SECURITIES AND EXCHANGE COMMISSION

[Release No. 34–89632; File No. S7–10–20]

RIN 3235–AM62

Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail To Enhance Data Security

AGENCY: Securities and Exchange Commission.

ACTION: Proposed amendments to national market system plan.

SUMMARY: The Securities and Exchange Commission is proposing amendments to the national market system plan governing the consolidated audit trail. The proposed amendments are designed to enhance the security of the consolidated audit trail.

DATES: Comments should be received on or before November 30, 2020.

ADDRESSES: Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission's internet comment form (*http://www.sec.gov/rules/proposed.shtml*); or
- Send an email to *rule-comments@sec.gov*. Please include File No. S7–10–20 on the subject line.

Paper Comments

- Send paper comments to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549–1090.

All submissions should refer to File No. S7–10–20. This file number should be included on the subject line if email is used. To help us process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's internet website (*http://www.sec.gov/rules/proposed.shtml*). Comments are also available for website viewing and printing in the Commission's Public Reference Room, 100 F Street NE, Washington, DC 20549 on official business days between the hours of 10:00 a.m. and 3:00 p.m. All comments received will be posted without change. Persons submitting comments are cautioned that the Commission does not redact or edit personal identifying information from comment submissions. You should submit only information that you wish to make available publicly.

Studies, memoranda, or other substantive items may be added by the Commission or staff to the comment file during this rulemaking. A notification of the inclusion in the comment file of any such materials will be made available on the Commission's website. To ensure direct electronic receipt of such notifications, sign up through the ''Stay Connected'' option at *www.sec.gov* to receive notifications by email.

FOR FURTHER INFORMATION CONTACT: Erika Berg, Special Counsel, at (202) 551–5925, Jennifer Colihan, Special Counsel, at (202) 551–5642, Rebekah Liu, Special Counsel, at (202) 551–5665, Susan Poklemba, Special Counsel, at (202) 551–3360, Andrew Sherman, Special Counsel, at (202) 551–7255, Gita Subramaniam, Attorney Advisor, at (202) 551–5793, or Eugene Lee, Attorney Advisor, at (202) 551–5884, Division of Trading and Markets, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549–7010.

SUPPLEMENTARY INFORMATION: The Commission is proposing amendments to the CAT NMS Plan.

TABLE OF CONTENTS

I. Background

In July 2012, the Securities and Exchange Commission (the ''Commission'') adopted Rule 613 of Regulation NMS, which required national securities exchanges and national securities associations (the ''Participants'') [1] to jointly develop and submit to the Commission a national market system plan to create, implement, and maintain a consolidated audit trail (the ''CAT'').[2] 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. On November 15, 2016, the Commission approved the national market system plan required by Rule 613 (the ''CAT NMS Plan'').[3]

The security and confidentiality of CAT Data [4] has been—and continues to be—a top priority of the Commission. The CAT NMS Plan approved by the Commission already sets forth a number of requirements regarding the security and confidentiality of CAT Data. The CAT NMS Plan states, for example, that the Plan Processor [5] shall be responsible for the security and confidentiality of all CAT Data received and reported to the Central Repository.[6] In furtherance of this directive, the CAT NMS Plan requires the Plan Processor to develop and maintain an information security program for the Central Repository. The Plan Processor must have appropriate solutions and controls in place to address data confidentiality and security during all communication between CAT Reporters,[7] Data Submitters,[8] and the Plan Processor; data extraction, manipulation, and transformation; data loading to and from the Central Repository; and data maintenance by the CAT System.[9] The CAT NMS Plan also sets forth minimum data security requirements for CAT that the Plan Processor must meet, including requirements governing connectivity and data transfer, data encryption, data storage, data access, breach management, data requirements for personally identifiable information (''PII''),[10] and applicable data security industry standards.[11] CAT Data reported to and retained in the Central Repository is thus subject to what the Commission believes are stringent security policies, procedures, standards, and controls. Nevertheless, the Commission believes that it can and should take additional steps to further protect the security and confidentiality of CAT Data. Therefore, the Commission proposes to amend the CAT NMS Plan to enhance the security of the CAT and the protections afforded to CAT Data.

Specifically, the Commission proposes to amend the CAT NMS Plan to: (1) Define the scope of the current

[1] The Participants include BOX Exchange LLC, Cboe BYX Exchange, Inc., Cboe BZX Exchange, Inc., Cboe C2 Exchange, Inc., Cboe EDGA Exchange, Inc., Cboe EDGX Exchange, Inc., Cboe Exchange, Inc., Financial Industry Regulatory Authority, Inc., Investors' Exchange LLC, Long-Term Stock Exchange, Inc., MEMX LLC, Miami International Securities Exchange LLC, MIAX Emerald, LLC, MIAX PEARL, LLC, Nasdaq BX, Inc., Nasdaq GEMX, LLC, Nasdaq ISE, LLC, Nasdaq MRX, LLC, Nasdaq PHLX LLC, The Nasdaq Stock Market LLC, New York Stock Exchange LLC, NYSE American LLC, NYSE Arca, Inc., NYSE Chicago, Inc., and NYSE National, Inc.

[2] *See* Securities Exchange Act Release No. 67457 (July 18, 2012), 77 FR 45722 (August 1, 2012) (''Rule 613 Adopting Release'').

[3] Securities Exchange Act Release No. 78318 (November 15, 2016), 81 FR 84696, (November 23, 2016) (''CAT NMS Plan Approval Order''). The CAT NMS Plan is Exhibit A to the CAT NMS Plan Approval Order. *See* CAT NMS Plan Approval Order, at 84943–85034. The CAT NMS Plan functions as the limited liability company agreement of the jointly owned limited liability company formed under Delaware state law through which the Participants conduct the activities of the CAT (the ''Company''). Each Participant is a member of the Company and jointly owns the Company on an equal basis. The Participants submitted to the Commission a proposed amendment to the CAT NMS Plan on August 29, 2019, which they designated as effective on filing. Under the amendment, the limited liability company agreement of a new limited liability company named Consolidated Audit Trail, LLC serves as the CAT NMS Plan, replacing in its entirety the CAT NMS Plan. *See* Securities Exchange Act Release No. 87149 (September 27, 2019), 84 FR 52905 (October 3, 2019).

[4] ''CAT Data'' is a defined term under the CAT NMS Plan and means ''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.'' *See* CAT NMS Plan, *supra* note 3, at Section 1.1.

[5] ''Plan Processor'' is a defined term under the CAT NMS Plan and means ''the Initial Plan Processor or any other Person selected by the Operating Committee pursuant to SEC Rule 613 and Sections 4.3(b)(i) and 6.1, and with regard to the Initial Plan Processor, the Selection Plan, to perform the CAT processing functions required by SEC Rule 613 and set forth in this Agreement.'' *See id.*

[6] *See id.* at Section 6.5(f)(i). ''Central Repository'' is a defined term under the CAT NMS Plan and means ''the repository responsible for the receipt, consolidation, and retention of all information reported to the CAT pursuant to SEC Rule 613 and this Agreement.'' *See id.*

[7] ''CAT Reporter'' is a defined term under the CAT NMS Plan and means ''each national securities exchange, national securities association and Industry Member that is required to record and report information to the Central Repository pursuant to SEC Rule 613(c).'' *See id.*

[8] ''Data Submitter'' is a defined term under the CAT NMS Plan and means ''national securities exchanges, national securities associations, broker-dealers, the SIPs for the CQS, CTA, UTP and Plan for Reporting of Consolidated Options Last Sale Reports and Quotation Information (''*OPRA*'') Plans, and certain other vendors or appropriate third parties.'' *See id.* at Appendix C, Section A(1)(a).

[9] *See id.* at Appendix D, Section 4.1. ''CAT System'' is a defined term in the CAT NMS Plan and means ''all data processing equipment, communications facilities, and other facilities, including equipment, utilized by the Company or any third parties acting on the Company's behalf in connection with operation of the CAT and any related information or relevant systems pursuant to [the CAT LLC Agreement].'' *See* CAT NMS Plan, *supra* note 3, at Section 1.1.

[10] ''PII'' is a defined term under the CAT NMS Plan and means ''personally identifiable information, including a social security number or tax identifier number or similar information; Customer Identifying Information and Customer Account Information.'' *See id.* at Section 1.1.

[11] *See id.* at Section 6.12; *see also id.* at Appendix D, Section 4.

information security program; (2) require the Operating Committee [12] to establish and maintain a security-focused working group; (3) 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 that will enable Participants to use the user-defined direct query and bulk extract tools in other environments; (4) limit the amount of CAT Data that can be extracted from the Central Repository outside of a secure analytical workspace through the online targeted query tool described in Section 6.10(c)(i)(A) of the CAT NMS Plan and require the Plan Processor to implement more stringent monitoring controls on such data; (5) impose requirements related to the reporting of certain PII; (6) define the workflow process that should be applied to govern access to customer and account attributes that will still be reported to the Central Repository; (7) modify and supplement existing requirements relating to Participant policies and procedures regarding the confidentiality of CAT Data; (8) refine the existing requirement that CAT Data be used only for regulatory or surveillance purposes; (9) codify existing practices and enhance the security of connectivity to the CAT infrastructure; (10) require the formal cyber incident response plan to incorporate corrective actions and breach notifications; (11) amend reporting requirements relating to Firm Designated IDs and Allocation Reports; and (12) clarify that Appendix C of the CAT NMS Plan has not been updated to reflect subsequent amendments to the CAT NMS Plan. The proposed amendments are discussed in more detail below.

II. Description of Proposed Amendments

A. Comprehensive Information Security Program

Section 6.12 of the CAT NMS Plan requires the Plan Processor to develop and maintain an information security program for the Central Repository that, at a minimum, meets the security requirements set forth in Section 4 of Appendix D to the CAT NMS Plan.[13] Section 4 of Appendix D sets out information security requirements that cover ''all components of the CAT System'' and is not limited to the Central Repository.[14] The Commission preliminarily believes that the scope of the information security program referenced in Section 6.12 of the CAT NMS Plan should be more explicitly defined to apply to the CAT System, as well as to the Plan Processor.

Accordingly, the Commission proposes to add the term ''Comprehensive Information Security Program'' (the ''CISP'') to Section 1.1 of the CAT NMS Plan and to define this term to mean the ''organization-wide and system-specific controls and related policies and procedures required by NIST SP 800–53 [15] that address information security for the information and information systems of the Plan Processor and the CAT System, including those provided or managed by an external organization, contractor, or source.'' The proposed definition would further state that the CISP will also apply to Secure Analytical Workspaces, new environments within the CAT System to which CAT Data may be downloaded.[16] The Commission also proposes to make corresponding changes to Section 6.12 of the CAT NMS Plan. Specifically, the Commission proposes to rename Section 6.12 as ''Comprehensive Information Security Program'' [17] and to delete the phrase ''for the Central Repository'' in Section 6.12.[18]

The Commission preliminarily believes that these proposed amendments are appropriate to set forth all elements of the information security program that must be developed and maintained by the Plan Processor and approved and reviewed at least annually by the Operating Committee.[19] While Section 6.12 of the CAT NMS Plan currently refers to the Central Repository, as noted above, Section 4 of Appendix D refers to information security program requirements that apply more broadly to the entire CAT System [20] and also references the NIST SP 800–53 standard as one that must be followed by the Plan Processor.[21] NIST SP 800–53 defines and recommends security controls, policies, and procedures that should be employed as part of a well-defined risk management process for organizational-level information security programs, including personnel security controls.[22] NIST SP 800–53, which sets forth security and privacy controls for federal information systems and organizations, requires the establishment of information security and risk management due diligence on an organizational level.[23] 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.

As explained above, the proposed amendments, by referencing NIST SP

[12] ''Operating Committee'' is a defined term in the CAT NMS Plan and means ''means the governing body of the Company designated as such and described in Article IV.'' *See id.* at Section 1.1.

[13] *See id.* at Appendix D, Section 4 (Data Security). In Appendix D, Section 4, the Plan sets out the basic solutions and controls that must be met to ensure the security and confidentiality of CAT Data. Such requirements relate to Connectivity and Data Transfer (Section 4.1.1); Data Encryption (Section 4.1.2); Data storage and Environment (Section 4.1.3); Data Access (Section 4.1.4); Breach Management (Section 4.1.5); PII Data Requirements (Section 4.1.6); and Industry Standards (Section 4.2).

[14] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 4 (''The Plan Processor must provide to the Operating Committee a comprehensive security plan that covers *all components of the CAT System,* including physical assets and personnel . . . .'' (emphasis added)).

[15] *See* Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800–53 Revision 4, National Institute of Standards and Technology, U.S. Dep't of Commerce (April 2013), *available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf* (''NIST SP 800–53'').

[16] *See* Part II.C. *infra,* for a discussion of the definition of ''Secure Analytical Workspace'' and the specific CISP requirements that would apply to such environments under proposed Section 6.13.

[17] Similar changes have been made throughout the CAT NMS Plan, at proposed Section 6.2(a)(v)(H), proposed Section 6.5(f)(i)(C), proposed Section 6.6(b)(ii)(B)(3), and proposed Section 4.1 of Appendix D.

[18] A similar change has been made at proposed Section 6.5(f)(i)(C) to replace a reference to the Central Repository with a reference to the CAT System.

[19] To the extent that the CISP would be made up of multiple policies, procedures, or other documents, the Commission preliminarily believes that the Operating Committee could review each document on an independent or rolling timeline, rather than reviewing all components of the CISP at the same time.

[20] *See* note 14 *supra.*

[21] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 4.2.

[22] *See* NIST SP 800–53, at 1, *supra* note 15.

[23] *See, e.g., id.* at vi, x–xii. *See also, e.g., id.* at 1 (''The security controls defined in this publication and recommended for use by organizations to satisfy their information security requirements should be employed as part of a well-defined risk management process that supports organizational information security programs.'').

800–53 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.[24] 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.[25] Appendix D, Section 4.1 of the CAT NMS Plan currently requires a comprehensive security plan, including information security requirements, that covers the entire CAT System, and the CAT System, as currently defined, encompasses the data processing equipment, communications facilities, and other facilities utilized by external parties acting on the Company's behalf in connection with the operation of the CAT.[26] The proposed amendments would consolidate these requirements into one definition and 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. As noted above, this is already a requirement under Appendix D, Section 4 of the CAT NMS Plan, which states 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.[27] Nevertheless, the Commission preliminarily believes that including an explicit reference to NIST SP 800–53 in the proposed definition of the CISP will reinforce that fact.

The Commission preliminarily believes that these changes should improve the security of the CAT by defining the scope of the information security program required to be developed and maintained by the Plan Processor to be sufficiently clear and to account for the entire CAT, with accompanying personnel security controls for all Plan Processor staff and relevant personnel from external organizations, contractors or other sources, and for all relevant information systems or environments.

The Commission requests comment on the proposed definition of the CISP and the proposed corresponding changes to the CAT NMS Plan. Specifically, the Commission solicits comment on the following:

1. Is the proposed definition for the CISP necessary? Is it already clear that the information security requirements described in Section 6.12 and Appendix D, Section 4 apply at an organizational level to the Plan Processor, to external parties acting on behalf of the Company to support CAT operations, and to all information systems or environments that are within the CAT System, including Secure Analytical Workspaces? Is it already clear that the information security requirements described in Section 6.12 and Appendix D, Section 4 must incorporate the controls, policies, and procedures required by NIST SP 800–53?

2. Should the proposed definition for the CISP be expanded or modified? Are there other personnel, information systems, organizations, or environments that should be covered by the CISP? If so, please specifically identify those personnel, information systems, organizations, or environments and explain why it would be appropriate to include them in the definition of the CISP.

3. Should additional references in the CAT NMS Plan related to the information security program be conformed to refer to the CISP? Should proposed Section 6.12 refer to any other provisions of the CAT NMS Plan in addition to Section 4 of Appendix D and Section 6.13? If so, please identify those provisions and explain why it would be appropriate to incorporate a reference to such provisions in proposed Section 6.12.

B. Security Working Group

To provide support and additional resources to the Chief Information Security Officer of the Plan Processor (the ''CISO'')[28] and the Operating Committee of the CAT NMS Plan, the proposed amendments would require the Operating Committee to establish and maintain a security working group composed of the CISO and the chief information security officer or deputy chief information security officer of each Participant (the ''Security Working Group'').[29] Commission staff would be permitted to attend all meetings of the Security Working Group as observers, and the CISO and the Operating Committee would further be allowed to invite other parties to attend specific meetings.[30] The proposed amendments would specify that the purpose of the Security Working Group shall be to advise the CISO and the Operating Committee,[31] 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

[24] Under the proposed amendments, Secure Analytical Workspaces would, by definition, be within the CAT System. *See* proposed Section 1.1, ''Secure Analytical Workspace.'' The inclusion of Secure Analytical Workspaces in the proposed definition of the CISP would therefore not be an expansion, as the current information security program is required to cover the entire CAT System pursuant to Appendix D, Section 4 of the CAT NMS Plan.

[25] For example, the Plan Processor engaged an external contractor to implement and operate the component of the CAT known as the Customer and Account Information System (''CAIS''). The Plan Processor also selected an external cloud provider as the host for the CAT System.

[26] *See* CAT NMS Plan, *supra* note 3, at Section 1.1; *see id.* at Appendix D, Section 4.

[27] *See id.* at Section 6.12, Appendix D, Section 4.2.

[28] ''Chief Information Security Officer'' is a defined term under the CAT NMS Plan and means ''the individual then serving (even on a temporary basis) as the Chief Information Security Officer pursuant to Section 4.6, Section 6.1(b), and Section 6.2(b).'' *See* CAT NMS Plan, *supra* note 3, at Section 1.1. The CISO is an officer of the Company and has a fiduciary duty to the Company. *See id.* at Section 4.6(a), Section 4.7(c). The CISO, among other things, is responsible for creating and enforcing appropriate policies, procedures, and control structures regarding data security. *See id.* at Section 6.2(b)(i) and 6.2(b)(v).

[29] *See* proposed Section 4.12(c).

[30] *See id.* Given the sensitive nature of the issues that would be discussed at meetings of the Security Working Group, the Commission believes that the CISO and the Operating Committee should consider requiring any non-member invitees to sign a non-disclosure agreement or to adhere to some other protocol designed to prevent the release of confidential information regarding the security of the CAT System. Members of the Security Working Group, and any Participant staff that they consult regarding matters before the Security Working Group, would likewise be subject to the confidentiality obligations set forth in Section 9.6 of the CAT NMS Plan. *See, e.g.,* CAT NMS Plan, *supra* note 3, at Section 9.6(a) (stating that information disclosed by or on behalf of the Company or a Participant to the Company or any other Participant (the ''Receiving Party'') shall be maintained by the Receiving Party in confidence with the same degree of care it holds its own confidential information and disclosed to its Representatives on a need-to-know basis and only to those of such Representatives who have agreed to abide by the non-disclosure and non-use provisions of Section 9.6).

