approval Order, supra note 2, at 84727, and Rule 613 Adoption Release, supra note 4.

[178] At least one SRO, FINRA, is paid fees to provide regulatory services for other SROs. As providing the regulatory service would be a commercial activity, it is not immediately clear whether FINRA would be permitted to access CAT Data to provide such services under proposed Section 8.1 as drafted.

[179] Proposal, at 66045.

pilots."[180] The Proposal does not meaningfully address the significantly restrictive effect of proposed Section 8.1 on the SROs' access to CAT Data for regulatory purposes, explain why information barriers at the SROs would be insufficient, or cite evidence that SROs have used regulatory data for commercial purpose.

Finally, it is unclear from the Proposal how the Commission would determine when an analysis of an SRO's rules would constitute a "commercial purpose," as that term in the Proposal is vague and not sufficiently delineated. A "commercial purpose" may be identified for almost every rule filing, but to abandon the use of CAT Data as a result would be contrary to a stated benefit of the CAT that the Commission has previously identified. Further, the Commission has not adequately described the anticipated benefits from the restriction, nor explained why it is deviating from the goals and criteria previously identified as desirable and contributing to the benefits of CAT.

2. The Proposed Rule Changes Would Impose Substantial New Costs Not Contemplated by Rule 613 or the CAT NMS Plan.

The Commission determined years ago that the existing CAT security framework is adequate,[181] but now seems to be reaching the opposite conclusion without explaining why. In the interim, the SROs have begun reporting data to the CAT as required by the CAT NMS Plan and Rule 613. That compliance has resulted in significant costs to the SROs.

The amounts involved are not small: as of October 15, 2020, the SROs' total costs for development of the CAT system were in excess of $221 million.[182] Already the budget for the CAT is far greater than the projections in the original CAT NMS Plan, a fact that the Proposal does not acknowledge.[183] Neither the $221 million nor the budget include the varied costs incurred by the SROs in reliance on current CAT NMS Plan requirements.[184] The NYSE believes that costs to

---

180 See CAT NMS Plan Approval Order, supra note 2, at 84803.

181 See id., at 84753 (noting that "the Commission believes that the Plan adequately addresses network security, firewalls, systems management, data loss prevention, business continuity plans and cyber incident response plans").

182 Report by the Chair of the CAT NMS LLC Operating Committee to Plan Participant Operating Committee Members, October 15, 2020.

183 See *Q4 2020 - CAT 2.0 Operating Budget v9.20.2020*, made available to Commission Staff via email on October 6, 2020; and CAT NMS Plan Approval Order, supra note 2, at 84851-84882. The 2019 audited financial statements for CAT NMS, LLC and Consolidated Audit Trail, LLC, and the audited financial statements for CAT NMS, LLC from inception through 2018, are available upon request at catllcfinancialaudit@deloitte.com.

184 The costs incurred by the SROs, including the NYSE Exchanges, include, among other things, costs for: (a) compensating and training for personnel, including regulatory and reporting compliance, project management, technology development, and legal personnel; (b) technology hardware and software systems to ensure proper CAT reporting by SROs and SRO member firms; (c) hardware and software systems for regulatory use of CAT Data; (d) coordinating implementation of SRO reporting and member firm reporting; and (e) legal resources to implement the CAT requirements. All of this investment and expenditure has been made in reliance on current CAT requirements, including the security requirements that are currently proposed to change.

comply with the CAT NMS Plan and prepare to integrate the use of CAT Data into its in-house regulatory programs would be substantial.

Now the Commission is demanding more. The Proposal would require the SROs to incur substantial additional costs—in technology costs, personnel resources, opportunity costs, and potential liability—to use CAT Data to comply with their obligations. The proposed amendments would require SROs to commit monetary, personnel, and technology resources to satisfy a wide range of new mandates, rendering the original cost/benefit analysis with respect to the CAT obsolete.[185] These costs could be significant for large exchange groups and prohibitive for smaller exchanges.

In addition, some of the Proposal's requirements would require significant alteration, or even abandonment, of projects or items for which SROs have already made investments in reliance on the existing, Commission-approved regulatory structure. For example, in reliance on the current CAT NMS Plan specifications and prior Commission guidance regarding the CAT's structure and security protocols, the NYSE Exchanges have invested considerable time and money in developing a regulatory environment to manage surveillance, investigations and enforcement, in which the NYSE Exchanges would use CAT Data pursuant to current requirements. If the Commission were to adopt the Proposal, amounts invested in that regulatory program would be largely wasted because of the mandate to either use a SAW or comply with the requirements for Non-SAWs.

In short, the proposed amendments would drive up the costs for the CAT, yet the Proposal fails to account for these costs, including technology costs, personnel resources, opportunity costs, and potential liability. The discussion below delineates additional specific costs that the Proposal would create but that the Proposal does not fully address or weigh against its expected benefits.

a. The SAWs

The detailed design specifications for the SAWs that would be required by the Proposal have not yet been created, so the SROs cannot fully estimate potential SAW-related costs at this time. A feasibility study would need to be done to quantify the estimated costs of the SAW as envisioned by the Commission. Some of the expected cost considerations for SROs and the Plan Processor with respect to the creation of, and migrating to, the proposed SAWs would include the following:

- Costs incurred to date to voluntarily create environments that comply with current CAT security requirements would become stranded costs, as those environments would likely be discarded for failing to comply with the new SAW requirement.

- Each SRO would incur costs to create a SAW under the proposed terms and migrate or recreate its systems in its SAW. These costs would relate to migrating non-CAT data and regulatory systems to a SAW.

- If an SRO attempted to create a second environment, whether or not the environment qualified as a Non-SAW, the SRO would incur costs relating to modifying or creating new regulatory, security and operational programs; creating controls, policies, and procedures;

---

[185] See CAT NMS Plan Approval Order, supra note 2, at 84799-84897. See also Sections C and D of the CAT NMS Plan for discussion of the costs and benefits associated with the present CAT.

hiring and training regulatory staff to work with the SAW and second environment; implementation planning; creating procedural tracking for regulatory activities occurring in parallel to activities occurring within the SAW; testing; accounting fees; licensing fees for third party data; reaching any new agreements with customers and third parties; insurance policies; and risk management procedures. For example, an SRO would have to either build duplicate surveillance and case management systems in the proposed SAW or move its surveillance and case management systems into the proposed SAW wholesale. Either choice represents a substantial project, perhaps hundreds of person-years of work.[186]

- The totality of the costs could be impossible for smaller SROs to meet, resulting in a competitive disadvantage for them as they would likely be forced to pursue other methods for fulfilling their regulatory oversight obligations for their markets, such as increased outsourcing to FINRA.

- The Proposal seems to posit that all SROs can use the same operational, network and security tools in their SAWs, and that the Plan Processor could provide and host such tools within the SAWs. In reality, SROs all have different tools, which would have to be altered to work with a SAW. SROs like the NYSE Exchanges have already expended resources to build surveillance and security tools that would work with CAT Data in their existing regulatory environments, but those would quickly become obsolete under the proposed SAW requirements. This outcome would create inefficiencies and security risk, which would be substantial if SROs could not use or otherwise leverage their own regulatory environments. For example, the Plan Processor and SROs have already built and tested user-defined direct query access. The proposed amendment would require needless extra effort and expense to recreate the access inside the proposed SAW and add security and operational risk.

- An SRO's data and systems could incur a cost due to reduced response time, technical impact, and reduction in regulatory ability during a migration to the SAW.

- The SROs would have to pay the Plan Processor for its work relating to creating and monitoring the SAWs, none of which is contemplated by the current Plan Processor Agreement. The Proposal does not adequately address the inefficiencies of paying more to the Plan Processor for a SAW that is redundant of the surveillance systems that SROs currently have and to which Regulation SCI applies.

Based on the current state of development of the SAW and Direct Read (the primary mechanism by which CAT data could be drawn into a SAW or a regulator's environment for use in surveillances), to use anything more than a miniscule quantity of CAT Data, SROs would have to perform substantial system development in the proposed SAW. Once those systems are created, some of the notable cost considerations for SROs and the Plan Processor with respect to the mandated use of the SAWs are as follows:

---

[186] NYSE regulation is currently migrating regulatory systems into a new platform, which is a much less complex process than would be migrating into a SAW described in the Proposal. Based on this experience, NYSE regulation projects that a migration into the SAW described in the Proposal would require substantially more resources and multiple years to complete.

- Because SROs essentially would be required to bring their regulatory systems and non-CAT data into their SAWs, storage costs for CAT Data could increase exponentially, due to the sheer volume of regulatory data within SROs' existing regulatory environments. Storage costs could also increase whenever an SRO downloaded CAT Data into its SAW, since each of those records would have to be retained pursuant to national securities exchange record retention obligations.[187]

- In addition to storage costs, compute costs to utilize the data within the SAW would increase, as the CAT would now house exponentially more data than previously contemplated.

- Because control of the SAW from a security and monitoring perspective would be in the hands of the Plan Processor, SROs would have to create additional oversight structures to seek to ensure the security of their own data and systems that they by necessity introduce to the SAW, creating an additional cost.

- As noted above, proposed Rule 6.13(a) would require that the only mechanism to extract CAT Data from the SAWs would be secure file sharing capability provided by the Plan Processor.[188] Based on experience, this method would result in data that is not machine readable, so more humans would be needed to read the data. Inevitably they would be less efficient than a machine and create more room for human error. This structure would increase staffing costs, as well as risk.[189]

b. Plan Processor, CISO and CCO Costs

Because the Plan Processor is a vendor to the SROs, the Plan Processor would pass all its additional costs to the SROs. If Plan Processor costs go up, costs to the entire industry go up, regardless of how much or whether SROs utilize the SAWs.

The Plan Processor's, and therefore the SROs', costs would be impacted by the Proposal as follows:

---

187 Under Rule 17a-1 of the Exchange Act, each national securities exchange must keep and preserve at least one copy of all documents and records that it makes or receives "in the course of its business as such and in the conduct of its self-regulatory activity." 17 CFR 240.17a-1(a). They must retain such records for not less than five years and must furnish copies of such documents to any representative of the Commission upon request. 17 CFR 240.17a-1(b) and (c). See also 17 CFR 240.17a-6 (providing that a document kept by a national securities exchange pursuant to the Exchange Act or any rule or regulation thereunder may be destroyed or otherwise disposed of by such exchange at an earlier date if in accordance with a plan filed with, and declared effective by, the Commission).

188 Proposal, at 65998. If the file transfer protocol referred to here is like the one used before the online query tool was available, each output file would be attached to a password-protected email that required manual intervention to open it before it could be used in an SRO's system. If so, it would be inefficient for anything but a handful of files.

189 It also seems counter to the Commission's apparent desire to limit the number of people with access to CAT Data. As noted above, reducing the number of regulators with access to CAT Data is contrary to one of the primary purposes of the CAT. See note 62, supra.

- The Plan Processor would incur substantial new costs related to its and its employees', the CISO and CCO, expanded roles.[190] These costs would include the expense of: creating the SAWs; creating controls, policies, and procedures; hiring and training regulatory staff to work with and monitor the SAWs and Non-SAW environments; hiring and training regulatory staff with sufficient expertise with every type of data, software and surveillance that an SRO might want to bring into its SAW; hiring and training regulatory staff to provide the mandated monitoring and oversight; testing; accounting fees; reaching any new agreements with customers and third parties; insurance policies; and risk management procedures.

- Because of the added requirements and increased risk, among other things, that the Proposal would place on the Plan Processor, CISO and CCO, a new Plan Processor agreement would need to be negotiated. Further, there is no guarantee that an agreement could be reached.[191] At a minimum, the new requirements would result in an increase in the negotiated fees for the Plan Processor. Such costs have not been estimated or considered by the Commission, nor have they been reviewed and weighed against the benefits that the Commission hopes to derive from the Proposal. Further, negotiating a revised Plan Processor agreement would likely affect the current CAT development timeline, hindering SROs' ability to meet the regulatory deadlines that Rule 613 and the CAT NMS Plan impose upon the SROs and subjecting the SROs to financial penalties.

- Under the Proposal, the SROs would be required to pay the Plan Processor to monitor the SROs' own compliance with the CAT NMS Plan, even though the SROs are obligated by law to comply with the CAT NMS Plan and the Plan Processor is the SROs' vendor.

c. Penalties under the Financial Accountability Milestones

The Proposal would affect the SROs' ability to meet the milestones set forth in the recent financial accountability milestone amendment (the "Financial Accountability Amendment").[192] The imposition of additional new requirements from the Proposal could jeopardize the overall implementation timeframe of the CAT and lead to substantial financial penalties for the SROs. The Commission has not reasonably considered the impact of imposing substantial new burdens on the SROs through the Proposal, and the potential for delays caused directly by those new burdens, on the SROs' ability to meet the requirements in the Financial Accountability Amendment.

d. General Costs on Market Participants

In addition to the above described costs, the Proposal raises the following cost considerations for the SROs, the Plan Processor, and the market as a whole:

---

[190] For the requirements for the Plan Processor, CISO and CCO under the proposed changes to the NMS CAT Plan, see Part I.A.2, Part I.B.1.a, and note 17, supra.

[191] Realistically, because the SROs would be obligated to implement any amendments to the CAT NMS Plan adopted by the Commission, in timeframes established by the Commission, they will have no choice but to agree to FINRA CAT's terms.

[192] Securities Exchange Release No. 88890, 85 FR 31322 (May 22, 2020) (Amendments to the National Market System Plan Governing the Consolidated Audit Trail).

- The Proposal does not sufficiently account for the cost to the entire market of decreased efficiency in market regulation; slowed, inefficient, or ineffective surveillance; or hindered diversity in, and volume of, regulation.

- The Proposal does not sufficiently account for the cost of potential liability to SROs for exposing their regulatory systems, member firm data, PII, and third-party data and systems to the SAW and the Plan Processor, as well as placing oversight of these elements with the Plan Processor.

- The Proposal does not sufficiently account for the impact on competition and efficiencies in price negotiations with data storage, infrastructure, and network vendors. Currently, such vendors negotiate with multiple SROs, but under the Proposal they would negotiate with a single party, which would pass its costs back to the SROs.

- Given the structure of the CAT NMS Plan, if one Participant incurred costs as a result of the Proposal, such as by requiring additional storage in the SAW, the costs attributable to the CAT would increase. Under the funding rules of Rule 613 and the CAT NMS Plan, the cost would not be borne by the individual Participant whose regulatory program gave rise to the expenses, but rather by all the SROs and industry participants.[193]

- The proposed expanded, more prescriptive requirements for the SWG would mean that SWG members would have increased time commitments relative to the ESWG. Consequently, SWG members would be less available to deal with other issues, CAT-related or otherwise. In some cases, not just the SWG but also other SRO subject matter experts may be required to participate in a SWG.

- There would be an additional cost to Participants in implementing, maintaining and monitoring the proposed CAT-required Confidentiality Policies and parallel internal policies. Imposing a generic security standard across SROs would create additional costs associated with implementing the standard across not just the SROs but also any applicable affiliated entities. In addition, the Plan Processor would incur costs in "learning" SROs' systems to create a Proposed Confidentiality Policy, irrespective of whether any of the SROs actually use a SAW.

- Each year, a Participant would be required to retain an independent accountant perform an examination of its compliance with the policies in accordance with attestation and Commission independence standards and submit the results to the Commission. In addition to not recognizing that an accountant may not be the best qualified to examine the technical controls, or explaining why a "security assessor" was previously sufficient but the Proposal requires an accountant, the Proposal does not adequately address the costs incurred by a custom engagement with an accountant that does not follow an existing engagement format, or the added cost and inefficiency of requiring multiple audits and assessments with varying requirements.