[31] The proposed amendments would clearly state that the CISO shall continue to report directly to the Operating Committee in accordance with Section 6.2(b)(iii) of the CAT NMS Plan. *See* proposed Section 4.12(c).

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.[32] In addition, the proposed amendments would require the CISO 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.[33]

The Commission preliminarily believes it is appropriate to require the Operating Committee to formally establish and maintain a Security Working Group.[34] Although a group has already been established by the Operating Committee to discuss the security of the CAT,[35] the Commission preliminarily believes it is important to require the formation of a Security Working Group with a defined set of participants and a defined purpose. The proposed amendments, for example, would require that each Participant's chief information security officer or deputy chief information security officer be a member of the Security Working Group; other security and regulatory experts would not fulfill the requirements of the proposed amendments.[36] The Commission preliminarily believes these membership requirements are appropriate, because the chief information security officer and deputy chief information security officer of each Participant are the parties that are most likely to have general expertise with assessing organizational-level security issues for complex information systems. Moreover, because the Central Repository is a facility of each Participant,[37] the Commission preliminarily believes that the chief information security officer and deputy chief information security officer of each Participant are likely to have specific expertise with assessing organizational-level and system-specific security issues for the CAT System, as well as an interest in making sure that the CAT System and CAT Data are sufficiently protected. The Commission therefore preliminarily believes that requiring the membership of each Participant's chief information security officer or deputy chief information security officer in the Security Working Group should help to provide effective oversight of CAT security issues.

The proposed amendments would permit the CISO and the Operating Committee to invite other parties, including external consultants with expertise in organizational-level or system-specific security or industry representatives, to attend specific meetings. In addition, the proposed amendments would permit Commission observers to attend all meetings. The Commission preliminarily believes these provisions will enable the Security Working Group to obtain a broad spectrum of views and to present such views to the CISO and the Operating Committee on key security issues.

Finally, the proposed amendments would state that the purpose of the group shall be to aid the CISO and the Operating Committee.[38] This is a broad mandate, because the Commission preliminarily believes that the CISO and the Operating Committee would generally benefit from the combined expertise of the Security Working Group on a broad array of matters. To enable the Security Working Group to provide the requisite aid, the proposed amendments would further state that the CISO must apprise the Security Working Group of relevant developments and provide the Security Working Group with all information and materials necessary to fulfill its purpose. This provision is designed to keep the Security Working Group adequately informed about issues that fall within its purview.

The proposed amendments would also require the Security Working Group to aid the CISO and the Operating Committee on certain issues that the Commission preliminarily believes are particularly important. For example, issues involving information technology matters that pertain to the development of the CAT System,[39] the development of the CISP,[40] or emerging cybersecurity topics[41] are likely to present questions of first impression, and it is important that such questions be handled appropriately in the first instance. The Commission preliminarily believes that the involvement of the Security Working Group could be of valuable assistance to the CISO. Similarly, issues involving the maintenance and application of the CISP[42] and the review and application of the confidentiality policies required by proposed Section 6.5(g)[43] relate to two initiatives that would protect the security and confidentiality of CAT Data. These initiatives would control access to and extraction of such data outside the Central Repository and would directly impact how Participants interact with CAT Data within and outside the CAT System.[44] The Commission preliminarily believes that the Security Working Group would be able to provide valuable feedback on these initiatives, which, as explained more fully below, are critical to the security of the CAT because they would govern the development and implementation of the Participants' confidentiality and security policies for handling non-public data generally and CAT Data specifically.[45] The Commission also preliminarily believes that the Security Working Group should aid the CISO in reviewing and analyzing third-party risk assessments conducted pursuant to Section 5.3 of Appendix D, as well as the results and corrective actions arising from such assessments.[46] Given the combined expertise of the Security Working Group, the Commission preliminarily believes that its membership would be uniquely adept at understanding the results, assessing the criticality of findings, prioritizing necessary corrective action, and providing valuable feedback on the plan of action to address any open

[32] *See id.*

[33] *See id.* With respect to this provision, the Commission does not preliminarily believe that members of the Security Working Group would need access to CAT Data to fulfill their function. Nonetheless, because members of the Security Working Group would not be considered ''Regulatory Staff'' under the proposed amendments described in Part II.G.2.a., Security Working Group members would only be able to gain access to CAT Data by following the policies set forth in proposed Section 6.5(g)(i)(E).

[34] *See id.* The Commission proposes a conforming change to the title of this section to make it clear that section will apply to both subcommittees and working groups.

[35] *See* CAT Security Overview: Safeguarding Data Reported to CAT, *available at https://www.catnmsplan.com/wp-content/uploads/2019/08/FINRA-CAT-Security-Approach-Overview_20190828.pdf.*

[36] *See* proposed Section 4.12(c).

[37] *See, e.g.,* CAT NMS Plan, *supra* note 3, at Appendix C (indicating that the CAT will be a facility of each Participant).

[38] The list of issues provided in proposed Section 4.12(c) is not exclusive; it may be appropriate for the Security Working Group to aid the CISO with respect to other issues, and the proposed amendments require the involvement of the Security Working Group on other matters. *See, e.g.,* proposed Section 6.13(d)(i)(A) (requiring a Participant seeking an exception from the proposed Secure Analytical Workspace usage requirements to provide the Security Working Group with specified application materials).

[39] *See* proposed Section 4.12(c)(i).

[40] *See id.* at (c)(ii).

[41] *See id.* at (c)(v).

[42] *See id.* at (c)(ii).

[43] *See id.* at (c)(iii).

[44] *See* Part II.A. *supra,* for a discussion of the proposed CISP and its importance to CAT security; Part II.C. *infra,* for a discussion of data access and extraction policies that would be applied as part of the proposed CISP. *See also* Part II.G. *infra,* for a discussion of the proposed amendments relating to Participants' data confidentiality policies, which would include restrictions on data access and extraction, and their importance to CAT security.

[45] *See id.*

[46] *See* proposed Section 4.12(c)(iv).

issues that might be identified by these assessments.

The Commission requests comment on proposed Section 4.12(c). Specifically, the Commission solicits comment on the following:

4. Should a Security Working Group be formally established and maintained?

5. The proposed amendments require the Security Working Group to be composed of the CISO and the chief information security officer or deputy chief information security officer of each Participant. Do commenters agree that the chief information security officer or deputy chief information security officer of each Participant is likely to be best informed regarding security issues that might affect the CAT? Should any other parties be included as required members of the Security Working Group? If so, please identify these parties and explain why it would be appropriate to include them. For example, should representatives from the Advisory Committee established by Section 4.13 of the CAT NMS Plan be added as required members to the Security Working Group? Should the CISO and the Operating Committee be permitted to invite other parties to attend specific meetings? Should any limitations be placed on the kinds of parties the CISO and the Operating Committee may invite? For example, should the CISO and the Operating Committee be limited to inviting personnel employed by the Participants, because such personnel would already be subject to the confidentiality obligations set forth in Section 9.6 of the CAT NMS Plan for Representatives? If not, should external parties invited by the CISO and the Operating Committee be explicitly required by proposed Section 4.12(c) to sign a non-disclosure agreement or to comply with any other kind of security protocol in order to prevent the disclosure of confidential information regarding the security of the CAT System? If so, please identify the security protocol such parties should comply with and explain why such protocol would be effective.

6. The proposed amendments state that the Security Working Group's purpose is to advise the CISO and the Operating Committee. Is that an appropriate mandate? If not, please identify a mandate that would be appropriate and explain why it is a better mandate for the Security Working Group. Should the Security Working Group advise the Plan Processor or some other party, instead of the CISO and the Operating Committee?

7. Will the proposed amendments keep the Security Working Group apprised of relevant information or developments? Should the proposed amendments require the CISO and/or the Operating Committee to consult the Security Working Group only on certain matters? If so, please identify these matters and explain why it would be appropriate to require the CISO and/or the Operating Committee to consult the Security Working Group only on such matters. Should the proposed amendments require periodic meetings among the CISO, the Operating Committee and the Security Working Group? If so, how often should such meetings occur and why? Should the proposed amendments require the Security Working Group to provide the CISO and/or the Operating Committee with feedback on a regular basis?

8. The proposed amendments include a non-exhaustive list of specific issues that would be within the purview of the Security Working Group. Should this list include any additional matters? Should any of these matters be removed from this list or amended?

C. Secure Analytical Workspaces

The CAT NMS Plan must sufficiently enable regulators to access and extract CAT Data in order to achieve specific regulatory purposes. The CAT NMS Plan currently describes various means by which regulators may access and extract CAT Data. Section 6.5(c) of the CAT NMS Plan, for example, requires the Plan Processor to provide regulators access to the Central Repository for regulatory and oversight purposes and to create a method of accessing CAT Data that enables complex searching and report generation. Section 6.10(c) of the CAT NMS Plan specifies two methods of regulator access: (1) An online targeted query tool with predefined selection criteria to choose from; and (2) user-defined direct queries and bulk extracts of data via a query tool or language allowing querying of all available attributes and data sources.[47] The CAT NMS Plan also specifies how regulators may download the results obtained in response to these queries. For example, with respect to the online targeted query tool, the CAT NMS Plan provides that, ''[o]nce query results are available for download, users are to be given the total file size of the result set and an option to download the results in a single or multiple file(s). Users that select the multiple file option will be required to define the maximum file size of the downloadable files. The application will then provide users with the ability to download the files. This functionality is provided to address limitations of end-user network environment[s] that may occur when downloading large files.'' [48] With respect to the user-defined direct queries and bulk extracts of data, the CAT NMS Plan provides that ''[t]he Central Repository must provide for direct queries, bulk extraction, and download of data for all regulatory users. Both the user-defined direct queries and bulk extracts will be used by regulators to deliver large sets of data that can then be used in internal surveillance or market analysis applications.'' [49]

To better protect CAT Data, the Commission preliminarily believes that efforts should be taken to minimize the attack surface associated with CAT Data; to 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 to leverage, wherever possible, security controls and related policies and procedures that are consistent with those that protect the Central Repository.

The Commission preliminarily believes that these objectives can be met by requiring the creation and use of Secure Analytical Workspaces (''SAWs'') that would be part of the CAT System and therefore subject to the CISP.[50] The proposed amendments would define a ''Secure Analytical Workspace'' as ''an analytic environment account that is part of the CAT System, and subject to the Comprehensive Information Security Program, where CAT Data is accessed and analyzed as part of the CAT System pursuant to [proposed] Section 6.13. The Plan Processor shall provide a SAW account for each Participant that implements all common technical security controls required by the Comprehensive Information Security Program.'' [51] The Commission also proposes to add a new Section 6.13 to the CAT NMS Plan to set forth the requirements that would apply to SAWs. The Commission understands that the Participants have recently

[47] *See* CAT NMS Plan, *supra* note 3, at Section 6.10(c)(i); *see also id.* at Appendix D, Section 8.1 through Section 8.2. Section 6.10(c) also requires the Plan Processor to reasonably assist regulatory staff with queries, to submit queries on behalf of regulatory staff (including regulatory staff of Participants) as reasonably requested, and to maintain a help desk to assist regulatory staff with questions about the content and structure of CAT Data. *Id.* at Section 6.10(c)(iv) through (vi).

[48] *See id.,* at Appendix D, Section 8.1.1.

[49] *See id.,* at Appendix D, Section 8.2.

[50] In addition, the Commission also preliminarily believes that certain limitations on the downloading capabilities of the online targeted query tool will help to achieve these objectives. *See* Part II.D. *infra,* for a discussion of these proposed limitations.

[51] *See* proposed Section 1.1, ''Secure Analytical Workspace.''

authorized the Plan Processor to build similar environments for some of the Participants and that each Participant would be responsible for the implementation of its own security controls.[52] The Commission preliminarily believes that it would be beneficial to require that the Plan Processor provide SAW accounts to be used by all Participants in certain circumstances and to formally codify the functionality available in and the security controls applicable to SAWs. The Commission preliminarily believes that this approach will best enable the implementation of the SAWs with a consistent and sufficient level of security.

Accordingly, the Commission is proposing amendments to the CAT NMS Plan that will specify: (1) The provision of the SAW accounts; (2) data access and extraction policies and procedures, including SAW usage requirements; (3) security controls, policies, and procedures for SAWs; (4) implementation and operational requirements for SAWs; and (5) exceptions to the SAW usage requirements. These proposed amendments are discussed in further detail below.

1. Provision of SAW Accounts

The proposed amendments would require each Participant to use a SAW for certain purposes,[53] but the proposed definition of ''Secure Analytical Workspace'' and proposed Section 6.1(d)(v) make it clear that Participants would not build their own SAWs within the CAT System or implement the technical security controls required by the CISP. Rather, the proposed amendments state that the ''Plan Processor shall provide a SAW account for each Participant that implements all common technical security controls required by the Comprehensive Information Security Program.'' [54]

The Commission preliminarily believes that requiring the Plan Processor to provide SAW accounts to the Participants that implement all common technical security controls required by the CISP is the most effective way to achieve a consistent level of security across multiple SAWs and between SAWs.[55] The 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. By centralizing provision of the SAW accounts with the Plan Processor, the common technical controls associated with the CISP should be built consistently and in a way that newly enables the Plan Processor to conduct consistent and comprehensive monitoring of analytic environments employed by Participants to access and analyze CAT Data—a task the Plan Processor is not currently able to perform.[56]

The Plan Processor is the party most familiar with the existing information security program and would be the party most familiar with the security controls, policies, and procedures that would be required under the proposed CISP. The Commission preliminarily believes this familiarity would enable the Plan Processor to build the required security controls more efficiently and more effectively than if each Participant were responsible for its own SAW account.[57] 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 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.[58]

The Commission also preliminarily believes that centralizing provision of the SAW accounts with the Plan Processor is the most efficient approach.[59] Given the size of the CAT database that the Plan Processor already manages in a cloud environment, the Plan Processor is in a position to leverage economies of scale and, possibly, to obtain preferential pricing in establishing SAW accounts with the same cloud provider and in the same cloud environment.[60] Having the Plan Processor be responsible for the provision of all SAW accounts could also make administration of SAW security easier. For example, cloud environments offer features that enable security-related administrative functions to be performed simultaneously and consistently across multiple accounts. Such features could also be leveraged by the Plan Processor to extend its existing information security controls for the Central

[52] *See* Letter from Michael Simon, CAT NMS Plan Operating Committee Chair, to Hon. Jay Clayton, Chairman, Commission, dated November 27, 2019, at 4–5, *available at https://www.catnmsplan.com/sites/default/files/2020-02/Simon-Letter-SIFMA-%28Final%29.pdf* (''Simon Letter'').

[53] *See* Part II.C.2. *infra,* for a discussion of the SAW usage requirements.

[54] *See* proposed Section 1.1, ''Secure Analytical Workspaces.'' *See also* proposed Section 6.1(d)(v) (stating that the Plan Processor shall ''provide Secure Analytical Workspaces in accordance with Section 6.13''). The Central Repository, as a facility of each of the Participants, is an SCI entity and the CAT System is an SCI system, and thus it must comply with Regulation SCI. *See* CAT NMS Plan Approval Order, *supra* note 3, at 84758; *see also* 17 CFR 242.1000 (definition of ''SCI system'' and ''SCI entity''). Because the CAT systems, including the Central Repository, are operated on behalf of the Participants by the Plan Processor, the Participants are responsible for having in place processes and requirements to ensure that they are able to satisfy the requirements of Regulation SCI for the CAT systems operated by the Plan Processor on their behalf. *See also* Securities Exchange Act Release No. 73639 (November 19, 2014), 79 FR 72251, 72276 (December 5, 2014) (''Regulation SCI Adopting Release''). The CAT NMS Plan states that data security standards of the CAT System shall, at a minimum, satisfy all applicable regulations regarding database security, including provisions of Regulation SCI. 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. *See* CAT NMS Plan Approval Order, *supra* note 3, at 84758–59; CAT NMS Plan, *supra* note 3, at Section 6.9(b)(xi)(A). *See also, e.g.,* Letter from Michael J. Simon, Chair, CAT NMS, LLC Operating Committee, to Brent J. Fields, Secretary, Commission, at 1–2, dated April 9, 2019, *available at https://www.sec.gov/divisions/marketreg/rule613-info-notice-of-plan-processor-selection-040919.pdf* (setting forth the material terms of the Plan Processor agreement, which obligate the Plan Processor to perform CAT-related functions and services in a manner that is consistent with and in accordance with the CAT NMS Plan and Commission rules and regulations).

[55] *See* Part II.C.3. *infra* for a discussion of the common technical security controls that must be required for SAWs by the CISP. The Commission also preliminarily believes that this requirement would enable the Plan Processor to achieve a consistent level of security across the CAT System, as the Central Repository and the SAWs would have common controls that were implemented by the same party.

[56] *See* Part II.C.4.b. *infra* for a discussion of the monitoring requirements for SAWs.

[57] *See, e.g.,* CAT NMS Plan, *supra* note 3, at Section 6.12 (requiring the Plan Processor to develop and maintain the information security program).

[58] *See* note 56 *supra.*

[59] Because SAW accounts are, by definition, part of the CAT System, the Commission preliminarily believes that SAW accounts would likely be built by the same cloud provider and in the same cloud environment as the Central Repository.

[60] *See* Part IV.C.1. *infra* for a discussion of the potential costs related to each Participant providing its own SAW account. With respect to SAW pricing, the Commission preliminarily believes that the Plan Processor will charge back variable cloud services fees to each Participant in a manner consistent with how current variable fees incurred by the Plan Processor are charged back to the Company. *See* Part IV.A.3. *infra* for further discussion of such pricing and potential fees.

Repository across all SAW accounts. Requiring each Participant to independently implement relevant security controls would be comparatively inefficient, needlessly duplicative, and, potentially, less secure.

Although the Plan Processor would provide each SAW account, the proposed amendments would still afford the Participants a fair amount of autonomy in the operation of the SAW. The definition of ''Secure Analytical Workspace'' would make it clear that proposed Section 6.13 would govern the use of the SAWs, and proposed Section 6.13 explicitly states that each Participant would be allowed 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.[61] This language would permit the Participants to create whatever analytic environment they prefer within the SAWs. For example, each Participant would be free to choose which hardware configurations inclusive of computing power and storage, analytical tools, and additional content should be available in its SAW. This language also would not prevent the Participants from collectively contracting with a third party, such as the Plan Processor, to provide each SAW with common tools or the infrastructure needed to query and process CAT Data. The Commission therefore preliminarily believes that the proposed amendments give each Participant sufficient flexibility to operate its SAW according to its own preferences, while still ensuring that the SAWs are built and implemented in a consistent and efficient manner.[62]

The Commission requests comment on the proposed requirements for SAWs. Specifically, the Commission solicits comment on the following:

9. Is the proposed definition for Secure Analytical Workspaces sufficient? Should the proposed definition specify that the SAW accounts must be built using the same cloud provider that houses the Central Repository? Is the Commission correct in its belief that SAW accounts would be built in the same environment as the Central Repository because they would be part of the CAT System? If not, should such a requirement be added?

10. Is it possible that Participants might perform tasks in a SAW other than accessing and analyzing CAT Data, such as workflows for generating and handling alerts? Please identify any such tasks with specificity and explain whether the definition should include those tasks. Is it appropriate to characterize SAWs as ''part of the CAT System''? Are there alternative definitions of a SAW that would be more appropriate? If so, what are those definitions and why are they appropriate.

11. Is it appropriate for the Plan Processor to provide the SAW accounts? To the extent that the Plan Processor has already been authorized to begin developing and/or implementing analytic environments for the Participants, will the Plan Processor be able to leverage any of this work to build the SAW accounts? If so, please explain what efforts have already been made by the Plan Processor and whether the Plan Processor will be able to leverage any of these efforts to build the SAW accounts. Should each Participant be permitted to provide its own SAW account? Is there a third party who should provide the SAW accounts? If so, please identify that party, explain why it would be appropriate for that party to provide the SAW accounts, and explain why such structure would not inhibit the Plan Processor's ability to control, manage, operate, and maintain the CAT System. Are there alternative structures that the Commission has not explicitly considered here? If so, please explain what these structures are and why they would be more appropriate for SAWs. Is it appropriate for the Plan Processor to implement all common security controls required by the CISP? Would implementation of such controls hamper the Participants' ability to customize their SAWs? Should each Participant be able to implement the common security controls on its own?

12. Should the Plan Processor be required to provide each Participant with a SAW account? Should the proposed amendments explicitly specify that Participants are permitted to share SAW account(s)? If a Participant does not believe it will need to use a SAW account, should the Plan Processor still be required to build a SAW account for that Participant? If not, how and at what point should the Participant inform the Plan Processor that it does not need a SAW account? Should such a Participant be allowed to change its mind if the Participant later determines that it needs to use a SAW account? If so, how long should the Plan Processor be given to build a SAW account for that Participant? Should the Plan Processor be required to provide each Participant with more than one SAW account upon request?

13. Do commenters agree that centralizing provision of the SAW accounts with the Plan Processor is the most effective and efficient way to implement the common technical controls associated with the CISP and to enable the Plan Processor to conduct consistent and comprehensive monitoring of SAWs? If not, please identify any alternative approaches that would be more effective and more efficient.

14. The proposed amendments state that the Participants may provide and use their choice of software, hardware configurations, and additional data within their SAWs, so long as such activities otherwise comply with the CISP. Should the Plan Processor, as the provider of each SAW account, be required to assist with any such activities? If not, do commenters believe that the Participants will be able to provide their own software, hardware configurations, and additional data without the assistance of the Plan Processor? For example, do commenters believe that a Participant would need the Plan Processor to grant special access or other administrative privileges in order to provide such software, hardware configurations, or additional data? Are there any other administrative tasks that the Plan Processor would or should be expected to provide? If so, please identify any such tasks and explain whether the proposed amendments should explicitly address the performance of such tasks.

15. Do commenters believe that the Plan Processor will charge back variable cloud services fees to each Participant for SAWs in a manner consistent with how current variable fees incurred by the Plan Processor are charged back to the Company? If not, how will the Plan Processor charge each Participant for SAW implementation and usage? Should the proposed amendments state how the Plan Processor may charge the Participants for SAW implementation and usage? If so, should each Participant be billed by the Plan Processor for providing a SAW, even if the Participants choose not to use that SAW? How should the Participants be billed for their use of the SAWs?

2. Data Access and Extraction Policies and Procedures

The 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 extraction does not compromise the security of CAT

[61] *See* proposed Section 6.13(c)(iii); *see also* Part II.C.4.b. *infra*, for a discussion of and questions about this provision.

[62] The Commission would have the same ability to configure its SAW to migrate third-party or in-house applications, analytical tools, or external data as the Participants.

Data. Proposed Section 6.13(a)(i) would therefore require the CISP to, at a minimum, establish certain data access and extraction policies and procedures.[63]

First, under proposed Section 6.13(a)(i)(A), the CISP must establish policies and procedures that would require Participants to use their SAWs as the only means of accessing and analyzing customer and account data. While the database containing customer and account data would no longer include social security numbers, dates of birth, and/or account numbers for individual retail investors,[64] the unauthorized access and use of the remaining customer and account data—Customer and Account Attributes—could still be damaging. Because Customer and Account Attributes data may currently be accessed outside of the CAT System, the Commission preliminarily believes that the proposed SAW usage requirement would better protect this information by ensuring that it is accessed and analyzed within the CAT System and therefore subject to the security controls, policies, and procedures of the CISP when accessed and analyzed by the Participants.[65]

Second, under proposed Section 6.13(a)(i)(B), the CISP must establish policies and procedures that would require the Participants to use their SAWs when accessing and analyzing CAT Data through the user-defined direct query and bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2 of the CAT NMS Plan, unless an exception is granted pursuant to proposed Section 6.13(d).[66] Under the CAT NMS Plan, the online targeted query tool facilitates access to focused, narrowly-defined queries, while the user-defined direct query and bulk extract tools enable the Participants to download much larger sets of data from the Central Repository to external systems that are not required to comply with the information security program described in Section 6.12.[67] The user-defined direct query and bulk extract tools therefore have a greater impact on the attack surface of the CAT. The Commission preliminarily believes that the proposed SAW usage restrictions will keep more CAT Data within the CAT System and subject to the CISP, while still providing the Participants with the flexibility of performing focused searches outside of the SAW through the online targeted query tool.[68]

Third, under proposed Section 6.13(a)(i)(C), the CISP must establish policies and procedures that would require that the Participants only extract from SAWs the minimum amount of CAT Data necessary to achieve a specific surveillance or regulatory purpose.[69] While the proposed amendments require access and analysis of CAT Data within the SAW for Customer and Account Attributes and transaction data accessed with the user-defined direct query or bulk extract tools, the Commission recognizes that it may sometimes be necessary for the Participants to extract CAT Data that is otherwise required to be accessed or analyzed in a SAW 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.[70] 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. The Commission preliminarily believes that these provisions strike an appropriate balance by maintaining CAT Data largely within the CAT System, but still enabling limited extraction of data to allow the Participants to comply with their regulatory or statutory obligations.

Fourth, under proposed Section 6.13(a)(i)(D), the CISP must establish policies and procedures that would require that secure file sharing capability provided by the Plan Processor be the only mechanism for extracting CAT Data from SAWs. Because file-based sharing systems have the ability to track file size and recipients, the Commission preliminarily believes that requiring the use of file-based sharing will help the Plan Processor to monitor for non-compliant use of the SAWs. The Commission further preliminarily believes that requiring the use of a secure file sharing capability will better protect CAT Data by enabling confidential transmission of data between authorized users. Finally, the Commission preliminarily believes that it is appropriate for the Plan Processor to provide this capability. As the party responsible for developing and maintaining the CISP, the Plan Processor is in the best position to determine which file-based sharing system will fit the security needs of the CAT System. Requiring that the Plan Processor provide one universally-used secure file-based sharing system may also reduce the administrative burdens and security risks that might arise if each Participant developed and used a different file-based sharing capability to extract CAT Data out of its SAWs.

Finally, the CAT NMS Plan currently states that the Chief Compliance Officer[71] (the ''CCO'') shall oversee the

[63] Proposed Section 6.13(a) also states explicitly that the CISP shall apply to every Participant's SAW. This is also required by the proposed definition of ''Comprehensive Information Security Program.'' *See* proposed Section 1.1; *see also* Part II.A. *supra,* for a discussion of the proposed CISP. Similarly, proposed Section 6.12 would make clear that the CISP should include the requirements set forth in proposed Section 6.13.

[64] *See* Securities Exchange Act Release No. 88393 (March 17, 2020), 85 FR 16152 (March 20, 2020) (granting conditional exemptive relief from certain requirements of the CAT NMS Plan, including requirements related to the reporting of PII). With the elimination of social security numbers, dates of birth, and/or account numbers from the CAT, the Commission proposes to eliminate the term ''PII'' and refer to the remaining customer and account data in the CAT as ''Customer and Account Attributes'' throughout the CAT NMS Plan. *See* Part II.E. *infra,* for a discussion of this proposed change.

[65] The Commission is also proposing amendments to the CAT NMS Plan to define the security requirements of the Customer Identifying Systems Workflow. *See* Part II.F. *infra,* for a discussion of these amendments.

[66] *See* Part II.C.5.a. *infra,* for a discussion of the proposed exception process.

[67] For example, the online targeted query tool limits searches using a date or time range and only makes certain predetermined fields available to users, whereas the user-defined direct query tool can be used to query all available attributes and data sources without such limitations. *Cf., e.g.,* CAT NMS Plan, *supra* note 3, at Section 6.10(c)(1)(A); *id.* at Section 6.10(c)(1)(B).

[68] To further protect CAT Data, the Commission is also proposing amendments to the CAT NMS Plan that would reduce the amount of information that the Participants could extract via the online targeted query tool. *See* Part II.D. *infra,* for a discussion of these proposed amendments.

[69] *See also* Part II.G. for further discussion of other proposed controls on access to and use of CAT Data, which would, among other things, limit the extraction of CAT Data to the minimum amount of data necessary to achieve a specific regulatory or surveillance purpose, define the staff that would be entitled to access or use CAT Data, and increase the oversight of the Chief Regulatory Officer (or similarly designated head(s) of regulation) of each Participant over access to and use of CAT Data.

[70] *See also* Part II.N. *infra,* for a discussion of how the proposed amendments would apply to Commission staff. The Commission preliminarily believes that the restrictions set forth in the proposed amendments would still enable the extraction of required data—for example, to support discussions with a regulated entity regarding activity that raises concerns, to file a complaint against a regulated entity, or to support an investigation or examination of a regulated entity.

[71] ''Chief Compliance Officer'' is a defined term in the CAT NMS Plan and means ''the individual then serving (even on a temporary basis) as the Chief Compliance Officer pursuant to Section 4.6, Section 6.1(b), and Section 6.2(a).'' *See* CAT NMS Plan, *supra* note 3, at Section 1.1. The CCO is an officer of the Company and has a fiduciary duty to the Company. *See id.* at Section 4.6(a), Section 4.7(c).

regular written assessment of the Plan Processor's performance that is required to be provided to the Commission and that this assessment shall include an evaluation of the existing information security program ''to ensure that the program is consistent with the highest industry standards for the protection of data.'' [72] In addition to replacing the reference to the ''information security program'' with a reference to the proposed ''Comprehensive Information Security Program,'' the proposed amendments would require the CCO, in collaboration with the CISO, to include in this evaluation a review 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 [73] and to identify any appropriate corrective measures.[74] The Commission preliminarily believes that these proposed requirements will facilitate Commission oversight of the security risks posed by the extraction of CAT Data. The proposed review should enable a thorough assessment of security risks to CAT Data and whether changes to the current security measures are appropriate.

The Commission requests comment on the proposed data access and extraction policies and procedures. Specifically, the Commission solicits comment on the following:

16. Is it appropriate to require the CISP to establish data access and extraction policies and procedures? Should the proposed amendments specify each component that should be included in the data access and extraction policies and procedures? If so, please describe what components should be included and explain why those components would be appropriate. For example, should the proposed amendments specify that the data access and extraction policies and procedures should establish which data will be provided to Participants in the form of data extraction logs, how the proposed confidentiality policies described in Part II.G. should apply to SAW usage, or when data extraction should be permissible? Is CAT Data sufficiently protected by the current terms of the CAT NMS Plan? If so, please explain how the current protection is adequate.

17. The proposed amendments require the CISP to establish policies and procedures that require the Participants to use SAWs as the only means of accessing and analyzing Customer and Account Attributes. Should Participants be allowed to analyze Customer and Account Attributes data outside of a SAW?

18. The proposed amendments require the CISP to establish policies and procedures that require Participants to use SAWs when accessing and analyzing CAT Data through the user-defined direct query and bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2, unless granted an exemption pursuant to proposed Section 6.13(d). Would it be more effective to limit the number of records that could be returned by these search tools? If so, please explain how those tools should be limited and explain why those limitations are appropriate. Should the proposed amendments also require the Participants to use SAWs when accessing and analyzing CAT Data retrieved through the online targeted query tool described in Section 6.10(c)(i)(A)? Should the proposed amendments require that all CAT Data be accessed and analyzed in a SAW, regardless of how it was retrieved?

19. The proposed amendments require the CISP to establish policies and procedures directing the Participants to extract only the minimum amount of CAT Data necessary to achieve a specific surveillance or regulatory purpose. Should the Commission revise this requirement to specifically limit the number of records, the size of the data that may be extracted, or the file types permitted for extraction in support of a specific surveillance or regulatory purpose? If so, what should the Commission specify as the number of records or the size of the data? For example, should the number of records be limited to 200,000 rows, the size of the data that may be extracted be limited to 1 gigabyte, or the file types permitted for extracted be limited to Excel spreadsheets? Please identify any appropriate limitations, explain why those limitations would be appropriate, and describe how regulatory use cases requiring the extraction of data from the SAW would be fully supported. Should the CISP be allowed to establish a more permissive policy governing the extraction of CAT Data from the SAWs? If so, please identify any conditions that should be placed on the extraction of CAT Data from the SAWs and explain why they are appropriate.

20. Should the proposed amendments require the application of additional security controls, policies, or procedures for data that is extracted from a SAW or that is extracted directly from the Central Repository by Participants into a non-SAW environment that has not been granted an exception pursuant to proposed Section 6.13(d)—*i.e.,* data extracted using the online targeted query tool? Or do existing rules and regulations under the Exchange Act, like Regulation SCI, sufficiently protect CAT Data that would be extracted from a SAW or from the Central Repository?

21. The proposed amendments require the CISP to establish policies and procedures that state that secure file sharing capability provided by the Plan Processor shall be the only mechanism for extracting CAT Data from the SAW. Do commenters understand what is meant by ''secure file sharing'' or should the Commission specify criteria that should be used to assess whether a system provides ''secure file sharing capability''? What criteria would evaluate whether a system provides ''secure file sharing capability''? Should a different method of extraction be permitted? If so, please identify that method of extraction and explain why it would be appropriate. Is it clear what the Commission means by ''secure file sharing capability''? Please explain what commenters understand this term to mean and whether it is appropriate for the Commission to add more detail to the proposed amendments. Should a different party provide the secure file sharing capability? If so, please identify that party and explain why that party would be a more appropriate choice. Should the proposed amendments be more specific about what kind of capability must be provided by the Plan Processor? If so, please explain what kinds of details would be helpful.

22. The proposed amendments require the CCO, in collaboration with

[72] *See id.* at Section 6.6(b)(i)(B), Section 6.6(b)(ii)(B)(3). The CAT NMS Plan requires the written assessment of the Plan Processor's performance to be provided to the Commission annually or more frequently in connection with any review of the Plan Processor's performance under the CAT NMS Plan pursuant to Section 6.1(n). *See id.* at Section 6.6(b)(i)(A).

[73] The Commission believes that such an evaluation could be performed using metrics associated with aggregated data. For example, the Plan Processor could review the amount of data that each Participant extracted on a monthly basis and analyze extraction trends for each Participant to identify any anomalies or to compare the amount of data extracted from the CAT against the amount of data ingested into the CAT.

[74] *See* proposed Section 6.6(b)(ii)(B)(3). The proposed amendments do not limit this review to CAT Data extracted from SAWs; the proposed review should also include CAT Data extracted using other methods, like the online targeted query tool. These requirements are also enshrined in proposed Section 6.2. *See also* proposed Section 6.2(a)(v)(T) (requiring the CCO to determine, pursuant to Section 6.6(b)(ii)(B)(3), to review CAT Data that has been extracted from the CAT System to assess the security risk of allowing such CAT Data to be extracted); proposed Section 6.2(b)(x) (requiring the CISO to determine, pursuant to Section 6.6(b)(ii)(B)(3), to review CAT Data that has been extracted from the CAT System to assess the security risk of allowing such CAT Data to be extracted).

the CISO, to include, in the regular written assessment of the Plan Processor's performance that is required to be provided to the Commission, a review of the quantity and type of CAT Data extracted from the CAT System to assess the security risk of permitting such extraction. This review must also identify any appropriate corrective measures. Is it appropriate to require this review to be included in the regular written assessment of the Plan Processor's performance that is required to be provided to the Commission? Is there a better vehicle for communicating this information to the Commission? If so, please identify that vehicle and explain why it would be a more appropriate way of communicating this information to the Commission. Should the Commission receive this information more often than it would receive the regular written assessment of the Plan Processor's performance? If so, how often should the Commission receive this information and through what means should such information should be communicated? Is there any other information that should be included in this review? If so, please identify such information and explain why it would be appropriate to include such information in the review.

3. Security Controls, Policies, and Procedures for SAWs

To protect the security of the SAWs, the Commission preliminarily believes that it is appropriate to require the CISP to set forth the security controls, policies, and procedures that must apply to the SAWs. The Plan Processor already must adhere to the NIST Risk Management Framework and implement the security controls identified in National Institute of Standards and Technology's Special Publication 800–53 to protect CAT Data that is reported to and retained at the Central Repository.[75] To promote the consistent treatment of CAT Data that might be downloaded to SAWs, the proposed amendments would state that the CISP must establish security controls, policies, and procedures for SAWs that require all NIST SP 800–53 security controls and associated policies and procedures required by the CISP to apply to the Participants' SAWs.[76]

The proposed amendments would also require the CISP to establish security controls, policies, and procedures that would specify that certain security controls, policies, and procedures must be applied to SAWs by the Plan Processor and that such security controls, policies, and procedures must be common to both the SAWs and the Central Repository in accordance with Section 2.4 of NIST SP 800–53, unless technologically or organizationally not possible.[77] Common security controls, policies, and procedures would be required for at least the following NIST SP 800–53 control families: Audit and accountability, security assessment and authorization, configuration management, incident response, system and communications protection, and system and information integrity.[78]

The NIST SP 800–53 control families specifically identified by the proposed amendments are core families that would enable the Plan Processor to better monitor the security of the SAWs.[79] For example, requiring that audit and accountability,[80] security assessment and authorization,[81] incident response,[82] and systems and information integrity[83] controls, policies, and procedures be ''common'' in accordance with Section 2.4 of NIST SP 800–53 would facilitate consistent monitoring of systems and personnel and associated analysis across the CAT System, including the generation and review of activity logs, identification of potential anomalies or attacks, incident-specific monitoring and notification, analysis of security-related infrastructure and possible system vulnerabilities, and uniform issuance of security alerts. In addition, by requiring that security assessment and authorization controls, policies, and procedures be ''common'' in accordance with Section 2.4 of NIST SP 800–53, the proposed amendments would include security assessments of the SAWs as part of the overall risk assessment of the CAT System; risks would be tracked and escalated in the same way. Common configuration management[84] and system and communication protection[85] controls, policies, and procedures would centralize the management of crucial infrastructure, so that each SAW would operate according to the same parameters as the rest of the CAT System and thereby enable the Plan Processor to conduct the above-described monitoring more efficiently.