- Applying the CISP beyond the Central Repository could severely limit the availability of CAT Data to certain SROs for use in their own environments, as they may not currently use the NIST Cyber Security Framework. The Proposal does not consider the cost for Participants

[193] See CAT NMS Plan, Sections 11.1 and 11.3.

that do not currently have their security program defined in NIST Cyber Security Framework terms to develop and maintain such a program for just areas in scope of the CISP. Similarly, the Proposal does not consider the potential risk of security implementation errors for participants forced into a maintaining dual control structures (NIST Cyber Security Framework and non-NIST) within their overall enterprise. Participants that don't use the NIST Cyber Security Framework for their Software Development Lifecycle ("SDLC") would face migration and development costs to migrate or recreate their systems into the SAW that were potentially higher than those of Participants that use the NIST Cyber Security Framework for their SDLC.

- The Proposal does not adequately consider the cost associated with widely specifying private lines. For example, the Proposal does not meaningfully consider the costs incurred with using private lines instead of VPN connections for machine-to-machine interfaces, or the cost of supporting VPN connections for a large number of small submitters relative to the cost of supporting a secure web interface.

- The Proposal does not adequately consider the cost for multinational entities to redesign their internal networks to prevent access to CAT by authorized users when they travel to locations where CAT access would be prohibited.

- The Proposal states that, to the extent that a systems or data breach affects not only the users of the CAT System, but the securities market and its participants as a whole, the Plan Processor would need to consider how it might mitigate any potential harm to the overall market to help protect market integrity.[194] Yet in the Proposal the Commission does not adequately consider the cost of creating and maintaining response resources for the described level of CAT impact, especially when such breach would not implicate market systems that impact trading because CAT and the SRO surveillances that CAT Data support do not operate in real time and have little to no impact on the "markets as a whole."

3. The Proposal is Arbitrary and Capricious Because it Fails to Address These Critical Issues.

The Proposal is arbitrary and capricious because it fails to sufficiently acknowledge or grapple with the problems discussed in Parts IV.B.1-2 above.[195] In particular, the Proposal does not account for the significant reduction in the CAT's benefits that the proposed amendments would cause, and likewise overlooks many of the substantial cost increases that would result.[196] As a result, the costs and benefits of the CAT would differ substantially under the Proposal than under the current CAT NMS Plan. Although the Commission determined that the CAT's costs were justified by its benefits

194 Proposal, at 66050 and 66101-66102 (proposed Appendix D, Section 4.1.5 of the CAT NMS Plan).

195 See *Motor Veh. Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983).

196 Although the Proposal includes an assessment of baseline costs and benefits, that assessment omits many of the reduced benefits and increased costs identified in Parts I.B.1-2 above, and relies on insufficient costs estimates with respect to other elements. See Proposal at 66073.

when it approved the CAT NMS Plan,[197] the Commission has not adequately demonstrated that the CAT's costs would continue to be justified if the Proposal were adopted.[198]

In this regard, the Proposal also fails to comply with the Commission's statutory obligation to weigh the costs and benefits of its proposed regulations. Section 23(a) of the Exchange Act authorizes the Commission "to make such rules and regulations as may be necessary or appropriate to implement" the Act,[199] and the Proposal invokes Section 23(a) as one of its bases.[200] The Supreme Court has interpreted nearly identical language as "requir[ing] at least some attention to cost" as well as the relation of a rule's costs to its benefits.[201] As a result, the Commission must reconsider its proposed changes in light of the substantially reduced benefits and increased costs described above, and must adhere to the APA's requirement of reasoned decision making in doing so.[202]

4. The Proposal Is Arbitrary and Capricious Because It Departs Without Explanation from the Commission's Longstanding Approach to CAT Security.

The Commission determined years ago that the existing CAT security framework is adequate and can be adapted to new needs and circumstances.[203] If adopted, the Proposal would significantly amend the CAT's security framework without acknowledging these prior conclusions or showing a need for the change. That unexplained departure from past Commission practice is arbitrary and capricious under *Fox Television*. [204]

Indeed, in accordance with *Fox Television*,[205] the Commission is obligated to provide a heightened justification for the Proposal's changes because those changes necessarily rest on an (unstated) factual conclusion (i.e., the current security measures are inadequate) that conflicts with the Commission's prior finding that the current CAT security framework *is* sufficient. The Proposal does not point to evidence sufficient to meet that standard. Similarly, the Commission must provide a heightened justification for the Proposal's sweeping changes because, as explained above, the SROs have made substantial investments, including in regulatory programs in reliance on the

---

197 See CAT NMS Plan Approval Order, supra note 2, at 84799-84897. See also Sections C and D of the CAT NMS Plan for discussion of the costs and benefits associated with the present CAT.

198 See, e.g., *Owner-Operator Independent Drivers Ass'n, Inc. v. FMCSA*, 494 F.3d 188, 206 (D.C. Cir. 2007). See also Bauguess Letter, supra note 31.

199 15 USC 78w(a).

200 See Proposal, at 66096.

201 See *Michigan v. EPA*, 576 U.S. 743, 751-52 (2015).

202 See *Owner-Operator Independent Drivers Ass'n, Inc. v. FMCSA*, supra note 198, at 206.

203 See CAT NMS Plan Approval Order, supra note 2, at 84753 (noting that "the Commission believes that the Plan adequately addresses network security, firewalls, systems management, data loss prevention, business continuity plans and cyber incident response plans").

204 *FCC v. Fox Television*, supra note 21, at 514-515.

205 See id. at 515 (agency must "provide a more detailed justification" when "its new policy rests upon factual findings that contradict those which underlay its prior policy").

CAT's current security framework.[206] The NYSE has been unable to find a mention of reliance interests in the Proposal, much less an explanation of why it is necessary to adopt amendments that would strand investments made based on the current CAT framework. As a result, the Proposal fails to comply with this element of the *Fox Television* standard as well.

II. The Proposal Does Not Adequately Address Its Effect on Efficiency, Competition, and Capital Formation.

Where, as here, the Commission exercises rulemaking authority under a provision requiring the Commission to consider "whether an action is necessary or appropriate in the public interest," the Commission must also consider "whether the action will promote efficiency, competition, and capital formation."[207] The Proposal fails to comply fully with that mandate. Although the Proposal purports to review its effect on efficiency, competition and capital formation, the Proposal does so in a way that overlooks important aspects of the problem—including in particular adverse effects on competition in the market for regulatory oversight. The upshot is that the Proposal rests on an analysis that is manifestly contrary to the record. As a result, the Commission's action is arbitrary and capricious under the APA.[208]

A. The Proposal Disproportionately Benefits One SRO.

1. The Proposal's Uneven Impact Would Benefit FINRA.

The Proposal does not contemplate the uneven impact its adoption would have on the SROs. As discussed above, the Proposal would force the SROs to unprecedented reliance on the Plan Processor—and grant the Plan Processor and its employees the CISO, and CCO an unprecedented level of responsibility.[209] At the same time, the technical knowledge and availability of the SWG could be reduced, increasing its reliance on the CISO, CCO and Plan Processor—a subsidiary of FINRA, one of the national securities exchanges' competitors in the market for regulation and market surveillance. Under the Proposal, all of an SRO's proprietary regulatory programs and associated technologies and data uploaded to its SAW would be exposed to a direct competitor.

From experience, the NYSE is aware that the Plan Processor already shares some technology services and policies with FINRA, and some FINRA employees also do Plan Processor work. This is not in itself a problem; it is often efficient for a subsidiary to use its parent's resources. However, in this case, the relationship between FINRA and the Plan Processor means that any implementation of the Proposal is likely to have an uneven effect in favor of FINRA, since the costs and risks created by the Proposal would be higher for the other SROs than FINRA.