The Commission preliminarily believes that it is appropriate for all NIST SP 800–53 security controls, policies, and procedures required by the CISP to apply to the SAWs; the same set of control families, policies, and procedures should apply when CAT Data is accessed and downloaded to a SAW. In addition, the Commission preliminarily believes that it is appropriate to further require common implementation for NIST SP 800–53 control families that relate to critical monitoring functions, unless technologically or organizationally not possible. By requiring the CISP to establish common security controls, policies, and procedures for these NIST SP 800–53 control families, the proposed amendments would establish security protections for SAWs that are harmonized to the greatest extent possible with the security protections of the Central Repository. The security of the SAWs should therefore be robust.[86] Moreover, the Commission preliminarily believes that the proposed amendments would facilitate the efficient implementation of the SAWs by specifying that the Plan Processor will be responsible for implementing the common security controls, policies, and procedures. If each Participant were allowed to implement the common security controls, policies, and procedures, different Participants might

[75] *See, e.g.,* CAT NMS Plan, *supra* note 3, at Appendix D, Section 4.2 (setting forth a non-exhaustive list of applicable industry standards, including NIST SP 800–53). *See also id.* at Appendix D, Section 5.3 (''The Plan Processor must conduct third party risk assessments at regular intervals to verify that security controls implemented are in accordance with NIST SP 800–53.''). *See also* NIST SP 800–53, *supra* note 15, at 7–8 (explaining how NIST SP 800–53 implements the NIST Risk Management Framework).

[76] *See* proposed Section 6.13(a)(ii).

[77] *See* proposed Section 6.13(a)(ii)(A). *See* NIST SP 800–53, *supra* note 15, at Section 2.4 (explaining what common controls are and how they should be implemented).

[78] *See* proposed Section 6.13(a)(ii)(A).

[79] Although the proposed amendments would require the Plan Processor to monitor the SAWs to verify that relevant security controls, policies, and procedures are being followed, the proposed amendments would not permit the Plan Processor to monitor analytical activities taking place within the SAWs, including analytical activities that may take place within any SAW provided for the Commission's use. *See* Part II.C.4.b. *infra* for further discussion of the monitoring requirements; *see also* Part II.N. *infra* for further discussion regarding the application of the proposed amendments to Commission staff.

[80] *See* NIST SP 800–53, *supra* note 15, at Appendix F–AU

[81] *See id.* at Appendix F–CA.

[82] *See id.* at Appendix F–IR.

[83] *See id.* at Appendix F–SI.

[84] *See id.* at Appendix F–CM.

[85] *See id.* at Appendix F–SC.

[86] By contrast, if the proposed amendments were not adopted, the Participants would be allowed to build these analytical environments with their own security measures. Although the CAT NMS Plan requires the CISO to review the Participants' information security policies and procedures related to any such analytical environments to ensure that such policies and procedures are comparable to the information security policies and procedures that are applicable to the Central Repository, the proposed amendments will promote uniformity, which the Commission preliminarily believes is more likely to protect CAT Data for the reasons discussed above. *See* CAT NMS Plan, *supra* note 3, at Section 6.2(b)(vii).

make different (and potentially less secure or less efficient) implementation choices. As the party who would be the most familiar with the CISP, the Plan Processor can more efficiently implement these common security controls, policies, and procedures [87] and is the best situated to verify that such security controls, policies, and procedures are implemented consistently.

The Commission recognizes, however, that common implementation will likely not be feasible for all of the NIST SP 800–53 security controls, policies, and procedures required by the CISP. Accordingly, proposed Section 6.13(a)(ii)(B) would permit the security controls, policies, and procedures established by the CISP to indicate that implementation of NIST SP 800–53 security controls, policies, and procedures required by the CISP may be done in a SAW-specific way and by either the Plan Processor or each Participant.[88] The Commission emphasizes, however, that ''SAW-specific'' does not mean that each Participant may independently select or assess the NIST SP 800–53 security controls, policies, and procedures that should apply for its SAWs. Rather, this provision would still require the CISP to provide the basis for the NIST SP 800–53 security controls, policies, and procedures that should be applied to SAWs, but allow that the implementation of controls, policies, and procedures may be different for each SAW. The Commission preliminarily believes this provision would provide an appropriate level of control to the Plan Processor while permitting SAW-specific implementation of the security controls, policies, and procedures that would apply to SAWs, as SAWs would have different functional and technical requirements from the Central Repository and may therefore require tailored implementation of controls.

The Commission requests comment on the proposed security controls, policies, and procedures requirements. Specifically, the Commission solicits comment on the following:

23. The proposed amendments require the CISP to establish security controls, policies, and procedures such that all NIST SP 800–53 security controls and associated policies and procedures required by the CISP apply to the SAWs. Should the CISP be required to establish security controls, policies, and procedures to implement any other industry standard for SAWs? If so, please identify the relevant industry standard(s) and explain why it would be appropriate to require the CISP to establish security controls, policies, and procedures to implement that standard(s). Should the CISP be required to implement additional NIST SP 800–53 security controls, policies, or procedures for SAWs, including security controls, policies, and procedures that would protect the boundary of each SAW from other SAWs and/or other components of the CAT System? If so, please identify those security controls, policies, or procedures and explain why they should be implemented for SAWs. Should the SAWs be required to implement all security controls, policies, and procedures required by the CISP? If not, please identify the security controls, policies, and procedures that might be required by the CISP (if adopted) that should not be applied to SAWs and explain why excluding such security controls, policies, or procedures would be appropriate.

24. Unless technologically or organizationally not possible, the proposed amendments require the CISP to establish controls, policies, and procedures that require the following NIST SP 800–53 control families to be implemented by the Plan Processor and to be common to both the SAWs and the Central Repository: Audit and accountability, security assessment and authorization, configuration management, incident response, system and communications protection, and system and information integrity. Are there technological, organizational, or other impediments to requiring common implementation for the specified control families? Should the security controls, policies, and procedures for other NIST SP 800–53 control families be commonly implemented for the SAWs and the Central Repository? If so, please identify these control families and explain why it would be appropriate to require common implementation. Is it appropriate to require that the common security controls be implemented by the Plan Processor? Is there another party that should implement the common security controls? If so, please identify that party and explain why it would be more appropriate for that party to implement the common security controls.

25. The proposed amendments require the CISP to establish security controls, policies, and procedures such that SAW-specific security controls, policies, and procedures are implemented to cover any NIST SP 800–53 security controls for which common controls, policies, and procedures are not possible. Should the proposed amendments provide this flexibility? Does providing this flexibility endanger the security of the SAWs?

4. Implementation and Operational Requirements for SAWs

To further the security of the CAT System, the Commission preliminarily believes it is important that the SAWs be implemented and operated consistently and in accordance with the CISP.

a. Implementation Requirements for SAWs

Proposed Section 6.13(b)(i) would require the Plan Processor to develop, maintain, and make available to the Participants detailed design specifications for the technical implementation of the access, monitoring,[89] and other controls required for SAWs by the CISP.[90] Proposed Section 6.13(b)(ii) would further require the Plan Processor to notify the Operating Committee that each Participant's SAW has achieved compliance with the detailed design specifications issued by the Plan Processor pursuant to proposed Section 6.13(b)(i) before such SAW may connect to the Central Repository.

The Commission preliminarily believes that it is appropriate to require the Plan Processor to develop and maintain detailed design specifications for the technical implementation of the CISP controls. As the party responsible for maintaining data security across the CAT System and for providing the SAWs, the Plan Processor would have the most information regarding the security requirements that are

[87] *See* Part II.C.1. *supra* (explaining why it is more efficient for the Plan Processor to implement and administer relevant security controls).

[88] It may also be technologically or organizationally impossible to commonly implement all of the security controls, policies, and procedures identified by proposed Section 6.13(a)(ii)(A), in which case proposed Section 6.13(a)(ii)(B) would control how the security controls, policies, and procedures established by the CISP for SAWs address such implementation.

[89] In addition to the controls, policies, and procedures that specifically relate to or require monitoring, monitoring of security controls is part of the general risk management framework established by NIST SP 800–53. *See, e.g.,* NIST SP 800–53, *supra* note 15, at 8. Detailed design specifications implementing the NIST SP 800–53 controls required by the CISP should therefore detail how the Plan Processor will perform such monitoring and give the Plan Processor sufficient access to the SAWs to conduct such monitoring.

[90] *See* Part II.A.1. and Part II.C.2.–3. *supra,* for a discussion of the CISP. The Commission preliminarily believes that the Plan Processor could make these detailed design specifications available to the Participants in a number of formats, including by making available a reference SAW account for the Participants to review and analyze.

applicable to SAWs.[91] The Commission preliminarily believes that it would be appropriate for the Plan Processor to share this information with the Participants through detailed design specifications,[92] because releasing such information through detailed design specifications would help the Participants to more precisely understand how they would be able to use and provision their SAWs, what information they would be required to share with the Plan Processor to enable the NIST SP 800–53 access and monitoring controls that are applicable to SAWs, and how the security parameters of the SAWs might impact their existing surveillance protocols.[93] Requiring the Plan Processor to make available detailed design specifications for SAWs may thus increase the likelihood that Participants provision their SAWs with hardware, software, and data that complies with the CISP. Moreover, the development of detailed design specifications would also provide the Plan Processor with uniform criteria with which to evaluate and validate SAWs, which the Commission preliminarily believes should make the notification process required by proposed Section 6.13(b)(ii) more efficient for the Plan Processor and more fair for the Participants.

The security of the CAT is critically important, and the Commission preliminarily believes that it would be prudent to confirm that the detailed design specifications have been implemented properly before permitting any Participant to use its SAW to access CAT Data. Accordingly, the Commission preliminarily believes it is appropriate to require the Plan Processor to evaluate each Participant's SAW and notify the Operating Committee that each Participant's SAW has achieved compliance with the detailed design specifications required by proposed Section 6.13(b)(i) before that SAW may connect to the Central Repository. The Commission preliminarily believes that such an evaluation would establish that the access, monitoring, and other technical controls required for SAWs by the CISP have been implemented properly. The Commission preliminarily believes that SAWs that comply with these detailed design specifications should be sufficiently secure, because those detailed design specifications must implement the full battery of technical controls associated with the CISP, including all required NIST SP 800–53 security controls.[94] The Plan Processor is not only knowledgeable about NIST SP 800–53 security controls, but is also responsible for developing the CISP and the detailed design specifications that would be used to implement the CISP controls.[95] In addition, the Plan Processor would have access, through the CISO, to the collective knowledge and experience of the Security Working Group.[96] For these reasons, the Commission further preliminarily believes that the Plan Processor is best situated to determine whether each Participant's SAW has achieved compliance with such detailed design specifications. Finally, the Commission believes it is appropriate to require that the Plan Processor notify the Operating Committee, that each Participant's SAW has achieved compliance with the detailed design specifications before that SAW may connect to the Central Repository, as this requirement would enable the Operating Committee to better oversee the Plan Processor and the security of the CAT.

The Commission requests comment on proposed Section 6.13(b). Specifically, the Commission solicits comment on the following:

26. Do commenters agree that development and maintenance of detailed design specifications for the technical implementation of the CISP will enable the consistent, efficient, and secure implementation of SAWs?

27. The proposed amendments require the Plan Processor to develop and maintain detailed design specifications for the technical implementation of the access, monitoring, and other controls required for SAWs by the CISP. Should a different party develop and maintain these detailed design specifications? If so, please identify the party that should develop and maintain these detailed design specifications and explain why. Should the detailed design specifications be subject to review by the Operating Committee, the Security Working Group, or some other entity? If so, please explain why and provide a detailed explanation of what such review process should entail.

28. Should the proposed amendments specify the nature of the monitoring required by NIST SP 800–53 controls? Should the proposed amendments specify that monitoring should be continuous? If so, please explain how that term should be defined and why such definition would be appropriate. Should the proposed amendments indicate whether manual or automated processes (or both) should be used by the Plan Processor and whether automated support tools should be used? Should the proposed amendments explicitly state that the NIST SP 800–53 controls, policies, and procedures require the Participants to give the Plan Processor sufficient access to SAWs in order to enable the monitoring inherently required by such NIST SP 800–53 controls, policies, and procedures? If so, please explain what details should be included in the proposed amendments.

29. The proposed amendments do not specify how the detailed design specifications should be provided by the Plan Processor. Should the proposed amendments require the Plan Processor to provide a reference SAW account? If a specific format should be used, please identify the format that the detailed design specifications should be provided in and explain why that format is appropriate.

30. The proposed amendments require the Plan Processor to notify the Operating Committee that each Participant's SAW has achieved compliance with the detailed design specifications required by Section 6.13(b)(ii) before that SAW may connect to the Central Repository. Is the Plan Processor the appropriate party to make this determination? If not, what other party should make this determination and why? Is evaluation against some benchmark appropriate in order to safeguard the security of CAT Data? Should the SAWs be allowed to connect to the Central Repository without any evaluation process? Are the detailed design specifications required by Section 6.13(b)(ii) an appropriate benchmark? If it is not an appropriate benchmark, please identify what benchmark would be appropriate and explain why. Is it appropriate for the Plan Processor to notify a third party? Should the Operating Committee receive the notification? Should any other parties receive the notification? If so, please identify the parties and

[91] *See* Part II.A, Part II.C.1. *supra*

[92] As public disclosure of these detailed design specifications could raise security concerns, the Commission believes that the Plan Processor and the Participants generally should keep these detailed design specifications confidential.

[93] The Commission emphasizes that these detailed design specifications need only implement the access, monitoring, and other controls required by the CISP. Each Participant will have the flexibility to otherwise design the analytic capabilities of its own SAW and to provision it with its own hardware, software, and other data, so long as such activities comply with the CISP. *See* proposed Section 6.13(c)(iii); *see also* Part II.C.4.b. *infra,* for a discussion of the flexibility afforded to the Participants by the proposed amendments.

[94] *See* proposed Section 6.13(b)(i); proposed Section 6.13(a)(ii). *See also* Part II.A.1. and Part II.C.2.–3. *supra,* for a discussion of the requirements of the CISP.

[95] *See* proposed Section 6.13(b)(i).

[96] *See* Part II.B. *supra* for a discussion of the proposed Security Working Group.

explain why it would be appropriate to provide the notification to these parties.

b. Operation of the SAWs

Proposed Section 6.13(c) would set forth requirements for the Plan Processor and the Participants that are designed to promote compliance with the CISP. First, proposed Section 6.13(c)(i) would require the Plan Processor to monitor each Participant's SAW in accordance with the detailed design specifications developed pursuant to proposed Section 6.13(b)(i), for compliance with the CISP and the detailed designs specifications only, and to notify the Participant of any identified non-compliance with the CISP or the detailed design specifications.[97] Second, proposed Section 6.13(c)(ii) would require the Participants to comply with the CISP, to comply with the detailed design specifications developed by the Plan Processor pursuant to proposed Section 6.13(b)(i), and to promptly remediate any non-compliance identified.[98]

The Commission preliminarily believes that these requirements will facilitate compliance with the CISP and, therefore, the overall security of the CAT. Requiring the Plan Processor to monitor each Participant's SAW in accordance with the detailed design specifications developed pursuant to proposed Section 6.13(b)(i) should enable the Plan Processor to conduct such monitoring consistently and efficiently across SAWs. It should also help the Plan Processor to identify and to escalate any non-compliance events, threats, and/or vulnerabilities as soon as possible, thus reducing the potentially harmful effects of these matters. Likewise, requiring the Plan Processor to notify the Participant of any identified non-compliance will likely speed remediation of such non-compliance by the Participant and thereby better protect the security of the SAW in question. The Commission also preliminarily believes it is appropriate to limit the scope of the Plan Processor's monitoring to compliance with the CISP and the detailed design specifications developed by the Plan Processor pursuant to Section 6.13(b)(i). The Commission preliminarily believes that this limitation would make it clear that analytical activities in the SAW would not be subject to third-party monitoring, without hampering the ability of the Plan Processor to adequately protect the security of each SAW.[99]

The Commission also preliminarily believes it is appropriate to set forth the Participants' obligations to comply with the CISP, as well as the detailed design specifications developed by the Plan Processor pursuant to Section 6.13(b)(i), and to require the Participants to promptly remediate any identified non-compliance.[100]

Such compliance is important, but the Commission does not wish to unnecessarily constrain the Participants from employing tools or importing external data that might support or enhance the utility of the SAWs. As noted above, the CISP and the detailed design specifications would only dictate that SAWs comply with certain security requirements; the Participants would still be responsible for building the internal architecture of their SAWs, for providing the analytical tools to be used in their SAWs, and for importing any desired external data into their SAWs. Accordingly, proposed Section 6.13(c)(iii) would explicitly state that the Participants may provide and use their choice of software, hardware, and additional data within their SAWs, so long as such activities otherwise comply with the CISP and the detailed design specifications developed by the Plan Processor pursuant to proposed Section 6.13(b)(i). The Commission preliminarily believes that this provision would provide the Participants with sufficient flexibility in and control over the use of their SAWs, while still maintaining the security of the SAWs and the CAT Data that may be contained therein.[101]

The Commission requests comment on proposed Section 6.13(c). Specifically, the Commission solicits comment on the following:

31. The proposed amendments would require the Plan Processor to monitor each Participant's SAW in accordance with the detailed design specifications developed by the Plan Processor pursuant to proposed Section 6.13(b)(i). Instead of specifying that such monitoring should be conducted in accordance with the detailed design specifications developed by the Plan Processor pursuant to proposed Section 6.13(b)(i), should the proposed amendments specify the nature of the access and monitoring required by relevant NIST 800–53 controls? Should the proposed amendments specify the nature of the monitoring required by NIST SP 800–53 controls? Should the proposed amendments specify that monitoring should be continuous? If so, please explain how that term should be defined and why such definition would be appropriate. If not, please explain how often such monitoring should be conducted and explain why. Should the proposed amendments indicate whether manual or automated processes (or both) should be used by the Plan Processor and whether automated support tools should be used?

32. The proposed amendments would restrict the Plan Processor to monitoring SAWs for compliance with the CISP and with the detailed design specifications developed pursuant to Section 6.13(b)(i). Is this an appropriate limitation?