---

206 See id. ("more detailed justification" required when agency's "prior policy has engendered serious reliance interests that must be taken into account").

207 15 USC 77b(b), 78c(f).

208 See Bauguess Letter, supra note 31. at Part V (Economic Considerations of Efficiency, Competition and Capital Formation).

209 For the proposed requirements for the Plan Processor, see Part I.A.2, Part I.B.1.a, and note 17, supra.

For example, the proposed SAWs would likely require regulatory system developments. To the NYSE's knowledge, FINRA is the only SRO with the infrastructure in place to use a data access system similar to the Direct Read access expected to be used for the bulk of the data access in the SAWs. To build a similar infrastructure around Direct Read is estimated to take at least several person years of effort and at least several months of real time, leading to higher costs for all SROs other than FINRA. Further, there would be a conflict of interest when the CISO or CCO determine what standards should apply because, as employees of FINRA, they may be more likely to pick standards already applicable to FINRA. Finally, FINRA could leverage its already large-scale use of AWS to move all or most of its surveillance program into a SAW more easily than could other SROs.

FINRA would have an additional structural advantage because the Plan Processor has adapted its policies from FINRA policies. Review and oversight of FINRA's policies by the Plan Processor would therefore cost FINRA relatively little, because all of its policies would be substantially similar to those of the Plan Processor.

2. The Proposal's Provisions on Programmatic Access Would Create Disparity of Access Between SROs.

Under the Proposal, any SRO that wishes to use Programmatic CAIS Access or Programmatic CCID Subsystem Access would be required to submit an application approved by its chief regulatory officer to the Commission for authorization.[210] Consequently, customer data would be segregated from transaction data for only some regulators. That outcome would create disparity of access between SROs, allowing some joint access to customer and transaction data and not allowing others. Giving some SROs more access than others would not promote a strong, diversified regulatory environment, as access to transaction and customer data together is essential to many regulatory purposes, as the Commission itself has recognized.[211] In addition, there is an inherent design conflict in requiring the separation of transactional and customer data yet requiring extracts from those databases to reside together in the SAW.

B. The Proposal Would Lead More National Securities Exchanges to Outsource their Regulatory Programs to FINRA, Reducing Competition.

The myriad issues raised under Part I above—the risks connected with importing non-CAT data and surveillance systems into the SAWs; the risks created by having a single, more valuable target; the risks created by the level of reliance on the Plan Processor; the risks related to the rigidity of proposed requirements; the risks tied to the unprecedented access of a FINRA subsidiary to non-CAT data and surveillance systems; the risks created if an SRO maintains a Non-SAW environment; and the substantial and in many cases unmeasurable new costs that would be incurred by an SRO that tried to comply with the requirements of the Proposal—all lead to one conclusion: a national securities exchange is likely to rationally conclude that outsourcing its regulatory program is less costly than maintaining its own regulatory program under the restrictive and costly conditions proposed for access to CAT Data.

---

[210] Id., at 66102 (proposed Section 4.1.6— Programmatic Access—Authorization for Programmatic CAIS Access and Programmatic CCID Subsystem).

[211] Id., at 65998.

The reality is that, if the Proposal is adopted, FINRA would become the provider of all or nearly all of the outsourced services. It already provides outsourced regulatory services for many of the SROs, under both regulatory service agreements ("RSAs")[212] and allocations of regulatory responsibilities pursuant to Rule 17d-2, and the NYSE believes it would be easier for FINRA to comply with the Proposal than for the other Participants. As other SROs make the rational decision to outsource regulatory obligations that depend on CAT Data, the most likely result is that FINRA would provide the services and become further entrenched and monopolistic.

This foreseeable consolidation could have the effect of reducing competition among regulators, which includes the competition to make regulatory oversight of the market more efficient and effective. That dynamic could reduce the amount of innovation in, and the diversity of, regulatory approaches. Ultimately, the consolidation could cause regulatory oversight to become less effective.

One of the CAT's original purposes was to increase and democratize regulatory oversight of the U.S. securities markets. The CAT was designed to "substantially enhance the ability of the SROs and the Commission to oversee today's securities markets and fulfill their responsibilities under the federal securities laws."[213] When approving the CAT NMS Plan, the Commission stated "its belief that the economic benefits of the CAT NMS Plan would come from any expanded or more efficient regulatory activities facilitated by improvements to the data regulators use" and that the "improvements would benefit investors, market participants, and markets in general."[214]

The Proposal would have the opposite effect. If adopted, the Proposal would effectively remove the ability for many, if not most, SROs to access CAT Data, whether due to increased risk or cost. Market data that was meant to be used for regulatory purposes would be rendered inaccessible to many SROs, and the expansion of regulatory oversight originally contemplated by the Commission when it adopted Rule 613 would be substantially curtailed, if not eliminated.

III. The Proposal Overlooks Alternative Approaches to Securing CAT Data.

The Commission has failed to adequately address meaningful alternatives to achieving its goals to further secure CAT Data,[215] and so its action, should the Proposal be adopted, would be arbitrary and capricious.

---

212 The Proposal states that "the Commission preliminarily believes it would be appropriate for Regulatory Staff to access CAT Data to oversee and audit the performance of the SRO under an RSA, since the ultimate regulatory responsibility remains with the outsourcing SRO." Id., at 66039. For an SRO to have access to CAT Data, it would have to comply with the requirements of the Proposal. It seems more likely that an SRO that outsources to FINRA would not, or could not, incur the discussed risks and cost for access to CAT Data in order to assess FINRA's performance, reducing its ability to oversee FINRA's work under the RSA.

213 See Rule 613 Adoption Release, supra note 4, at 45726.

214 See CAT NMS Plan Approval Order, supra note 2, at 84816-84817; and CAT NMS Plan, at Appendix C, Section 2(b).

215 See *Am. Ass'n of Cosmetology Schools v. Devos*, 258 F. Supp. 3d 50, 75 (D.D.C. 2017). Of the Proposal's 116 pages in the Federal Register, it dedicates fewer than two pages to the consideration of alternatives. Proposal, at 66092-66093.

One alternative would be to rely on the existing security requirements of the CAT NMS Plan and the SROs' obligations under Rule 608.[216] Currently, to meet their responsibilities, the SROs monitor the CAT System through a broad array of governance infrastructure, including the Operating Committee,[217] which has primary responsibility for the CAT's security. For its part, the Commission has the ability to review the Participants' compliance with existing statutory and regulatory requirements, and to bring enforcement actions when necessary. NYSE does not believe there is any need for the Commission to attempt to delegate large portions of its own and the SROs' responsibilities to a vendor such as the Plan Processor. The Proposal does not identify flaws in the current oversight from SROs that would require implementing any changes.

A second alternative would be for the Commission to continue to rely on Regulation SCI[218] as a means for securing CAT Data. Regulation SCI already governs both the CAT system and the SRO systems that would be used to access CAT data.[219] Regulation SCI applies to the CAT System because it is an SCI system of the Plan Processor, which is an SCI entity.[220] When the

---

216 See CAT NMS Plan Approval Order, supra note 2, at 84753 (noting that "the Commission believes that the Plan adequately addresses network security, firewalls, systems management, data loss prevention, business continuity plans and cyber incident response plans"). The present requirements include an exemption from reporting certain PII to the CAT, conditioned on the SROs meeting enumerated conditions. See 85 FR 16152, supra note 58.

217 See CAT NMS Plan, Appendix C, Section 11(b) (""The overarching role of the Operating Committee is to manage the Company and the CAT System similar to the manner in which a board of directors manages the business and affairs of a corporation. The primary and more specific role of the Operating Committee is to make all policy decisions on behalf of the Company in furtherance of the functions and objectives of the Company under the Exchange Act, any rules thereunder, including SEC Rule 613, and the CAT NMS Plan."). See also CAT NMS Plan, Sections 4.1 and 4.2.

218 17 CFR 242.1000 et seq. Reg SCI applies to "SCI Entities," including all SROs, and requires, among other things, that each SCI Entity "[i]mplement policies and procedures reasonably designed to ensure that its 'SCI systems' and 'SCI security systems' have levels of capacity, integrity, resiliency, availability, and security, adequate to maintain the SCI entity's operational capability . . . with deemed compliance for policies and procedures that are consistent with current SCI industry standards, including identified information technology publications listed on proposed Table A…" Id., at 72256.

219 See Proposal, at note 54 (noting that the "Plan Processor thus must establish, maintain, and enforce written policies and procedures reasonably designed to ensure that the CAT System has levels of capacity, integrity, resiliency, availability, and security adequate to maintain its operational capability to comply with Regulation SCI."), and 17 CFR 242.1000 (definition of "SCI system").

220 Under Rule 1000 of Regulation SCI, the Plan Processor is classified as an SCI entity because of its status as a "plan processor," which "has the meaning set forth in §242.600(b)(55)." 17 CFR 242.1000. 17 CFR 242.600(b)(55) defines "plan processor" as "any self-regulatory organization or securities information processor acting as an exclusive processor in connection with the development, implementation and/or operation of any facility contemplated by an effective national market system plan" (emphasis added). Section 3(a)(22)(B) of the Exchange Act defines the term "exclusive processor" as "any securities information processor or self-regulatory organization which, directly or indirectly, engages on an exclusive basis on behalf of any national securities exchange or registered securities association…in collecting, processing, or preparing for distribution or publication any information with respect to (i) transactions or quotations on or effected or made by means of any facility of such exchange or (ii) quotations distributed or published by means of any electronic system operated or controlled by such association." 15 USC 78c(22)(B). See also Securities Exchange Act Release No. 85764 (May 2, 2019), 89 FR 20173 (May 8, 2019) (Notice of Filing and Immediate Effectiveness of a Proposed Rule

Commission proposed Regulation SCI in March 2013—at the outset of the CAT bidding process—it stated its preliminary belief that the CAT Plan Processor would be an SCI entity "selected and acting as exclusive processor of a future NMS plan, such as that contemplated by the Commission's rules to create a consolidated audit trail."[221] In adopting Regulation SCI, the Commission did not alter its view that the Plan Processor for CAT would be an SCI entity.[222] In addition, the CAT NMS Plan Approval Order stated that "the Commission expects that the Participants will evaluate a Bidder's ability to comply with Regulation SCI as part of its Bidder evaluation process, as compliance with Regulation SCI is an explicit criteria [sic] of the CAT NMS Plan."[223]

As noted above,[224] the Commission does not adequately explain why additional security measures that differ from, or are additional to, Regulation SCI are necessary, why it views the Regulation SCI requirements as inadequate, why the CAT would need to have more stringent requirements than other SCI systems, or assess in detail how the proposed new security requirements are compatible with the application of Regulation SCI to the same systems. In these ways, the Proposal departs from the Commission's previous position that the SROs would work to meet their Regulation SCI obligations related to CAT "as efficiently as possible" and "without unnecessarily duplicating efforts."[225] Moreover, it beggars belief that Regulation SCI could be adequate for all SCI systems that, with respect to securities, support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance, but not adequate for the CAT.[226]

As an example, as discussed in more detail elsewhere, the Proposal does not adequately consider alternatives with respect to PII and Customer IDs.[227] Existing SRO databases include sensitive data, including PII, and have found reasonable methods to manage the balance between security and usability, all in compliance with Regulation SCI. Yet rather than explore such options, the Proposal would move from a flexible system that can develop with technology and best practices to a rigid prescriptive standard that cannot evolve or change without a CAT NMS Plan amendment.[228]

Change To Update the FINRA Manual To Reflect FINRA's New Subsidiary, FINRA CAT, LLC), at 20174 (stating that FINRA CAT LLC is an SCI entity).

221 See Securities Exchange Act Release No. 69077 (March 8, 2013), 78 FR 18084, 18096 n.131 (order proposing Regulation SCI).

222 See Securities Exchange Act Release No. 73639, 79 FR 72252 (December 5, 2014) (order adopting Regulation SCI), at 72270.

223 See CAT NMS Plan Approval Order, supra note 2, at 84759.

224 See Part I.A.4, above.

225 CAT NMS Plan, Appendix C, at C-4.

226 See 79 FR 72252, supra note 222.

227 See Bauguess Letter, supra note 31.

228 See Part I.A.4, above.

IV. The Proposal Exceeds the Commission's Authority.

A. The Proposal Conflicts with Rule 613.

The Proposal's new limitations are inconsistent with Rule 613's direction that the SROs must have access to CAT Data "for the purpose of performing [their] regulatory and oversight responsibilities," and that such access "shall not be limited."[229]

As described above, the Proposal's mandates would sharply limit SROs' ability to access and utilize CAT Data.[230] Rule 613 and the CAT NMS Plan call for a collaborative approach to management of the CAT and do not contemplate giving a vendor like the Plan Processor, directly or through the CISO and CCO, such broad access and control over an SRO's regulatory environment.[231] Nonetheless, the Proposal would charge the Plan Processor with substantial gatekeeping and monitoring authority.[232] Not only would it develop and maintain "detailed design specifications for the technical implementation of the access, monitoring, and other controls required for SAWs by the Comprehensive Information Security Program controls,"[233] but it would also determine whether a Participant's SAW has met the requirements to connect to the Central Repository.[234] Moreover, the Plan Processor would be charged with monitoring each SAW for compliance with the CISP and design specifications, notifying the Participant of any identified non-compliance.[235] As a result, the Plan Processor would be able to dictate the ways in which the SROs meet their regulatory requirements under the Exchange Act, the context and terms in which they will access CAT Data and, most likely, other data and regulatory surveillances.

The Proposal does not squarely confront the ways in which it departs from Rule 613, and indeed does not address Rule 613's "shall not be limited" language at all. Nor does the Proposal provide "good reasons" for replacing that open-access guarantee with a new, restrictive regime in which many SROs will be unable to make meaningful use of CAT Data.[236] The Proposal's "failure to come to grips with conflicting [agency] precedent constitutes 'an inexcusable departure from the essential requirement of reasoned decision making.'"[237]

---

229 17 CFR 242.613(e)(2).

230 See Part I.B.1, above.

231 See CAT NMS Plan Approval Order, supra note 2, at 84830 ("The Commission explained that the Plan would bring audit trail data related to trading on all venues into the Central Repository where it could be accessed by all regulators"); and CAT NMS Plan, Article IV, Section 4.2(a) (providing that the Operating Committee shall consist of one voting member from each SRO).

232 See Parts I.A.1 and 2 and Part I.B, above.

233 Proposal, at 66099 (proposed Section 6.13(b)(i)).

234 Id., at 66099 (proposed Section 6.13(b)(ii)).

235 Id. (proposed Section 6.13(c)(i)).

236 See *FCC v. Fox Television*, supra note 21, at 515.

237 *Ramaprakash v. FCC*, supra note 35, at 1125 (quoting *Columbia Broad. Sys. v. FCC*, 454 F.2d 1018, 1027 (D.C. Cir. 1971)).

B. The Proposal Unlawfully Delegates Significant Governmental Power to the Plan Processor and Its Officials.

1. The Proposal Is Inconsistent with the Exchange Act and Commission Rules.

Section 11A of the Exchange Act states that the Commission may "authorize or require *self-regulatory organizations* to act jointly with respect to matters as to which they share authority under this chapter in planning, developing, operating, or regulating a national market system."[238] Consistent with the Commission's limitations of authority, Rule 608 assigns the responsibility for "implementing" and "administering" every NMS Plan to the SROs themselves.[239] Each SRO, which is statutorily required to "protect investors and the public interest,"[240] is also legally obligated to comply with the terms of each NMS Plan of which it is a sponsor or participant and charged with "enforc[ing] compliance with any [NMS] plan by its members and persons associated with its members." Vesting that power exclusively with SROs makes sound policy sense because, unlike ordinary private persons, SROs are obligated under the Exchange Act to discharge quasi-governmental functions and, in so doing, are required to act in the public interest and in furtherance of the Exchange Act's statutory objectives.