33. Is the Plan Processor the right party to monitor each Participant's SAW for compliance with the CISP and with the detailed design specifications developed pursuant to Section 6.13(b)(i)? If a different party should

[97] The proposed amendments would require the Participant to comply with the CISP and the detailed design specifications developed by the Plan Processor pursuant to proposed Section 6.13(b)(i). *See* proposed Section 6.13(c)(ii). If adopted, these requirements would be part of the CAT NMS Plan. Any non-compliance by a Participant with the proposed amendments would constitute non-compliance with the CAT NMS Plan and Rule 613(h)(1) and would also be a systems compliance issue, as defined in Regulation SCI, by such Participant (each Participant being an SCI entity). *See* 17 CFR 242.613(h)(1) (requiring Participants to comply with the provisions of the CAT NMS Plan); 17 CFR 242.608(c) (''Each self-regulatory organization shall comply with the terms of any effective national market system plan of which it is a sponsor or a participant.''). *See also* 17 CFR 242.1000 (defining ''systems compliance issue'' as ''an event at an SCI entity that has caused any SCI system of such entity to operate in a manner that does not comply with the [Exchange] Act and the rules and regulations thereunder,'' defining ''SCI event'' to include ''systems compliance issues,'' and defining ''SCI entity'' to include self-regulatory organizations like the Participants); 17 CFR 242.1002 (setting forth the notification and recordkeeping obligations related to SCI events).

[98] This provision would require each Participant to remedy any non-compliance promptly, whether such non-compliance was identified by the Participant or by the Plan Processor.

[99] Similarly, any SAW operated by the Commission would only be subject to monitoring for compliance with the CISP and with the detailed design specifications developed by the Plan Processor pursuant to Section 6.13(b)(i). *See* Part II.N. *infra* for further discussion regarding how the proposed amendments would apply to Commission staff.

[100] Determining whether remediation is prompt may depend on the facts and circumstances surrounding the non-compliance event. The Commission understands that the Plan Processor has developed a risk management policy that outlines appropriate timeframes for remediation based on the risks associated with the non-compliance event, and the Commission preliminarily believes that referring to this policy may be one way of determining whether remediation is prompt under the proposed amendments.

[101] The Commission would have the same flexibility in and control over the use of its SAW. *See* Part II.N. *infra* for further discussion regarding the application of the proposed amendments to Commission staff. The proposed amendments would not prevent the importation of existing third-party or in-house applications or analytical tools into the SAWs, the migration of external data into the SAWs, or the configuration of the internal architecture of the SAWs.

conduct this monitoring, please identify that party and explain why it would be a more appropriate choice. Is there a different set of standards that should control the monitoring process? If so, please identify that set of standards and explain why it is a more appropriate choice.

34. The proposed amendments would require the Plan Processor to notify the Participant of any identified non-compliance with the CISP or the detailed design specifications developed by the Plan Processor pursuant to proposed Section 6.13(b)(i). Should a different party notify the Participant of any identified non-compliance? If so, please identify that party and explain why it would be appropriate for them to provide the notification. Are there any additional parties that the Plan Processor should notify of any identified non-compliance—for example, the Security Working Group or the Operating Committee? If so, please identify the party or parties that should also be notified, explain why such notification would be appropriate, and explain whether such notification would raise any confidentiality, security, or competitive concerns.

35. The proposed amendments would specify that the Participants must comply with the CISP and the detailed design specifications developed pursuant to Section 6.13(b)(i). Should the proposed amendments specify that the Participants must comply with any other security protocols or industry standards? If so, please identify these security protocols or industry standards and explain why it would be appropriate to require the Participants to comply with them.

36. Should the proposed amendments specify a process to govern the resolution of potential disputes regarding non-compliance identified by the Plan Processor? For example, should the proposed amendments permit Participants to appeal to the Operating Committee? If such an appeal process should be included in the proposed amendments, please identify all aspects of that appeal process in detail and explain why those measures would be appropriate. How long should a Participant be given to make such an appeal and what materials should be provided to the Operating Committee? Would it be appropriate to require a Participant to appeal the determination to the Operating Committee within 30 days? Is 30 days enough time for a Participant to prepare an appeal? How long should the Operating Committee have to issue a final determination? Would 30 days be sufficient? Should the final determination be required to include a written explanation from the Operating Committee supporting its finding? Once the final determination has been issued, how long should the Participant be given to remediate any non-compliance that is confirmed by the Operating Committee's determination? Should Participants who are appealing to the Operating Committee be permitted to continue to connect to the Central Repository while such an appeal is pending?

37. Is it appropriate to require the Participants to promptly remediate any identified non-compliance or should another standard be used? Should the proposed amendments specify what would qualify as ''prompt'' remediation? If so, please explain what amount of time should be specified and explain why that amount of time is sufficient. Would it be appropriate for the proposed amendments to refer specifically to the risk management policy developed by the Plan Processor for appropriate remediation timeframes? Is there another policy that provides remediation timeframes that would be more appropriate for these purposes? If so, please identify that policy and explain why it would be a better benchmark.

38. The proposed amendments clarify that the Participants may provide and use their choice of software, hardware, and additional data within the SAWs, so long as such activities otherwise comply with the CISP. Is it appropriate to provide Participants with this level of flexibility in and control over their use of the SAWs?

39. The proposed amendments do not require the Plan Processor to customize each SAW account for Participant use. Should the proposed amendments require the Plan Processor to provide each Participant with a SAW that already has certain analytic capabilities or internal architecture built into it? If so, please explain why that would be more appropriate and identify what analytic capabilities or internal architecture the Plan Processor should provide. Should the Plan Processor be required to take specific and individual instructions from each Participant as to how each SAW should be built? Should the proposed amendments specify that each SAW should be of a certain size and/or capable of supporting a certain amount of data? If so, please explain what parameters would be appropriate.

5. Exceptions to the SAW Usage Requirements

As explained above, the Commission preliminarily believes that the CAT NMS Plan should be amended to better protect CAT Data accessed via the user-defined direct query or bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2 of the CAT NMS Plan, as the current CAT NMS Plan does not limit the download capabilities associated with these tools.[102] The Commission, however, recognizes that some Participants may have a reasonable basis for not using a SAW to access CAT Data via the user-defined direct query or bulk extract tools and may have built a sufficiently secure non-SAW environment in which these tools may be employed. The Commission therefore proposes to add provisions to the CAT NMS Plan that would set forth a process by which Participants may be granted an exception from the requirement in proposed Section 6.13(a)(i)(B) of the CAT NMS Plan to use a SAW to access CAT Data through the user-defined direct query and bulk extract tools.[103] The Commission also proposes to add provisions to the CAT NMS Plan that would set forth implementation and operational requirements for any non-SAW environments granted such an exception.

a. Exception Process for Non-SAW Environments

The proposed amendments would permit a Participant to be granted an exception to employ the user-defined direct query and bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2 of the CAT NMS Plan in a non-SAW environment. Proposed Section 6.13(d)(i)(A) would require the Participant requesting the exception to provide the Plan Processor's CISO, the CCO, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group with various application materials. First, the Participant would be required to provide a security assessment of the non-SAW environment, conducted within the prior twelve months by a named, independent third party security assessor,[104] that (a) demonstrates the extent to which the non-SAW environment complies with the NIST SP 800–53 security controls and associated

[102] *See also* Part II.C. *supra.*

[103] Only transactional data can be accessed through the user-defined direct query and bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2 of the CAT NMS Plan. Therefore, the proposed exception process would not permit the Participants to access Customer and Account Attributes data in a non-SAW environment.

[104] For the purposes of the proposed amendments, affiliates of a Participant would not be considered ''independent third party security assessors.''

policies and procedures required by the CISP pursuant to Section 6.13(a)(ii), (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 the user-defined direct query or bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2 of the CAT NMS Plan, and (c) includes a Plan of Action and Milestones document detailing the status and schedule of any corrective actions recommended by the assessment.[105] Second, the Participant would be required to provide 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 proposed Section 6.13(b)(i), and (b) that the design specifications will enable the operational requirements set forth for non-SAW environments in proposed Section 6.13(d)(iii), which include, among other things, Plan Processor monitoring.[106]

Proposed Section 6.13(d)(i)(B) would then require the CISO and the CCO to simultaneously notify the Operating Committee and the requesting Participant of their determination within 60 days of receipt of these application materials. Under the proposed amendments, the CCO and CISO may jointly grant an exception if they determine, in accordance with policies and procedures developed by the Plan Processor, that the residual risks [107] 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.[108] This standard effectively subjects each non-SAW environment to the same risk management policy as the CAT System itself, as the Commission preliminarily believes that the Participant applying for the exception should demonstrate that the CAT Data in its non-SAW environments will be protected in a similar manner as CAT Data within the CAT System.

If the exception is granted or denied, the proposed amendments would require the CISO and the CCO to provide the requesting Participant [109] with a detailed written explanation setting forth the reasons for that determination. For applications that are denied, the proposed amendments would further require the CISO and the CCO to specifically identify the deficiencies that must be remedied before an exception could be granted.[110]

The proposed amendments state that continuance of any exceptions that are granted is dependent upon an annual review process.[111] To continue an exception, the proposed amendments would require the requesting Participant to provide a new security assessment that complies with the requirements of proposed Section 6.13(d)(i)(A)(1) and up-to-date versions of the materials required by proposed Section 6.13(d)(i)(A)(2) to the CISO, the CCO, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group at least once a year, as measured from the date that the initial application materials were submitted.[112] Exceptions would be revoked by the CISO and the CCO for Participants who do not submit these application materials on time, in accordance with remediation timeframes developed by the Plan Processor.[113] Such Participants would be required to cease using their non-SAW environments to access CAT Data through the user-defined direct query and bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2 of the CAT NMS Plan.[114]

Within 60 days of receipt of these updated application materials, the CISO and the CCO would then be required to simultaneously notify the Operating Committee and the requesting Participant of their determination.[115] The proposed amendments would require the CISO and the CCO to make this determination using the same criteria, and issue that determination following the same process, set forth for initial exceptions.[116] Participants that receive a determination granting a continuance would be required to repeat this process annually; participants that receive a determination denying a continuance would be required by the CISO and the CCO to cease using the user-defined direct query and bulk extract tools to access CAT Data in their non-SAW environments in accordance with the remediation timeframes developed by the Plan Processor.[117]

The proposed exception process is designed to help improve the security of CAT Data while allowing the Participants some flexibility in how they access CAT Data. Participants may have reasons for needing to use a non-SAW environment to access CAT Data, including, for example, reduction of burdensome costs and/or operational complexity. The Commission therefore preliminarily believes it is appropriate to provide the Participants with the option to use non-SAW environments, if that can be accomplished in a manner that will not compromise the overall security of CAT Data. To that end, the proposed exception process would not

[105] *See* proposed Section 6.13(d)(i)(A)(1). NIST SP 800–53 defines a Plan of Action and Milestones document as a ''document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.'' *See* NIST SP 800–53, *supra* note 15, at B–16.

[106] *See* proposed Section 6.13(d)(i)(A)(2). *See also* proposed Section 6.13(d)(iii); Part II.C.5.b. *infra,* for a discussion of the operational requirements that must be enabled by the design specifications for a non-SAW environment.

[107] By ''residual risks,'' the Commission means any risks that are associated with the absence of a security control or the deficiency of a security control, as evaluated by the required security assessment.

[108] *See* proposed Section 6.13(d)(i)(B)(1). NIST SP 800–53 requires the Plan Processor to develop an organization-wide risk management strategy that includes, among other things, ''an unambiguous expression of the risk tolerance for the organization . . . .'' *See* NIST SP 800–53, *supra* note 15, at Appendix G–6 (providing supplemental guidance for the PM–9 control).

[109] *See* proposed Section 6.13(d)(i)(B)(1).

[110] *See* proposed Section 6.13(d)(i)(B)(2). Denied Participants would be permitted to re-apply for an exception, after remedying the deficiencies identified by the CISO and the CCO, by submitting a new security assessment that complies with the requirements of proposed Section 6.13(d)(i)(A)(1) and up-to-date versions of the materials specified in proposed Section 6.13(d)(i)(A)(2). *See* proposed Section 6.13(d)(i)(C).

[111] *See* proposed Section 6.13(d)(ii).

[112] *See* proposed Section 6.13(d)(ii)(A).

[113] *See id.* The Commission understands that the Plan Processor has developed a risk management policy that outlines appropriate timeframes for remediation based on the risks presented by a non-compliance event, and the Commission preliminarily believes that referring to this policy would be an appropriate method for determining what timeframe is appropriate for revoking a Participant's exception.

[114] *See* proposed Section 6.13(d)(ii)(C).

[115] *See* proposed Section 6.13(d)(ii)(B). *See also* proposed Section 6.2(a)(v)(S) (requiring the CCO to determine, pursuant to Section 6.13(d), whether a Participant should be granted an exception from Section 6.13(a)(i)(B) and, if applicable, whether such exception should be continued); proposed Section 6.2(b)(ix) (requiring the CISO to determine, pursuant to Section 6.13(d), whether a Participant should be granted an exception from Section 6.13(a)(i)(B) and, if applicable, whether such exception should be continued).

[116] *See* proposed Section 6.13(d)(ii)(B). Likewise, denied Participants would be permitted to re-apply following the same process that was outlined above for initial exceptions. *See* proposed Section 6.13(d)(ii)(C); *see also* note 110 *supra.*

[117] *See* proposed Section 6.13(d)(ii)(A); proposed Section 6.13(d)(ii)(C). *See also* note 113 *supra.* Denied Participants would be permitted to re-apply for an exception, after remedying the deficiencies identified by the CISO and the CCO, by submitting new and updated versions of the application materials that have been prepared within twelve months of the date of submission. *See* proposed Section 6.13(d)(ii)(C).

permit the Participants to access Customer and Account Attributes data in a non-SAW environment; only transactional data is retrievable through the user-defined direct query or bulk extract tools described by Section 6.10(c)(i)(B) and Appendix D, Section 8.2 of the CAT NMS Plan.[118] Non-SAW environments meeting the requirements outlined above may provide a sufficient level of security for all CAT Data, but it is of paramount importance that access to Customer and Account Attributes data is guarded by the highest possible level of protection. Because the Commission preliminarily believes that such protection is only available through the use of a SAW environment and through the proposed limitations on the extraction of Customer and Account Attributes data from a SAW environment,[119] the proposed exception process would not apply to Customer and Account Attributes data.

With respect to the specific features of the proposed exception process, the Commission preliminarily believes it is appropriate to require Participants seeking an exception to provide the CISO and the CCO with the proposed application materials, because such materials should provide critical information to the parties responsible for deciding whether to grant an exception.[120] The proposed requirement that the Participant produce a security assessment conducted within the last twelve months by an independent and named third party should give these decision-makers access to up-to-date, accurate, and unbiased information about the security and privacy controls put in place for the relevant non-SAW environment, including reliable information about risk mitigation measures and recommended corrective actions.[121] The Commission also preliminarily believes that it is appropriate, as part of this security assessment, to require the requesting Participant to demonstrate 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 pursuant to proposed Section 6.13(a)(ii), to explain whether and how the Participant's security and privacy controls mitigate the risks associated with extracting CAT Data to the non-SAW environment, and to include a Plan of Action and Milestones document detailing the status and schedule of any recommended corrective actions.[122] The CAT NMS Plan requires the Plan Processor to perform similar security assessments to verify and validate the security of the CAT System,[123] so the Commission preliminarily believes that it is reasonable to require a Participant seeking to export CAT Data outside of the CAT System to demonstrate a similar level of due diligence and a similar level of security as would be required for SAWs pursuant to proposed Section 6.13(a)(ii). The Commission also preliminarily believes that this information will help the CISO and the CCO to determine whether the non-SAW environment is sufficiently secure to be granted an exception from the SAW usage requirements set forth in proposed Section 6.13(a)(i)(B).[124]

Similarly, the Commission preliminarily believes that it is appropriate to require the requesting Participant to provide detailed design specifications for its non-SAW environment that demonstrate the extent of adherence to the SAW design specifications developed by the Plan Processor pursuant to Section 6.13(b)(i). The detailed design specifications developed by the Plan Processor pursuant to proposed Section 6.13(b)(i) would implement the access, monitoring, and other technical controls of the CISP that are applicable to SAWs. Requiring Participants seeking an exception to the SAW usage requirements to demonstrate whether the design specifications for their non-SAW environment adhere to the SAW design specifications would therefore provide the CISO and the CCO with specific technical information regarding the security capabilities of the non-SAW environment and may therefore prove more informative than the review of the Participant's information security policies for comparability that is currently required by Section 6.2(b)(vii) of the CAT NMS Plan. The Commission further preliminarily believes that it is appropriate to require the requesting Participant to demonstrate that the design specifications will enable the proposed operational requirements for non-SAW environments.[125] This information would help the CISO and the CCO to assess the security-related infrastructure of the non-SAW environment and whether the non-SAW environment would support the required non-SAW operations.[126]

The Commission preliminarily believes that it is also appropriate for the members of the Security Working Group (and their designees) and Commission observers of the Security Working Group to receive the above-described application materials.[127] Although the Security Working Group is not a decision-maker under the proposed amendments, the Commission preliminarily believes that it would be in the public interest to enable both the decision-makers and the members of the Security Working Group (and their designees)—a body of information security experts that would be specifically established to assess and protect the security of the CAT—to review any application materials. Given the expertise of its members, which would include the chief or deputy chief information security officer for each Participant, the Security Working Group may be able to provide valuable feedback to the CISO and the CCO regarding any request for an exception to the SAW usage requirements.[128] Moreover, by providing the application materials to the Commission observers of the Security Working Group, the Commission preliminarily believes that

[118] *See, e.g.,* CAT NMS Plan, *supra* note 3, at Appendix D, Section 4.1.6 (''PII data must not be included in the result set(s) from online or direct query tools, reports or bulk data extraction. Instead, results will display existing non-PII unique identifiers (*e.g.,* Customer-ID or Firm Designated ID).'').

[119] *See* Part II.C.2. *supra* for additional discussion of these proposed limitations.

[120] Certain aspects of the proposed amendments put the burden of proof on the requesting Participant. For example, in its application, the Participant would be required to demonstrate that the non-SAW environment complies with the NIST SP 800–53 security controls required by the CISP pursuant to proposed Section 6.13(a)(ii) and that the design specifications enable the operational requirements for non-SAW environments. The Commission preliminarily believes that this is the most appropriate and efficient approach; the party seeking an exception from the security requirements of the CAT should be required to bear the burden of demonstrating that such an exception is justified, and the requesting Participant will be better situated to marshal evidence to prove that its systems are secure than would be the CISO, the CCO, or the Security Working Group.