The Plan Processor, by contrast, has no obligations under Rule 608 to administer or implement the CAT Plan or to comply with its terms. In addition, although they owe a fiduciary duty to CAT NMS Plan LLC, the CISO and CCO are Plan Processor employees and, similarly, have no obligations under Rule 608.

Nonetheless, the Proposal would delegate authority to the Plan Processor, CISO and CCO.[241] More specifically, the Proposal would delegate the following regulatory responsibilities:

- Responsibility to the CISO and CCO to review the SROs' policies developed pursuant to Section 6.5(g)(i), and determine whether an SRO may use, or continue to use, a Non-SAW environment, after review of the SRO's initial or annual application.[242]

- Responsibility to the CISO and CCO to review the CAT Data extracted from the CAT System, "to assess the security risk of allowing such CAT Data to be extracted."[243]

- Responsibility to the Plan Processor to notify the Operating Committee when an SRO's SAW has met the requirements of the detailed design specifications, which is required

---

238 15 USC 78k-1(a)(3)(B) (emphasis added).

239 17 CFR 242.608(a)(3)(iii).

240 15 USC 78f(b)(5),

241 For the requirements for the Plan Processor, CISO and CCO under the proposed changes to the NMS CAT Plan, see Part I.A.2, Part I.B.1.a, and note 17, supra.

242 See Proposal, at 66097 (proposed Sections 6.1(a)(v)(R), 6.1(a)(v)(S), 6.1(b)(v)(F)(viii) and 6.1(b)(v)(F)(ix)), and 66099 (proposed Sections 6.13(d)(i)(B) and 6.13(d)(i)(B)).

243 Id., at 66097 and 66098 (proposed Sections 6.2(a)(v)(T), 6.2(b)(v)(F)(x), and 6.6(b)(ii)(B)(3)).

before a SAW may connect to the Central Repository.[244] Implicit in the requirement is a rule that, before such notice can be given, the Plan Processor would have to make a determination whether the SAW met the relevant requirements.

- Responsibility to the Plan Processor to monitor each SRO's SAW, for compliance with the CISP and the relevant design specifications, and to notify the SRO of any identified non-compliance.[245]

As a federal agency, the Commission may only take actions expressly or implicitly authorized by statute,[246] and Section 11A does not authorize the Commission to delegate its regulatory responsibility to entities or persons that, like the Plan Processor, CISO and CCO, are not SROs. Such non-SROs have no regulatory obligations vis à vis the Plan and the Commission cannot create such obligations, as it does in its Proposal.

The Commission is charged with ensuring Participants' compliance with their obligations under the securities laws[247] and, as their regulator, is uniquely positioned to fulfill that role. The Commission regularly conducts investigations into the SROs' operations and structures, including their compliance with obligations under the CAT NMS Plan. Nothing under the Exchange Act permits the Commission to delegate these responsibilities to the Plan Processor or its employees.

Moreover, as previously discussed, Rule 613(e)(2) mandates SROs' access to and use of CAT Data to meet their regulatory and oversight responsibilities "shall not be limited."[248] Delegating the above responsibilities to the CISO and CCO and Plan Processor would put these non-SROs in the position of causing the SROs to be in violation of that provision, because the CISO, CCO and Plan Processor would have the authority to determine whether SROs could have access to and use of CAT Data, whether in a SAW or Non-SAW. There is no caveat to Rule 613(e)(2) stating that SROs' access to and use of CAT Data may be limited or even blocked if not approved by employees of a third-party unregulated vendor, or the vendor itself. A vendor cannot, and should not, have regulatory oversight of an SRO's use of a regulatory system that Commission rules require the SRO to use.[249]

Another untenable consequence of the Commission's Proposal is that the SROs' obligation under Rule 608(c) to comply with the terms of the CAT NMS Plan would require the SROs to monitor whether the Plan Processor and its employees are fulfilling their assigned oversight responsibilities over the SROs. It makes no sense for the vendor that is hired by a group of SROs to enable the SROs to meet their obligations under the Rules 608 and 613 and the CAT NMS Plan to regulate those same SROs. Any failure by the Plan Processor and its employees to meet their obligations,

---

244 See id., at 66099 (proposed Section 6.13(b)(ii)).

245 See id. (proposed Section 6.13(c)(i)).

246 See *Louisiana Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986) (finding that A federal agency has "literally has no power to act . . . unless and until Congress confers power upon it").

247 See 15 USC 78k-1.

248 17 CFR 242.613(e)(2).

249 Id.

which the SROs would have no alternative but to allow, would ultimately be the SROs' failure to meet their obligations under Rule 608(c).

Reviewed as a whole, under the Proposal the Commission would effectively cede its review of many aspects of the SROs' compliance with CAT NMS Plan requirements to the Plan Processor and require the SROs to rely on the Plan Processor to meet the SROs' own obligations. It is the Commission's responsibility to conduct inspections of SRO usage of CAT Data and to inspect SRO systems to ensure compliance with the CAT NMS Plan. However, with the Proposal, the Commission proposes to have a limited liability company that is a subsidiary of one of the competing SROs and has no regulatory obligations to the SROs or the Commission, carry out the Commission's oversight responsibilities.

The NYSE cannot support that proposal. Such delegation of regulatory oversight by the Commission is not permitted under the Exchange Act.

2. The Proposal Violates the Appointments Clause of the U.S. Constitution.

Under the Appointments Clause of the Constitution, every "Officer of the United States" must be appointed by the President, the courts, or the head of an executive branch department.[250] There are two requirements to qualify as an "officer" subject to the Appointments Clause's restrictions. *First*, a person must occupy a "continuing or permanent" office "established by law." *Second*, that person must exercise "significant authority pursuant to the laws of the United States."[251]

Commission regulations establish the offices of Chief Information Security Officer and Chief Compliance Officer, and the Proposal would grant those offices significant authority by empowering them to regulate SROs' access to CAT data. As a result, the CISO and CCO are "Officers of the United States." Because they are appointed by the Plan Processor, [252] rather than the Commission (or any other eligible party), the Proposal would violate the Appointments Clause if adopted. Any actions taken by the CISO or CCO to implement the Proposal would thus be invalid.

a. The CISO and CCO are Continuing Offices Established by Law

Offices are "established by law" under the meaning of the Appointments Clause when they are "created either by regulations or by statute."[253] The Commission's regulations create the offices of the CISO and CCO: Rule 613 requires the appointment of a Chief Compliance Officer for the CAT

---

250 *Ass'n of American Railroads v. Dept. of Transportation*, supra note 44, at 36.

251 *Lucia v. SEC*, supra note 46, at 2051. The Commission qualifies as an executive branch department under *Lucia.* See id., at note 3.

252 The NMS Plan instructs the Plan Processor to appoint a Chief Compliance Officer and a Chief Information Security Officer, subject to the approval of the Operating Committee by supermajority vote. See CAT NMS Plan Sections 6.2(a)(i) and 6.2(b)(i).

253 See *Free Enterprise Fund v. Pub. Co. Accounting Oversight Bd.*, 561 U.S. 477, 540 (2010) (Breyer, J., dissenting) (interior quotations removed); *United States v. Mouat*, 124 U.S. 303, 307–08 (1888). See also *Willy v. Admin Review Board*, 423 F.3d 483, 491 (5th Cir. 2005) (holding that members of the administrative review board of Department of Labor, whose positions were created by regulation, were officers of the United States).

system,[254] and the CAT NMS Plan—approved by Order of the Commission—requires the appointment of a Chief Information Security Officer.[255] In addition, Commission regulations detail the duties and functions of the two offices.[256] Under Rule 613 and the NMS Plan, the CISO and CCO must regularly review the CAT's operations, make appropriate recommendations,[257] and monitor participant compliance,[258] among other enumerated duties. The Proposal would expand these duties in significant ways, as described in Part IV.B.1 above.[259]

In addition to being "established by law," the offices of the CISO and CCO are also "continuing" under the meaning of the Appointments Clause. Commission regulations bestow on both offices ongoing responsibilities and duties, rather than ad hoc or occasional obligations.[260] The CAT NMS Plan states that both positions are full-time and identified several "regular and frequent" responsibilities for both officials.[261] Notably, although the particular individual serving as the CISO or CCO can be replaced, neither the Plan Processor nor the Operating Committee has the power to eliminate the positions wholesale.[262]

b. The Proposal Grants Significant Authority to the CISO and CCO

---

[254] See 17 CFR 242.613(b)(5) (mandating that the NMS plan "require the appointment of a Chief Compliance Officer to regularly review the operation of the central repository to assure its continued effectiveness in light of market and technological developments, and make any appropriate recommendations for enhancements to the nature of the information collected and the manner in which it is processed").

[255] See 17 CFR 242.613(b)(i); id. at 6.2(a)(i). Cf. Securities Exchange Act, 15 USC 78(d)(b)(1) (granting Commission power to appoint and compensate officers, attorneys, economists, examiners, and other employees).

[256] See *Freytag v. C.I.R.*, 501 U.S. 868, 882 (1991) (citing *Burnap v. United States*, 252 U.S. 512, 516–17 (1920) and *United States v. Germaine*, 99 U.S. 508, 511–12 (1878)) (finding a position to be established by law where the law specifies the offices' duties, salary, and means of appointment).

[257] See 17 CFR 242.613(5)(b).

[258] See CAT NMS Plan Section 6.2(a)(v)(J).

[259] See Proposal, at 66097-66100 (proposed Sections 6.1(a)(v)(R), 6.1(a)(v)(S), 6.1(b)(v)(F)(viii), 6.1(b)(v)(F)(ix), 6.13(d)(i)(B), 6.13(d)(i)(B)), and 6.6(b)(ii)(B)(3)).

[260] See *United States v. Germaine*, supra note 256, at 511–12 (surgeon with occasional and intermittent duties is not an "Officer of the United States"); *Auffmordt v. Hedden*, 137 U.S. 310, 326–27 (1890) (similar conclusion regarding merchant appraiser with occasional and temporary duties).

[261] See CAT NMS Plan, Appendix C-(A)(4)(a); and id., Section 4.6(a) ("The Chief Compliance Officer shall work on a regular and frequent basis with the Compliance Subcommittee.").

[262] That the offices of the CISO and CCO are housed within the Plan Processor, a private entity, does not place them outside the scope of the Appointments Clause. See, e.g., *Officers of the United States Within the Meaning of the Appointments Clause*, 31 Op. O.L.C. 73, 114 (2007) (rejecting prior conclusion that qui tam relator was not an Officer of the United States simply because he was not employed by federal government).

An official is subject to the Appointments Clause if the official possesses "significant discretion in carrying out important functions."[263] The CISO and CCO would meet that test if the Proposal were adopted, because the proposed amendments would empower the CISO and CCO to exercise wide-ranging discretion over the SROs' access to CAT data. Without advance approval from the Commission (or any other authority), the CISO and CCO would determine whether and when an SRO may extract data in a Non-SAW environment, whether SROs are in compliance with security requirements, and whether SROs may take other actions as described in Part IV.B.1 above.

These powers distinguish the CISO and CCO from private parties who are obligated to act under federal law but are not Officers of the United States. An officer, unlike an employee or a contractor, performs a "significant *governmental* duty" [264] involving the "administration and enforcement of the public law."[265] The CISO and CCO do not merely exercise private authority pursuant to a statutory or regulatory obligation. Rather, by controlling SROs' access to CAT Data and safeguarding the sensitive materials contained within, the CISO and CCO in essence exercise federal regulatory authority over private companies, on behalf of the Commission, for the benefit of the public.

Because the CISO and CCO would exercise "significant authority pursuant to the laws of the United States" in a "continuing" office "established by law" under the Proposal, the Appointments Clause would require that they be appointed by the Commission, the courts, or the President. But under the Commission's regulations, the CISO and CCO are both appointed by the Plan Processor, with the approval of the Operating Committee.[266] So far as the NYSE Exchanges are aware, the Commission is not involved in the selection of the CISO and CCO and does not exercise final approval power. While the Operating Committee does send notice to the Commission after the CISO and CCO have been appointed,[267] the Commission's mere receipt of this notice is insufficient to comply with the Appointments Clause.

Finally, because the CISO and CCO would be unlawfully appointed if the Proposal were adopted, any steps they took to implement the Proposal would be invalid and without effect. The Commission should remedy this problem by withdrawing the Proposal, or at a minimum structuring any changes to the CAT NMS Plan in a way that avoids delegating substantial new authority to the CISO and CCO.

V. The Proposed Implementation Periods are Unrealistic.

Assuming the Plan Processor would agree to undertake the Proposal's requirements, the Proposal would make substantial changes to structures, governance, policies, procedures, and environments the Plan Processor and SROs have already created or have in development. The SROs, Plan Processor, CISO, and CCO would have to expend considerable effort in ensuring that the requirements set forth in the Proposal were met and impacts to the implementation of the

---

263 *Lucia v. SEC*, supra note 46, at 2047–48; *Freytag v. C.I.R.*, supra note 256, at 881–82.

264 *Buckley v. Valeo*, 424 U.S. 1, 141 (1976) (emphasis added).

265 Id. at 139.

266 See CAT NMS Plan Sections 6.2(a)(i) and 6.2(b)(i).

267 See id.

Proposal's requirements as well as to the development and operation of the CAT itself would be all but inevitable.

Based on experience, the NYSE disagrees with the implementation periods set out in the Proposal. Those periods would not provide the various entities and individuals with sufficient time to meet the Proposal's demands, and each of the described tasks are too significant, consequential, and risky, to rush through. The Plan Processor and SROs should not adopt incomplete or cursory policies, procedures, or designs, or incur operational incidents—any of which could adversely affect the security and confidentiality of the CAT and CAT Data—simply to meet ill-conceived, arbitrary deadlines. Nonetheless, the Proposal offers no real explanations for its proposed timeline, cites no feasibility study with respect to costs or implementation, and gives no meaningful consideration to the myriad risks and concerns discussed above.

First, the Proposal posits that 90 days would be sufficient for the SROs and Plan Processor to complete specific tasks:

> the Commission believes this timeframe would provide sufficient time for the Participants to collectively develop and approve the Proposed Confidentiality Policies . . ., as well as to develop and establish their own procedures and usage restrictions related to these policies. The Commission also believes that a 90-day timeframe would provide sufficient time for the Plan Processor to implement SAW-specific policies and procedures for the CISP pursuant to proposed Sections 6.12 and 6.13(a), and to develop detailed design specifications for the SAWs pursuant to proposed Section 6.13(b) . . . . In addition, the Commission believes that the 90-day timeframe would provide sufficient time for the Plan Processor to make necessary programming changes to implement the new logging requirements contained in proposed Appendix D, Section 8.1.1. [268]

With respect to the Proposed Confidentiality Policies, the two steps of "collectively develop" and "develop and establish their own procedures" cannot be done in parallel. The collective process in the first step may be lengthy given the number of parties that must agree. A policy that will affect the practices and procedures of every SRO would be crafted through the work of multiple committees, each bringing a different perspective. As previously stated, SROs are unique and there are substantial differences in their regulatory, security, and risk profiles. Because of these differences, it would require significant time to establish a meaningful Proposed Confidentiality Policy. The effort to make unique needs known and represented, negotiate amongst competitors, the Plan Processor, and Commission staff involved in the process, and determine acceptable policies that are meaningful and feasibly applied across all parties and affiliates would be significant. Moreover, SRO policy governance processes may be purposely designed to be deliberative rather than reactive, and so it may take more than 90 days to approve policy changes incorporating the draft Proposed Confidentiality Policies, especially if board approvals are required. The Proposal does not address a scenario whereby these policy changes could be rejected by SRO boards and governing bodies.