[121] *See* proposed Section 6.13(d)(i)(A)(1).

[122] *See id.*

[123] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 5.3 (''The Plan Processor must conduct third party risk assessments at regular intervals to verify that security controls implemented are in accordance with NIST SP 800–53.'').

[124] *See* proposed Section 6.13(d)(i)(B)(1).

[125] *See* note 106 *supra.*

[126] *See* proposed Section 6.13(d)(iii).

[127] *See* proposed Section 6.13(d)(i)(A). The proposed amendments specifically limit the distribution of the application materials to members of the Security Working Group and their designees so that the confidentiality obligations of Section 9.6 of the CAT NMS Plan will apply to protect the sensitive information contained in the application materials. *See* note 30 *supra.*

[128] The Commission does not preliminarily believe that competitive relationships between the Participants would affect how individual members of the Security Working Group review the application materials and advise the CISO and the CCO, because each Participant has an overriding interest in the security of the CAT. *See* CAT NMS Plan, *supra* note 3, at Appendix C (indicating that the CAT will be a facility of each Participant); *see also* Part IV.A.2. *infra* for further discussion of this concern.

the proposed amendments will better facilitate Commission oversight of the security of CAT Data.

The Commission preliminarily believes, however, that only the CISO and the CCO should be the decision-makers regarding any requested exceptions. Not only are the CISO and the CCO fiduciaries to the Plan Processor and to the Company,[129] but they also have the most experience, knowledge, and expertise regarding the overall operation of the CAT, the state of the CAT's security, and compliance with the CAT NMS Plan. These two officers are likely to be the best situated to identify any issues that may be raised by applications for exceptions from the SAW usage requirements. As the decision-makers, the CISO and the CCO would ultimately be responsible under the proposed amendments for determining whether an exception from the SAW usage requirements may be granted.

The proposed amendments state that the CISO and the CCO must simultaneously notify the Operating Committee and the requesting Participant of their determination within 60 days of receiving the above-described application materials.[130] The Commission preliminarily believes that the proposed 60-day review period provides the CISO and the CCO with sufficient time to examine, analyze, and investigate the application materials. Moreover, the Commission preliminarily believes that this limitation should also provide the requesting Participant with some amount of certainty regarding the length of the review period and the date by which a determination will be issued, which could be useful for planning purposes.[131]

The proposed amendments also specify that an exception may only be granted if the CISO and the CCO determine, in accordance with policies 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.[132] The Commission preliminarily believes that it is appropriate to identify the conditions under which an exception from the SAW usage requirements may be granted. By making it clear that an exception may only be granted if an objective standard is met or exceeded, the proposed amendments should facilitate a consistent and fair decision-making process.[133]

Furthermore, the Commission preliminarily believes that is it appropriate to require the CISO and the CCO to determine, in accordance with policies 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. This criterion would prohibit granting an exception to non-SAW environments that are not sufficiently secure to house CAT Data.

As noted above, the Commission preliminarily believes that it is important that the review by the CISO and the CCO be consistent and fair, and transparency will advance both objectives. The proposed amendments therefore include measures designed to protect the transparency of the review process. First, the CISO and the CCO would be required to simultaneously notify both the requesting Participant and the Operating Committee of their determination.[134] This requirement is designed to provide the Operating Committee with the most up-to-date information about non-SAW environments that house CAT Data. Second, the CISO and the CCO would be required to provide the Participant with a detailed written explanation setting forth the reasons for their determination and, for denied Participants, specifically identifying the deficiencies that must be remedied before an exception could be granted.[135] The Commission preliminarily believes that this kind of feedback could be quite valuable—not only because it should require the CISO and the CCO to thoroughly review an application and to identify and articulate any deficiencies, but also because it should provide denied Participants with the information needed to effectively bring their non-SAW environments into compliance with the proposed standards.[136]

For exceptions that are granted, the proposed amendments would require the requesting Participant to seek a continuance of this exception by initiating an annual review process through the submission of a new security assessment that complies with the requirements of proposed Section 6.13(d)(i)(A)(1) and up-to-date application materials at least once a year, as measured from the date that the initial application materials were submitted. Participants that fail to submit updated application materials on time would have their exceptions revoked in accordance with the remediation timelines developed by the Plan Processor, and the proposed amendments would require such Participants to cease using their non-SAW environments to access CAT Data through the user-defined direct query or bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2 of the CAT NMS Plan.

These proposed requirements essentially would impose an annual term on any exception granted by the CISO and the CCO. The Commission preliminarily believes that this limitation is appropriate. Technology and security concerns are constantly and rapidly evolving, and the conditions that might justify the initial grant of an exception from the proposed SAW usage requirements may no longer be in place at the end of an annual term.[137] Accordingly, the Commission

[129] *See* CAT NMS Plan, *supra* note 3, at Section 4.6(a), Section 4.7(c). In addition, to the extent that competitive relationships between the Participants may affect how individual members of the Security Working Group review the application materials and advise the CISO and the CCO, the Commission preliminarily believes that identifying the CISO and the CCO as the decision-makers will protect against any such bias in the review process. *See* Part IV.A.2. *infra* for further discussion of the Security Working Group.

[130] *See* proposed Section 6.13(d)(i)(B).

[131] Participants that choose to rely solely on a non-SAW environment for certain surveillance or regulatory functions may not be able to perform those functions unless and until an exception is granted; therefore, placing a time limit on the review period may help these Participants to stage their resources appropriately.

[132] *See* proposed Section 6.13(d)(i)(B)(1).

[133] Similarly, the Commission believes that requiring the CISO and the CCO to reach their determination in accordance with policies developed by the Plan Processor will facilitate a consistent and fair decision-making process. *See id.*

[134] *See* proposed Section 6.13(d)(i)(B)(1)–(2). The Commission preliminarily believes that the Advisory Committee generally should be notified when the Operating Committee is notified.

[135] *See* proposed Section 6.13(d)(i)(B)(2).

[136] *See* proposed Section 6.13(d)(i)(C). The Commission does not believe that a formal appeals process is appropriate or necessary. However, the Commission preliminarily believes that a denied Participant should not be barred from re-applying for an exception from the SAW usage requirements set forth in proposed Section 6.13(a)(i)(B) if a Participant is able to remediate the issues identified by the CISO and the CCO.

[137] This annual term is also consistent with existing requirements in the CAT NMS Plan that the Plan Processor's performance be evaluated on at least an annual basis. *See* CAT NMS Plan, *supra* note 3, at Section 6.6(b). The Commission preliminarily believes it is reasonable to require a Participant seeking to export CAT Data outside of the CAT System to be evaluated with a similar frequency.

preliminarily believes that it is appropriate to require a requesting Participant to provide a new security assessment and up-to-date design specifications for the non-SAW environment. Updated design specifications may adequately capture any technical changes made to a non-SAW environment over the course of a year, but the Commission preliminarily believes that a more in-depth approach is needed with respect to the required security assessment. Requiring the requesting Participant to provide a new security assessment that complies with the requirements of proposed Section 6.13(d)(i)(A)(1)—as opposed to an updated version of the security assessment provided with the initial application—would better identify and describe any risks presented by a non-SAW environment, based on the current security control implementation of the Participant.

For similar reasons, the Commission preliminarily believes that the proposed continuance process is appropriate. The proposed continuance process is substantially identical to the proposed process for initial exceptions; it requires that the requesting Participant submit a new security assessment that complies with the requirements of proposed Section 6.13(d)(i)(A)(1) and up-to-date versions of the materials required by proposed Section 6.13(d)(i)(A)(2) to the CISO, the CCO, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group and that the CCO and CISO notify the Operating Committee and the requesting Participant of their determination, using the same criteria and process outlined for the initial exception process, within 60 days of receiving those application materials. The Commission preliminarily does not believe that it is appropriate to lighten the requirements for the continuance process. To best protect the CAT and CAT Data, Participants seeking a continued exception to the SAW usage requirements should not be allowed to meet a lesser standard for continuance than was required for the initial exception.[138] Because technology and security concerns are constantly evolving, as noted above, the Commission preliminarily believes it is crucial to implement a continuance process that emphasizes regular and consistent reevaluation of the security of non-SAW environments.

Finally, and for the same reasons expressed above, the Commission preliminarily believes it is appropriate for the proposed amendments to cut off access to the user-defined direct query and bulk extract tools if a Participant is denied a continuance or fails to submit updated application materials in a timely manner. Participants should not be indefinitely allowed to continue to access large amounts of CAT Data outside the security perimeter of the CAT without an affirmative determination that their systems are secure enough to adequately protect that information. However, the Commission preliminarily believes that the risks involved with permitting a Participant to continue using a non-SAW environment, after its exception has lapsed and while transitioning into a SAW, will likely depend on the facts and circumstances related to that particular Participant and the way it uses the non-SAW environment. Immediate revocation of access to CAT Data may be appropriate in some situations, particularly where a significant risk is posed to CAT Data, but a long transition period may be more appropriate in other situations. Requiring an exception to be revoked by the CISO and the CCO in accordance with remediation timeframes developed by the Plan Processor would allow the CISO and the CCO to take into account any relevant facts and circumstances and to craft an appropriate response to the presented risks.

The Commission requests comment on the proposed exception process. Specifically, the Commission solicits comment on the following:

40. Should Participants be permitted to seek an exception from the requirement in proposed Section 6.13(a)(i)(B) to use a SAW to access CAT Data through the user-defined direct query and bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2 of the CAT NMS Plan? Should Participants only be able to employ user-defined direct query and bulk extract tools in connection with a SAW?

41. As noted above, Customer and Account Attributes data is not available through the user-defined direct query and bulk extraction tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2 of the CAT NMS Plan. Therefore, the proposed amendments would not permit any Participants to access Customer and Account Attributes in a non-SAW environment via the exceptions process. Should Participants be allowed to access Customer and Account Attributes data in a non-SAW environment approved by the CISO and the CCO? If so, please explain under what circumstances such access should be allowed and what limits, if any, should be applied.

42. The proposed amendments would require the requesting Participant to submit to CISO, the CCO, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group the following materials: (1) A security assessment of the non-SAW environment, conducted within the last twelve 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 pursuant to proposed Section 6.13(a)(ii), (b) explains whether and how the Participant's security and privacy controls mitigate the risks associated with exporting CAT Data to the non-SAW environment through the user-defined direct query or bulk extraction tools, and (c) includes a Plan of Action and Milestones document detailing the status and schedule of any corrective actions recommended by the assessment; and (2) 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 proposed Section 6.13(b)(i), and (b) that the design specifications will enable the operational requirements set forth for non-SAW environments in proposed Section 6.13(d)(iii).

a. Is it appropriate to require that the requesting Participant submit a security assessment of the non-SAW environment that has been conducted by a named, independent third party security assessor within the last twelve months? Should the Commission require that a more recent security assessment be submitted or permit a less recent security assessment to be submitted? If so, how recent should the security assessment be? Please explain. Would the security assessment be as reliable if the Commission eliminated the requirement that it be conducted by a named, independent third party security assessor?

b. Is it appropriate to require that the proposed security assessment demonstrate the extent to which the non-SAW environment complies with

[138] For similar reasons, the Commission believes it is appropriate to require denied Participants to re-apply by submitting a new security assessment that complies with the requirements of proposed Section 6.13(d)(i)(A)(1) and up-to-date materials that comply with the requirements of proposed Section 6.13(d)(i)(A)(2) and by subjecting their non-SAW environments to the same review processes used for initial evaluations.

the NIST SP 800–53 security controls and associated policies and procedures required by the CISP established pursuant to proposed Section 6.13(a)(ii)? Would a different set of security and privacy controls be more appropriate? If so, please identify that set of security and privacy controls and explain in detail why that standard would be a better benchmark. Would it be more appropriate to require the non-SAW environment to demonstrate compliance with the security and privacy controls described in NIST SP–800–53 for low, moderate, and high baselines, as described in NIST SP 800–53? If so, please indicate which benchmark would be more appropriate and explain why.

c. Is it appropriate to require that the proposed security assessment explain whether and how the Participant's security and privacy controls mitigate the risks associated with exporting CAT Data to the non-SAW environment through the user-defined direct query or bulk extraction tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2 of the CAT NMS Plan?

d. Is it appropriate to require that the proposed security assessment include a Plan of Action and Milestones document detailing the status and schedule of any recommended corrective actions?

e. Are there any other items that should be included in the security assessment, including any items that would assist the CISO and the CCO to determine whether the non-SAW environment is sufficiently secure to be granted an exception from the SAW usage requirements set forth in proposed Section 6.13(a)(i)(B)? Please identify these items and explain why they should be included.

f. Is it appropriate to require that the requesting Participant provide detailed design specifications for its non-SAW environment that demonstrate the extent of adherence to the SAW design specifications developed by the Plan Processor pursuant to proposed Section 6.13(b)(i)? Is a different set of design specifications a better benchmark by which to judge the non-SAW environment's operational capabilities? If so, please identify that set of design specifications and explain why it is more appropriate. The proposed amendments also require that the requesting Participant demonstrate that the submitted design specifications will enable the proposed operational requirements for non-SAW environments under proposed Section 6.13(d)(iii). Is this an appropriate requirement?

g. Is it appropriate to require that the proposed application materials be submitted to the CISO, the CCO, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group? Should any different or additional parties receive the proposed application materials? If so, please identify those parties and explain why they should receive the proposed application materials. Does the inclusion of the members of the Security Working Group and their designees raise any confidentiality, security, or competitive concerns? If so, please identify such concerns and explain whether the benefits of including the Security Working Group nevertheless justify providing the members of the Security Working Group and their designees with the required application materials.

43. The proposed amendments state that the CISO and the CCO must notify the Operating Committee and the requesting Participant of their determination regarding an exception (or a continuance) within 60 days of receiving the application materials described in proposed Section 6.13(d)(i)(A).

a. Is it appropriate to require that the CISO and the CCO make this determination? If it is not appropriate to require the CISO and the CCO to make this determination, which party or parties should be required to make this determination? Please explain why those parties would be appropriate decision-makers.

b. Is it appropriate that the CISO and the CCO simultaneously notify the Operating Committee and the requesting Participant of their determination? Should the Participant be notified before the Operating Committee? If so, how long should the CISO and the CCO be required to wait before notifying the Operating Committee? Are there any different or additional parties that should receive the determination? If so, please identify those parties and explain why it would be appropriate for them to receive the determination issued by the CISO and the CCO. For example, should the proposed amendments require notification of the Advisory Committee, even though the Advisory Committee is likely to be informed of these determinations in regular meetings of the Operating Committee? Would notification of the Advisory Committee raise any security or confidentiality concerns, such that these matters should only be addressed in executive sessions of the Operating Committee? Should the rule specify that any issues related to exceptions should only be discussed in executive sessions of the Operating Committee? Does a Participant's application for an exception create circumstances in which it would be appropriate to exclude non-Participants from discussion of such applications? Should the Participants be required to submit requests to enter into an executive session of the Operating Committee on a written agenda, along with a clearly stated rationale for each matter to be discussed? If so, should each such request have to be approved by a majority vote of the Operating Committee?

c. Is it appropriate to require the CISO and the CCO to make their determination within 60 days of receiving the application materials? If a different review period would be more appropriate, please state how much time the CISO and the CCO should have to review the application materials and explain why that amount of time would be more appropriate.

d. Should the proposed amendments include provisions allowing the CISO and the CCO to extend the review period? If so, what limitations should be placed on their ability to extend the review period?

44. The proposed amendments specify that an exception (or a continuance) may only be granted if the CISO and the CCO 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 pursuant to proposed Section 6.13(d)(i)(A) or proposed Section 6.13(d)(ii)(A) 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.

a. This standard puts the burden of proof on the requesting Participant. Is that appropriate? If it is inappropriate, please identify the party that should bear the burden of proof and explain why putting the burden of proof on that party is a better choice.

b. Is it appropriate for the proposed amendments to specify the exact conditions under which an exception (or a continuance) may be granted? Should the CISO and the CCO be required to make any specific findings before granting an exception? If so, please state what these findings should be and explain why they would be appropriate requirements. Are there any conditions that should bar the CISO and the CCO from granting an exception (or a continuance)? If so, please identify these conditions and explain why they are appropriate.

c. Is it appropriate to specify that an exception (or a continuance) may not be granted unless the CISO and the CCO determine, in accordance with policies and procedures developed by the Plan Processor, that the residual risks identified in the provided security assessment or detailed design specifications 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? Should the proposed amendments use a different set of risk tolerance levels as a benchmark? If so, please explain what risk tolerance levels should be used and why those levels would be more appropriate. Should the CISO and the CCO determine whether to grant an exception using a different standard of review? If so, please describe the standard of review that should be used and why that standard would be more appropriate. Should the CISO and the CCO make their determination in accordance with policies and procedures developed by the Plan Processor? Should a different party develop these policies and procedures—for example, the Operating Committee? If so, please identify the party that should develop the policies and procedures and explain why it would be appropriate for that party to do so.

45. Is it appropriate to require the CISO and CCO to provide the requesting Participant with a detailed written explanation setting forth the reasons for that determination and, for denied Participants, specifically identifying the deficiencies that must be remedied before an exception (or a continuance) could be granted? Should the Operating Committee also be provided with this explanation? If so, should the CISO and the CCO be required to wait for a certain period of time before notifying the Operating Committee? How long should they be required to wait?

46. Should the proposed amendments provide a process for denied Participants to appeal to the Operating Committee, or is it sufficient that a denied Participant may re-apply for an exception after remedying the deficiencies identified by the CISO and the CCO, by submitting a new security assessment that complies with the requirements of proposed Section 6.13(d)(i)(A)(1) and up-to-date versions of the materials specified in proposed Section 6.13(d)(i)(A)(2)? If such an appeal process should be included in the proposed amendments, please identify all aspects of that appeal process and explain why those measures would be appropriate. How long should a denied Participant be given to make such an appeal and what materials should be included? Please explain your response in detail. For example, would it be appropriate to require a denied Participant to appeal the determination to the Operating Committee within 30 days by providing the Operating Committee with its most up-to-date application materials, the detailed written statement provided by the CISO and the CCO, and a rebuttal statement prepared by the denied Participant? Is 30 days enough time for a denied Participant to prepare an appeal? Should any additional materials be provided? If so, please describe those materials and describe why it would be helpful to provide them. How long should the Operating Committee have to issue a final determination? Would 30 days be sufficient? Should the final determination be required to include a written explanation from the Operating Committee supporting the finding? Once the final determination has been issued, should the requesting Participant be allowed to remedy any deficiencies and re-apply? Do different considerations apply to appeals brought by Participants denied the initial exception and appeals brought by Participants denied a continuance of an exception? If so, what are these considerations, and how should the appeal process for each type of Participant differ? Please explain in detail. Should Participants who are denied a continuance be permitted to continue to connect to the Central Repository while any appeal is pending, even if that would enable them to connect to the Central Repository beyond the remediation timeframes developed by the Plan Processor?

47. Is it appropriate to condition the continuance of any exception from the proposed SAW usage requirements on an annual review process to align with the Participants' review of the Plan Processor's performance? In light of the constantly-evolving nature of technology and security standards, should the continuance be evaluated more often? Should the continuance be evaluated less often? If so, please explain how often the continuance should be evaluated and why that frequency is appropriate.

48. The proposed amendments provide that an exception will be revoked if a Participant fails to submit a new security assessment that complies with the requirements of proposed Section 6.13(d)(i)(A)(1) and up-to-date versions of the materials specified by proposed Section 6.13(d)(i)(A)(2) at least once a year, as measured from the date that the initial application materials were submitted. Should another date be used to measure the annual review—for example, the date that the CISO and the CCO issue their joint determination granting the exception? If so, please identify the date that should be used and explain why that date is more appropriate.

49. Should the CISO and the CCO be enabled to revoke any exception at will, and prior to the expiration of the annual term, if they are able to determine that the residual risks presented in a security assessment or detailed design specifications for a non-SAW environment are no longer within 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 or if the Plan Processor identifies non-compliance with the detailed design specifications submitted by the requesting Participant? If the CISO and the CCO should be enabled to revoke the exception at will, should the proposed amendments set forth a process for appealing to the Operating Committee that should be followed before the exception is revoked and the non-SAW environment is disconnected from the Central Repository? If such an appeal process should be included, please identify all aspects of that appeal process and explain why those measures would be appropriate. How long should a revoked Participant be given to make such an appeal and what materials should be included? Please explain your response in detail. For example, should the CISO and the CCO be required to provide a revoked Participant with a detailed written statement setting forth the reasons for that determination and specifically identifying the deficiencies that must be remedied? Would it be appropriate to require a revoked Participant to appeal the determination to the Operating Committee within 30 days by providing the Operating Committee with the most up-to-date application materials, the detailed written statement provided by the CISO and the CCO, and a rebuttal statement prepared by the denied Participant? Is 30 days enough time for the revoked Participant to prepare an appeal? Should revoked Participants be permitted to connect to the Central Repository while an appeal is pending, even if such appeal would last beyond the remediation timeframe developed by the Plan Processor? Is 30 days too much time for a revoked Participant to be allowed to access CAT Data through the Central Repository if the CISO and the CCO have identified a deficiency? Should any additional materials be provided to the Operating Committee? If

so, please describe those materials and describe why it would be helpful to provide them. How long should the Operating Committee have to issue a final determination? Would 30 days be sufficient or too long? Should the final determination be required to include a written explanation by the Operating Committee supporting the finding? Once the final determination has been issued, should the requesting Participant be allowed to remedy any deficiencies and re-apply?

50. The proposed amendments provide that Participants who are denied a continuance, or Participants who fail to submit their updated application materials on time, must cease using their non-SAW environments to access CAT Data through the user-defined direct query and bulk extract tools in accordance with the remediation timeframes developed by the Plan Processor. Should the exception be revoked immediately and automatically? Are there other processes that would be more appropriate here? If so, please identify such processes and explain why those processes are appropriate. Should such Participants be provided a standard grace period in which to cease using this functionality in their non-SAW environments? If so, please explain how long this grace period should be and why such a grace period would be appropriate. Should the proposed amendments instead indicate that such Participants should promptly cease using their non-SAW environments to access CAT Data through the user-defined query and bulk extract tools or specify a specific timeframe? Should the proposed amendments require the CISO and the CCO to provide preliminary findings to Participants that will be denied a continuance, such that those Participants have the ability to minimize any disruption? Should the proposed amendments address how CAT Data already exported to non-SAW environments that lose their exception should be treated? If so, how should the proposed amendments treat such data? Should the proposed amendments require that all such CAT Data be immediately or promptly deleted? Should the Participants be allowed to retain this data in their non-SAW environment? If so, please explain why this would be appropriate in light of the Commission's security concerns. Would such data be sufficiently stale so as to pose a minimal security threat?

51. Is it appropriate to require that a Participant seeking a continued exception (or a Participant re-applying for an exception) provide a new security assessment that complies with the requirements of proposed Section 6.13(d)(i)(A)(1) and up-to-date versions of the materials specified by proposed Section 6.13(d)(i)(A)(2) to the CISO, the CCO, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group? Should a Participant seeking a renewed exception be allowed to provide an updated security assessment instead of a new security assessment? Should a Participant seeking a renewed exception be required to provide new design specifications instead of updated design specifications? Should a Participant seeking a renewed exception (or re-applying for an exception) be required to provide any additional materials? If so, please describe such additional materials and explain why such additional materials might be appropriate to include in an application for a renewed exception. Are there different or additional parties that should receive the application materials for a continued exception? If so, please identify these parties and explain why it would be appropriate for them to receive the application materials.

52. Is it appropriate for the CISO and the CCO to follow the same process and to use the same standards to judge whether to grant initial exceptions and continued exceptions? If the standards or process should be different, please explain which aspects should differ and explain why that would be appropriate.

b. Operation of Non-SAW Environments

To further safeguard the security of the CAT, the proposed amendments also include provisions that would govern how non-SAW environments are operated during the term of any exception granted by the CISO and the CCO.

Specifically, proposed Section 6.13(d)(iii)(A) would state that an approved Participant may not employ its non-SAW environment to access CAT Data through the user-defined direct query or bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2 until the Plan Processor notifies the Operating Committee that the non-SAW environment has achieved compliance with the detailed design specifications submitted by that Participant as part of its application for an exception (or continuance). This provision mirrors the proposed requirements set forth for SAWs [139] and serves the same purpose—namely, to protect the security of the CAT. The Commission preliminarily believes that it is important to require approved Participants to adhere to and implement the detailed design specifications that formed a part of their application packages, because such detailed design specifications will have been reviewed and vetted by the CISO, the CCO, and the Security Working Group.[140] Detailed design specifications for non-SAW environments that have been granted an exception by the CISO and the CCO should be detailed design specifications for an environment that does not exceed the risk tolerance levels set forth in the risk management strategy developed by the Plan Processor pursuant to NIST SP 800–53.[141] Therefore, the Commission preliminarily believes that non-SAW environments that implement their submitted design specifications should be sufficiently secure, and, for an additional layer of protection and oversight, the proposed amendments require the Plan Processor [142] to determine and notify the Operating Committee that the non-SAW environment has achieved compliance with such detailed design specifications before CAT Data can be accessed via the user-defined direct query or bulk extraction tools.

Proposed Section 6.13(d)(iii)(B) would require the Plan Processor to monitor the non-SAW environment in accordance with the detailed design specifications submitted with the exception (or continuance) application, for compliance with those detailed design specifications only,[143] and to notify the Participant of any identified non-compliance with such detailed

[139] *See, e.g.,* proposed Section 6.13(b); *see also* Part II.C.4. *supra,* for further discussion of these proposed requirements.

[140] *See* proposed Section 6.13(d)(i)(A), (d)(ii)(A).

[141] *See* proposed Section 6.13(d)(i)(B), (d)(ii)(B).

[142] The Commission preliminarily believes that the Plan Processor is best situated to perform this task. Under the proposed amendments, the Plan Processor will be required to perform a similar task for SAWs, *see* proposed Section 6.13(b)(ii), so the Plan Processor will be most familiar with the task and with similar design specifications. Moreover, the Plan Processor will be responsible for monitoring any approved non-SAW environments for compliance with the design specifications, so it makes sense to require the Plan Processor to perform the initial evaluation. *See* proposed Section 6.13(d)(iii)(B).

[143] The Commission preliminarily believes it is appropriate to limit the scope of the Plan Processor's monitoring to compliance with the detailed design specifications submitted by the Participant pursuant to proposed Section 6.13(d)(i)(A)(2) or proposed Section 6.13(d)(ii)(A). The Commission preliminarily believes that this limitation would protect the Participants by making it clear that analytical activities in their non-SAW environments would not be subject to monitoring by the Plan Processor, without hampering the ability of the Plan Processor to adequately protect the security of CAT Data.

design specifications.[144] This provision would also require the Participant to comply with the submitted design specifications and to promptly remediate any identified non-compliance.[145] Moreover, proposed Section 6.13(d)(iii)(C) would require the Participant to simultaneously notify the Plan Processor, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group of any material changes to its security controls for the non-SAW environment.

The Commission preliminarily believes that these requirements will improve the security of the non-SAW environments that are granted an exception by the CISO and CCO and, therefore, the overall security of the CAT. Requiring the Plan Processor to monitor each non-SAW environment that has been granted an exception for compliance with the submitted design specifications would help the Plan Processor to identify and notify the Participants of any non-compliance events, threats, and/or vulnerabilities, thus reducing the potentially harmful effects these matters could have if left unchecked and uncorrected.[146] The Commission also preliminarily believes that it is appropriate to require approved Participants to simultaneously notify the Plan Processor, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group of any material changes to the security controls for the non-SAW environment.[147] Exceptions would be granted after a review of a non-SAW environment's existing security controls, policies, and procedures, but the importance of such protocols does not end at the application stage. Therefore, if the security controls reviewed and vetted by the CISO, the CCO, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group change in any material way, the Commission preliminarily believes it is appropriate to require the escalation of this information to the party responsible for monitoring the non-SAW environment for compliance—the Plan Processor. The Commission also preliminarily believes that it is appropriate to simultaneously provide this information to the members of the Security Working Group (and their designees) and Commission observers of the Security Working Group.[148] As noted above, the proposed amendments would require the Security Working Group to include the chief or deputy chief information security officers for each Participant. These experts would likely be able to provide valuable feedback to the CISO and the CCO (or to the Operating Committee) on how to address such non-compliance or how to prevent similar events in the future, and simultaneous notification of the members of the Security Working Group (and their designees) would help them to provide such feedback in a timely manner.

Finally, the Commission wishes to emphasize that the above-stated requirements for non-SAW environments only dictate that Participants must meet certain security requirements. The Participants would still be wholly responsible for all other aspects of their non-SAW environment, including the internal architecture of their non-SAW environment(s), the analytical tools to be used in their non-SAW environment(s), and the use of any additional data. Accordingly, proposed Section 6.13(d)(iii)(D) indicates that an approved Participant may provision and use its choice of software, hardware, and additional data within the non-SAW environment, so long as such activities otherwise comply with the detailed design specifications provided by the Participant pursuant to proposed Section 6.13(d)(i)(A)(2) or proposed Section 6.13(d)(ii)(A). The Commission preliminarily believes that this provision will give the Participants sufficient flexibility in and control over the use of their non-SAW environments, while still maintaining the security of such environments and the CAT Data that may be contained therein.

The Commission requests comment on the proposed operational requirements for non-SAW environments. Specifically, the Commission solicits comment on the following:

53. The proposed amendments would require the Plan Processor to notify the Operating Committee that an approved Participant's non-SAW environment has achieved compliance with the detailed design specifications submitted pursuant to proposed Section 6.13(d)(i) or (ii) before that non-SAW may access CAT Data through the user-defined direct queries or bulk extraction tools. Is the Plan Processor the appropriate party to make this notification? If not, what other party should make the notification and why? Is it appropriate to notify the Operating Committee? Should any other parties be notified? If so, please identify those parties and explain why it would be appropriate for them to be notified. Should approved non-SAW environments be allowed to connect to the Central Repository without any evaluation process? Are the detailed design specifications submitted by the approved Participant as part of the application process an appropriate benchmark? If it is not an appropriate benchmark, please identify what benchmark would be appropriate and explain why.

54. The proposed amendments would require the Plan Processor to monitor an approved Participant's non-SAW environment in accordance with the detailed design specifications submitted with that Participant's application for an exception. Is the Plan Processor the right party to conduct this monitoring? If a different party should conduct this monitoring, please identify that party and explain why it would be a more appropriate choice. Is it appropriate to require that the proposed monitoring be conducted in accordance with the detailed design specifications submitted with the Participant's application for an exception? Should a different benchmark provide the controlling standard for such monitoring? If so, please identify that benchmark and explain why it would provide a more appropriate standard. Instead of specifying that such monitoring should be conducted in accordance with the detailed design specifications submitted by the Participant, should the proposed amendments specify the nature of the access and monitoring required? Should the proposed amendments specify that monitoring should be continuous? If so, please explain how that term should be defined and why such definition would

[144] The proposed amendments would require the Participant to comply with the detailed design specifications submitted pursuant to proposed Section 6.13(d)(i)(A)(2) or proposed Section 6.13(d)(ii)(A). *See* proposed Section 6.13(d)(iii)(B); *see also* note 97 *infra.*

[145] This provision would require each Participant to remedy any non-compliance promptly, whether such non-compliance was identified by the Plan Processor or by the Participant. *See* note 100 *supra,* for a discussion of what might constitute ''prompt'' remediation.

[146] The detailed design specifications submitted pursuant to proposed Section 6.13(d)(i) or (ii) must demonstrate the extent to which they adhere to the detailed design specifications developed by the Plan Processor for SAWs pursuant to proposed Section 6.13(b)(i), and they must enable substantially similar operational functions. Accordingly, the Commission does not preliminarily expect the monitoring required by proposed Section 6.13(d)(iii) to impose an undue burden on the Plan Processor, because the Plan Processor should be able to leverage and use the monitoring processes developed for SAWs. *See, e.g.,* note 534 *infra.*

[147] An example of such a change would be if a Participant implements a new system which establishes a new control or changes a detail design specification.

[148] *See* note 30 *supra* for a discussion of the confidentiality obligations to which the members of the Security Working Group and their designees would be subject.

be appropriate. If not, please explain how often such monitoring should be conducted and explain why. Should the proposed amendments indicate whether manual or automated processes (or both) should be used by the Plan Processor and whether automated support tools should be used? Should the proposed amendments indicate whether the Participant should provide the Plan Processor with market data feeds, log files, or some other data? Please identify any data that should be provided to the Plan Processor to enable the required monitoring.

55. The proposed amendments would restrict the Plan Processor to monitor SAWs for compliance with the detailed design specifications submitted pursuant to proposed Section 6.13(d)(i)(A)(2) or proposed Section 6.13(d)(ii)(A). Is this an appropriate limitation? Should the Plan Processor be able to monitor any of the activities that might be conducted within a Participant's non-SAW environment? If so, please specify what activities the Plan Processor should be permitted to monitor and explain why such monitoring would be appropriate.

56. The proposed amendments would require the Plan Processor to notify the Participant of any identified non-compliance with the design specifications provided pursuant to proposed Section 6.13(d)(i) or (ii). Should a different party notify the Participant of any identified non-compliance? If so, please identify that party and explain why it would be appropriate for that party to provide the notification. Are there any additional parties that the Plan Processor should notify of any identified non-compliance—for example, the Operating Committee? If so, please identify the party or parties that should also be notified, explain why such notification would be appropriate, and explain whether notification of those parties would raise any confidentiality, security, or competitive concerns.

57. The proposed amendments would specify that approved Participants must comply with the detailed design specifications provided pursuant to proposed Section 6.13(d)(i) or (ii). Should the proposed amendments specify that the Participants should comply with another set of requirements? If so, please identify those requirements and explain why it would be more appropriate for a non-SAW environment to comply with those requirements.

58. The proposed amendments would require the Participants to promptly remediate any identified non-compliance. Should the proposed amendments specify what would qualify as ''prompt'' remediation? If so, please explain what amount of time should be specified and explain why that amount of time is sufficient. Would it be appropriate for the proposed amendments to refer specifically to the risk management policy developed by the Plan Processor for appropriate remediation timeframes? Is there another policy that provides remediation timeframes that would be more appropriate for these purposes? If so, please identify that policy and explain why it would be a better benchmark.

59. The proposed amendments would specify that approved Participants must simultaneously notify the Plan Processor, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group of any material changes to its security controls. Is it appropriate to require the Participant to simultaneously notify the members of the Security Working Group (and their designees) and Commission observers of the Security Working Group? Should the Plan Processor be provided with a notification before the members of the Security Working Group (and their designees) and Commission observers of the Security Working Group? If so, how long should the Participant be required to wait before notifying the members of the Security Working Group (and their designees) and Commission observers of the Security Working Group? What kinds of changes should be considered ''material''? Please provide specific and detailed examples. Should the proposed amendments specify that the Participants must comply with any other security protocols? If so, please identify these security protocols and explain why it would be appropriate to require the Participants to comply with them. Should the Participants be allowed to make material changes to their non-SAW environments without first getting the express approval of the CISO and the CCO? Does the proposed notification of the members of the Security Working Group and their designees raise any confidentiality, security, or competitive concerns? If so, please identify such concerns and explain whether the benefits of notifying the members of the Security Working Group (and their designees) nevertheless justify such notification. Are there any other parties that should be notified if a material change is made to the security controls of a non-SAW environment—for instance, the CISO and the CCO? If so, please identify these parties and explain why it would be appropriate to notify them.

60. The proposed amendments clarify that the Participants may provision and use approved non-SAW environments with their choice of software, hardware, and additional data, so long as such activities are sufficiently consistent with the detailed design specifications submitted by the Participant pursuant to proposed Section 6.13(d)(i)(A)(1) or proposed Section 6.13(d)(ii)(A). Are there specific software, hardware, or additional data that the Commission should explicitly disallow in the proposed amendments? If so, please identify such software, hardware, or data specifically and explain why it would be appropriate to disallow it.

D. Online Targeted Query Tool and Logging of Access and Extraction

The CAT NMS Plan does not limit the amount of CAT Data a regulator can extract or download through the online targeted query tool; the CAT NMS Plan states that the Plan Processor must define the maximum number of records that can be viewed in the online tool as well as the maximum number of records that can be downloaded.[149] The Commission believes that certain limitations and changes are required to prevent the online targeted query tool from being used to circumvent the purposes of the proposed CISP and SAW usage requirements.[150] Specifically, the Commission proposes to amend Appendix D, Section 8.1.1 of the CAT NMS Plan to remove the ability of the Plan Processor to define the maximum number of records that can be downloaded via the online query tool, and instead limit the maximum number of records that can be downloaded via the online targeted query tool to 200,000 records per query request.[151] In addition, the Commission proposes to

[149] The CAT NMS Plan does specify that the minimum number of records that the online targeted query tool is able to process is 5,000 (if viewed within the online query tool) or 10,000 (if viewed via a downloadable file). *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 8.1.1. Section 8.1.1 of Appendix D of the CAT NMS Plan also requires that result sets that exceed the maximum viewable or download limits must return to testers a message informing them of the size of the result set and the option to choose to have the result set returned via an alternate method (*e.g.,* multiple files).