The Proposal would direct the SROs to create and approve the required policies, procedures, and design specifications, carry out the required programming changes, and integrate all of these changes into existing policies and procedures in one of the most sensitive areas of the system within an artificially short deadline of 90 days. As a result, the Proposal would increase the

---

[268] Proposal, at 66053.

likelihood of producing sub-optimal results and introduce the risk of establishing protocols that staff cannot fully comply with, due to having insufficient time to analyze and test the proposals and train staff on the changes. Further, all of this work to attempt to meet the deadline would detract from the ongoing effort to build and implement the CAT itself.

The Commission states that it believes that 90 days would be sufficient for the Plan Processor to implement SAW-specific policies and develop detailed design specifications for the SAWs "because the Plan Processor is already familiar with the security requirements necessary to protect CAT Data and would merely be extending these requirements to the SAWs for the purposes of implementation and creating a roadmap for Participants to follow via the design specifications."[269] This is incorrect. The SAWs would not merely be extensions of the current security requirements and CAT environments. The proposed SAWs fundamentally change the scope of what is housed within CAT environments, and therefore the Plan Processor's CAT perimeter, and the associated means of protecting that scope. Ninety days would not provide the Plan Processor with sufficient time to collaborate with the SROs, ESWG, and Operating Committee to create designs for SAWs that were sufficiently flexible and durable to handle all of the demands that would be put on them, including to incorporate SRO non-CAT data and regulatory surveillances without detriment to the operation of those systems and handle the increased risk and corresponding security problems discussed above. The SAWs would be the cornerstones of the CAT: it would be imprudent to rush their design to meet an arbitrary deadline.

*Second, t*he Proposal suggests that an implementation period of 120 days from the effective date would be sufficient for the Plan Processor to establish the SROs' SAWs, "because the Plan Processor has already been authorized to build similar environments for some of the Participants since November 2019."[270] It adds that the Plan Processor will have a head start on the interim elements of SAW implementation, "to the extent that the Plan Processor has already developed design specifications and implemented the policies and procedures for the SAWs within the 90-day timeframe following the effective date of the amendment . . . ."[271]

One hundred twenty days for the Plan Processor to establish the SRO SAWs would be woefully inadequate, even if the SAWs were similar to the current SRO environments. In reality, the current tailored environments will be substantially different from the Proposal's SAWs, which must accommodate all SROs' regulatory systems and non-CAT data, making 120 days even less sufficient. The design of the current environments is not be appropriate for a SAW that has to support the non-CAT data and regulatory surveillance that would be introduced if all SROs were required to use the SAW, and 120 days would not be sufficient to securely re-design, develop, and validate the proposed SAW.

As just one example of how 120 days would not be sufficient, consider that the proposed SAWs are likely to require regulatory system developments. To the NYSE's knowledge, FINRA is the only SRO with the infrastructure in place to use a data access system similar to the Direct Read access expected to be used for the bulk of the data access in the SAWs. To build a similar infrastructure

---

269 Id.

270 Id.

271 Id.

around Direct Read is estimated to take at least several person years of effort and at least several months of real time.

Third, the Commission proposes to set 180 days from the effective date as the deadline for the for the SROs to either comply with the SAW requirements or obtain an exemption. In other words, the Commission posits that 60 days from finalization of the SAW design specifications would be sufficient "for the Participants to (1) build internal architecture for their SAWs and customize their SAWs with the desired analytical tools, (2) import external data into their SAWs as needed, and (3) demonstrate their compliance with the SAW design specifications."[272] It would be unrealistic to think that 60 days would be sufficient to not just build the SAWs, but also conduct proper security testing, validate the proper functioning of surveillance functions, and train staff to work in the SAW—much less import the data and regulatory surveillance functions that would be required. SROs may have to transfer into their SAWs PII and proprietary third-party data obtained from sources other than the CAT, any transaction data not required to be reported to the CAT, surveillance programs and patterns, surveillance exceptions, investigation records, and a case management system. This means that sensitive and proprietary information, including the granular details of surveillance patterns, code, alerts, and investigations, as well as SRO-specific data needed for surveillance, would be required to move to the SAW.

The Commission contends that the timeframe is sufficient to seek an exemption allowing for a Non-SAW environment, as SROs would have 30 days from finalization of the SAW design to gather the application materials they must submit to the CISO, CCO, and SWG. The CISO and CCO would then issue a determination within 60 days of receipt.[273] A review of the requirements for the application materials shows that the 30 days would be insufficient.

First, the materials would have to include a security assessment of the proposed Non-SAW environment, conducted within the previous 12 months by a named independent third-party security assessor, that:

> (a) demonstrates the extent to which the non-SAW environment complies with the NIST SP 800–53 security controls and associated policies and procedures required by the [CISP] . . ., (b) explains whether and how the Participant's security and privacy controls mitigate the risks associated with extracting CAT Data to the non-SAW environment through user-defined direct query or bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2, and (c) includes a Plan of Action and Milestones document detailing the status and schedule of any corrective actions recommended by the assessment.[274]

Second, the application would have to include detailed design specifications for the Non-SAW environment "demonstrating: (a) the extent to which the non-SAW environment's design specifications adhere to the design specifications developed by the Plan Processor for SAWs . . .

---

[272] Id.

[273] Id.

[274] Id., at 66099 (proposed Section 6.12(d)(i)(A)(1)).

and (b) that the design specifications will enable the operational requirements set forth for non-SAW environments . . . ."[275]

For most SROs, review of a proposed Non-SAW environment could not occur within the timeline allotted by the Proposal. SRO environments existing as of the date that the SAW design was finalized likely would not comply with the requirements for a SAW, since those requirements did not exist previously. A new Non-SAW environment, or adjustments to an existing environment to have it meet the requirements for a Non-SAW environment, would have to be designed, and detailed design specifications with the required demonstrations would have to be drafted, reviewed, tested, approved, and validated, all of which would require substantially more than 30 days. In addition, even if an SRO had environments that could meet the Non-SAW design requirements running on the day the SAW design was finalized, it is doubtful that an independent third party security assessor could conduct a thorough review and prepare the requested report within 30 days. For perspective, even small to medium technology changes, such as configuration or infrastructure changes or code releases with minimal scope, must adhere to an organization's software development lifecycle procedures. Average technology implementations take longer than 30 days. It is just not feasible that all the required steps could be completed within the 30 days after the SAW designs are completed.

Moreover, if the Plan Processor missed its deadline to produce design specifications for the SAWs, that would not alter the Proposal's 180 day deadline for the Non-SAWs, making it more likely that the SROs would miss the deadline through no fault of their own.

The concerns about the implementation timelines are not trivial. Given the penalties for failing to meet the deadlines set forth in the recent Financial Accountability Amendment, unrealistic timelines for implementation of the Proposal's new requirements could further jeopardize the overall implementation timeframe of the CAT and could lead to substantial financial penalties for the SROs.[276] The Proposal does not adequately consider this impact of its proposed implementation time nor the potential costs that could result if the SROs miss a deadline outlined in the Financial Accountability Amendment.

* * * * *

For the reasons set forth above, the NYSE respectfully requests that the Proposal be withdrawn.

Respectfully submitted,

Elizabeth K. King

---

[275] Id.

[276] For a discussion of these costs, see Part II.B.2, above.

Cc: Honorable Jay Clayton, Chairman
Honorable Caroline A. Crenshaw, Commissioner
Honorable Hester M. Peirce, Commissioner
Honorable Elad L. Roisman, Commissioner
Honorable Allison Herren Lee, Commissioner
Brett Redfearn, Director, Division of Trading and Markets