[150] Under the proposed amendments described in Part II.A above, regulators would be permitted to use the online targeted query tool outside of a Participant SAW.

[151] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 8.1.1. If the Plan Processor provides more than one online targeted query tool, the proposed requirements of Appendix D, Section 8.1.1, and existing requirements of the CAT NMS Plan, would apply to each online targeted query tool.

amend Appendix D, Section 8.1.1 of the CAT NMS Plan to permit the downloading of a result set through the online targeted query tool, in either a single or multiple file(s), only if the download per query result does not exceed 200,000 records. Proposed Appendix D, Section 8.1.1 would also provide that users that select a multiple file option will be required to define the maximum file size of the downloadable files subject to the download restriction of 200,000 records per query result. As proposed, the Plan Processor may still define a maximum number of records that can be downloaded to a number lower than 200,000.

As proposed, regulatory users that need to download specific result sets for regulatory and surveillance purposes from the targeted online query tool must refine their searches to fewer than 200,000 records in order to be able to download entire record sets. If a regulatory user receives a result set larger than 200,000 records in the online targeted query tool, the Commission believes that it is appropriate for the regulatory user to further refine the query used so that the result set is smaller than 200,000 records before the regulatory user would be permitted to download the entire record set. Alternatively, if a regulatory user must download more than 200,000 records for surveillance or regulatory purposes, the Commission believes that it is appropriate that the regulatory user be required to access CAT Data through the SAWs.

The Commission preliminarily believes that limiting the number of records that can be downloaded to 200,000 is reasonable and appropriate because it is a sufficiently large number to allow for result sets to be generated for the type of targeted searches for which the online targeted query tool is designed.[152] Based on the Commission's experience a 200,000 download limit would not prevent regulators from performing many investigations, such as investigations into manipulation schemes in over-the-counter stocks or investigations based on shorter-term trading activity. However, the Commission believes that programmatic analysis of very large downloaded datasets is more appropriately provided for in a SAW or approved non-SAW environment, which would be subject to the requirements of proposed Section 6.13.[153] The Commission also preliminarily believes that a 200,000 download limit would help prevent large scale downloading of CAT Data outside of SAW or approved non-SAW environments using the online targeted query tool.

The Commission preliminarily believes that the proposed limitations on downloading records would not prevent regulatory users from using the online query tool to perform regulatory analysis of result sets greater than 200,000 records,[154] even if such result sets could not be downloaded. The Commission understands that the Plan Processor's online targeted query tool is designed to provide for the analysis of massive data sets like the CAT database. This functionality would allow users to perform their surveillance and regulatory functions within the online targeted query tool, as appropriate, and allow regulatory users to narrow queries to obtain more manageable data sets that are not greater than 200,000 records for download or further analysis.

The CAT NMS Plan currently requires the targeted online query tool to log submitted queries, query parameters, the user ID of the submitter, the date and time of the submission, and the delivery of results.[155] The CAT NMS Plan further requires that the Plan Processor provide monthly reports based on this information to each Participant and the SEC of its respective metrics on query performance and data usage, and that the Operating Committee receive the monthly reports to review items, including user usage and system processing performance.[156] The CAT NMS Plan, however, does not require that the online query tool log information relating to the extraction of CAT Data.[157] The Commission now proposes to make changes to these logging requirements.

First, the Commission proposes to amend Appendix D, Section 8.1.1 of the CAT NMS Plan to define the term ''delivery of results,'' to mean ''the number of records in the result(s) and the time it took for the query to be performed.'' As noted above, the CAT NMS Plan requires the logging of ''the delivery of results,'' but does not define what that term means. The Commission preliminarily believes the proposed definition would result in logs that provide more useful information to the Plan Processor and Participants and will assist in the identification of potential issues relating to the security or access to CAT Data. For example, this information would provide the Plan Processor data that could be used to help assess the performance of access tools, and whether the system is meeting performance criteria related to the speed of queries.[158]

The Commission also proposes to amend Appendix D, Section 8.1.1 of the CAT NMS Plan to require that the online targeted query tool also log information relating to the access and extraction of CAT Data, when applicable. The CAT NMS Plan already requires the logging of access, but the Commission is proposing the change to require both access and extraction of CAT Data be logged. This change would also require the same logging of access and extraction of CAT Data from the user-defined direct queries and bulk extraction tools, which the Commission believes would be possible because of the required usage of SAWs proposed above. The Commission preliminarily believes that the requirement to log access and extraction of CAT Data for all three types of access is appropriate because the monthly reports of information relating to the query tools will be provided to the Operating Committee so that the Participants can review information concerning access and extraction of CAT Data regularly and to identify issues related to the security of CAT Data in accordance with Participants' data confidentiality policies, which are also being amended as described in Part II.G below.

Lastly, the Commission proposes to amend Appendix D, Section 8.2.2 of the CAT NMS Plan to modify the sentence ''[t]he Plan Processor will use this logged information to provide monthly reports to the Operating Committee, Participants and the SEC of their respective usage of the online query tool,'' by replacing ''online query tool'' with ''user-defined direct query and bulk extraction tool,'' because the relevant section of the CAT NMS Plan is about bulk extraction performance and the subject of the preceding sentence concerns logging of the user-defined direct query and bulk extraction tool. The Commission preliminarily

[152] The Participants have stated that when fully complete, CAT will ingest ''in excess of 58 billion records per day.'' *See* CAT NMS, LLC, ''CAT NMS Selects FINRA as Consolidated Audit Trail Plan Processor,'' *available at: https://www.catnmsplan.com/wp-content/uploads/2019/02/CAT_FINRA_Press_Release_FINAL.pdf.*

[153] *See* Part II.C.

[154] The proposed amendments would not limit the query results that can be viewed within the online targeted query tool. The limitation would only apply to downloads from the tool.

[155] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 8.1.1.

[156] *Id.*

[157] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 8.2.

[158] The Commission also preliminarily believes that this information could be used to help monitor whether or not Regulatory Staff are accessing CAT Data appropriately and whether or not Participants' extraction of CAT Data is limited to the minimum amount of data necessary to achieve specific surveillance or regulatory purposes. *See infra* Parts II.G.2 and II.G.3.a.

believes that the intent of the sentence was to refer to user-defined direct query and bulk extraction tool and that it is appropriate to amend this to provide clarity and consistency to the sentence and section of the CAT NMS Plan.

The Commission requests comment on the proposed amendments to the provisions regarding the targeted online query tool and logging of access and extraction of CAT Data. Specifically, the Commission solicits comment on the following:

61. Should the maximum the number of records that can be downloaded from the online targeted query tool to 200,000 records? If not, what should the maximum number of records be set at?

62. Should the CAT NMS Plan define what ''delivery of results'' means in the context of logging? Is the proposed definition of ''delivery of results'' reasonable and appropriate?

63. Should the CAT NMS Plan require the CAT System to log extraction of CAT Data from the targeted online query tool, as the CAT System must do for the user-defined query tool and bulk extraction tool? Should other information be logged by the CAT System?

E. CAT Customer and Account Attributes

Citing to data security concerns raised with regard to the reporting and collection of information that could identify a Customer in the CAT, and in particular the reporting of SSN(s)/ITIN(s), dates of birth and account numbers, the Participants submitted a request for an exemption from certain reporting provisions of the CAT NMS Plan pursuant to Section 36 of the Securities Exchange Act of 1934 (''Exchange Act'') [159] and Rule 608(e) of Regulation NMS under the Exchange Act [160] (the ''PII Exemption Request'').[161] Specifically, the Participants requested an exemption from (1) the requirement that Industry Members [162] report SSN(s)/ITIN(s) to the CAT in order to create the Customer-ID, so as to allow for an alternative approach to generating a Customer ID without requiring SSN(s)/ITIN(s) to be reported to the CAT; and (2) the requirement that Industry Members report dates of birth and account numbers associated with natural person Customers to the CAT, and instead requiring Industry Members to report the year of birth associated with natural person Customers, and the Industry Member Firm Designated ID for each trading account associated with all Customers.[163]

On March 17, 2020, the Commission granted the Participants' request for an exemption from reporting the SSN(s)/ITIN(s), date of birth and account number associated with natural person Customers to the CAT, conditioned on the Participants meeting certain conditions (the ''PII Exemption Order'').[164] The proposed amendments would modify the Customer-ID creation process and reporting requirements in a manner consistent with the PII Exemption Request, including all changes requested by the Participants to the data elements required to be reported to and collected by the CAT.[165]

The Commission proposes to amend the CAT NMS Plan to: (1) Adopt revised Industry Member reporting requirements to reflect that ITINs/SSNs, dates of birth and account numbers will not be reported to the CAT; (2) establish a process for creating Customer-ID(s) in light of the revised reporting requirements; (3) impose specific obligations on the Plan Processor that would support the revised reporting requirements and creation of Customer-ID(s); and (4) amend existing provisions of the CAT NMS Plan to reflect the new reporting requirements and process for creating Customer-ID(s), as further discussed below.

1. Adopt Revised Industry Member Reporting Requirements

The CAT NMS Plan requires Industry Members to collect and report ''Customer Account Information'' [166] and ''Customer Identifying Information'' [167] to the CAT in order to identify Customers.[168] As noted above, the PII Exemption Order permits the Participants to no longer require Industry Members to report SSN(s)/ITIN(s), dates of birth and account numbers for natural person Customers, which are data elements in the definition of Customer Account Information and Customer Identifying Information, provided that Industry Members report the year of birth for natural person Customers to the CAT.[169] Consistent with the PII Exemption Order, the Commission proposes to amend the CAT NMS Plan to delete the requirement that SSN(s)/ITIN(s) be reported to and collected by the CAT, and to replace the requirement that Industry Members report the dates of birth for their natural person Customers with the requirement that Industry Members report the year of birth for their natural person Customers.[170] In addition, the Commission proposes to delete the requirement that account numbers be reported to and collected by the CAT as a data element in Account Attributes.[171] The proposed amendments also would require that the Customer-ID of a legal entity Customer

[159] 15 U.S.C. 78mm(a)(1).

[160] 17 CFR 242.608(e).

[161] *See* letter from Michael Simon, Chair, CAT NMS Plan Operating Committee, to Vanessa Countryman, Secretary, U.S. Securities and Exchange Commission, dated January 29, 2020 (the ''PII Exemption Request'').

[162] ''Industry Member'' is a defined term under the CAT NMS Plan and means ''a member of a national securities exchange or a member of a national securities association.'' *See* CAT NMS Plan *supra* note 3 at Article I, Section 1.1.

[163] The ''Industry Member Firm Designated ID'' refers to the Firm Designated ID associated with that specific Industry Member.

[164] *See* Securities Exchange Act Release No. 88393 (March 17, 2020), 85 FR 16152, (March 20, 2020) (''PII Exemption Order'').

[165] *See* PII Exemption Request, *supra* note 161.

[166] The CAT NMS Plan defines ''Customer Account Information'' to ''include, but not be limited to, account number, account type, customer type, date account opened, and large trader identifier (if applicable); except, however, that (a) in those circumstances in which an Industry Member has established a trading relationship with an institution but has not established an account with that institution, the Industry Member will (i) provide the Account Effective Date in lieu of the ''date account opened''; (ii) provide the relationship identifier in lieu of the ''account number''; and (iii) identify the ''account type'' as a ''relationship''; (b) in those circumstances in which the relevant account was established prior to the implementation date of the CAT NMS Plan applicable to the relevant CAT Reporter (as set forth in Rule 613(a)(3)(v) and (vi)), and no ''date account opened'' is available for the account, the Industry Member will provide the Account Effective Date in the following circumstances: (i) Where an Industry Member changes back office providers or clearing firms and the date account opened is changed to the date the account was opened on the new back office/clearing firm system; (ii) where an Industry Member acquires another Industry Member and the date account opened is changed to the date the account was opened on the post-merger back office/clearing firm system; (iii) where there are multiple dates associated with an account in an Industry Member's system, and the parameters of each date are determined by the individual Industry Member; and (iv) where the relevant account is an Industry Member proprietary account.''

[167] The CAT NMS Plan defines ''Customer Identifying Information'' to mean ''information of sufficient detail to identify a Customer, including, but not limited to, (a) with respect to individuals: name, address, date of birth, individual tax payer identification number (''ITIN'')/social security number (''SSN''), individual's role in the account (*e.g.,* primary holder, joint holder, guardian, trustee, person with the power of attorney); and (b) with respect to legal entities: name, address, Employer Identification Number (''EIN'')/Legal Entity Identifier (''LEI'') or other comparable common entity identifier, if applicable; provided, however, that an Industry Member that has an LEI for a Customer must submit the Customer's LEI in addition to other information of sufficient detail to identify a Customer.''

[168] The CAT NMS Plan defines ''Customer'' as having the same meaning provided in SEC Rule 613(j)(3). *See* CAT NMS Plan *supra* note 3 at Article I, Section 1.1 ''Customer.''

[169] *See* PII Exemption Order, *supra* note 164.

[170] *See id.*

[171] *See infra* this Part II.E.1 for a description and discussion of Account Attributes and the data elements contained in Account Attributes. *See also* PII Exemption Order, *supra* note 164 at 16154.

be based on the transformation of that legal entity's EIN by the CCID Transformation Logic,[172] just as the SSN of a natural person Customer would be transformed.[173]

The Commission proposes the following additional amendments to reflect the revised reporting requirements for Industry Members: The defined term ''Customer Attributes,'' would replace the defined term ''Customer Identifying Information'' and ''Account Attributes'' would replace the defined term ''Customer Account Information'' to more accurately reflect the data elements being reported by Industry Members; and a newly defined term ''Customer and Account Attributes'' would be defined to include all the data elements, or attributes, in both ''Customer Attributes'' and ''Account Attributes.'' [174] Finally, as a result of the changes to the Customer and Account Attributes that are reported to and collected by the CAT, which will no longer require the reporting of the most sensitive PII, the Commission proposes to delete the defined term ''PII'' from the CAT NMS Plan.

''Customer Attributes'' would include all of the same data elements as ''Customer Identifying Information'' except the proposed definition would not include the requirement to report ITIN/SSN and date of birth, and the proposed definition would add the requirement that the year of birth for a natural person Customer be reported to CAT.[175] As such, ''Customer Attributes'' would be defined to mean ''information of sufficient detail to identify a Customer, including, but not limited to, (a) with respect to individuals: name, address, year of birth, individual's role in the account (*e.g.,* primary holder, joint holder, guardian, trustee, person with the power of attorney); and (b) with respect to legal entities: Name, address, Employer Identification Number (''EIN'') and Legal Entity Identifier (''LEI'') or other comparable common entity identifier, if applicable; [176] provided, however, that an Industry Member that has an LEI for a Customer must submit the Customer's LEI in addition to other information of sufficient detail to identify a Customer'' [177]

In addition, ''Account Attributes'' would be defined to include all of the same data elements as ''Customer Account Information,'' except a Customer's account number and the relationship identifier in lieu of an account number would not be reported by an Industry Member as an Account Attribute.[178] As proposed, therefore, ''Account Attributes'' would be defined in part to ''include, but not limited to, account type, customer type, date account opened, and large trader identifier (if applicable).'' [179]

The Commission preliminarily believes that eliminating reporting of SSNs to the CAT is appropriate because SSNs are considered among the most sensitive PII that can be exposed in a data breach, and the elimination of the SSNs from the CAT may reduce both the risk of attracting bad actors and the impact on retail investors in the event of a data breach.[180] The Commission preliminarily believes that the same concern applies to the reporting of account numbers and thus it is appropriate to no longer require account numbers to be reported to the CAT as part of Account Attributes to the CAT.[181] The removal of account numbers and dates of birth is expected to further reduce both the attractiveness of the database as a target for hackers and the impact on retail investors in the event of a data breach.[182] The Commission also preliminarily believes that replacing the requirement that Industry Members report the date of birth with the year of birth of natural person Customers is appropriate because it will continue to allow Regulatory Staff to carry out regulatory analysis that focuses on certain potentially vulnerable populations, such as the elderly.

In addition, replacing the term ''Customer Identifying Information'' with the term ''Customer Attributes'' and replacing the term ''Customer Account Information'' with the term ''Account Attributes'' is also appropriate because the data elements in both categories are more accurately described as information that can be attributed to a Customer or a Customer's account in light of the PII that has been removed from these categories. Furthermore, adopting a new defined term, ''Customer and Account Attributes,'' that refers collectively to all the attributes in Customer Attributes and Account Attributes is a useful and efficient way to refer to all the attributes associated with a Customer that is either a natural person or a legal entity that are required to be reported by Industry Members and collected by the CAT.

---

[172] ''CCID Transformation Logic'' refers to ''the mathematical logic identified by the Plan Processor that accurately transforms an individual tax payer identification number(s)(ITIN(s))/social security number(s)(SSN(s))/Employer Identification Number (EIN(s)) into a Transformed Value(s) for submission into the CCID Subsystem, as set forth in Appendix D, Section 9.1.'' *See* proposed Section 1.1 ''CCID Transformation Logic''.

[173] *See infra* Part II.E.2 for a description of the use of the CCID Transformation Logic by Industry Members. The Commission is not changing the CAT NMS Plan's requirement that a legal entity's EIN be reported as part of Customer and Account Attributes to CAIS. *See supra* Part II.F.2 for a discussion of how Regulatory Staff and SEC staff can access and use a legal entity's EIN to obtain that entity's Customer-ID through the CCID Subsystem, or access the legal entity's EIN in CAIS to obtain related Customer and Account Attributes, Customer-ID or other identifier (*e.g.,* Industry Member Firm Designated ID) associated with that legal entity.

[174] *See id.*

[175] Specifically, name, address, individual's role in the account (*e.g.,* primary holder, joint holder, guardian, trustee, person with the power of attorney); and legal entity name, address, EIN and LEI or other comparable common entity identifier, if applicable (provided, however, that an Industry Member that has an LEI for a Customer must submit the Customer's LEI in addition to other information of sufficient detail to identify a Customer) are data elements that will not be changed pursuant to the amendments proposed by the Commission.

[176] The proposed amendment also would clarify that a legal entity's EIN is different than the legal entity's Legal Entity Identifier (''LEI''). In relevant part, the CAT NMS Plan currently provides that the Industry Member will report ''Employer Identification Number (''EIN'')/Legal Entity Identifier (''LEI'') or other comparable common entity identifier, if applicable.'' The Commission is amending the CAT NMS Plan to require that an Industry Member report the ''Employer Identification Number (''EIN'') and Legal Entity Identifier (''LEI'') or other comparable common entity identifier, if applicable; provided, however, that an Industry Member that has an LEI for a Customer must submit the Customer's LEI in addition to other information of sufficient detail to identify a Customer.'' *See* Proposed Appendix D, Section 9.2.

[177] *See id.* As is currently required, Customer Attributes would be defined to ''include, but not be limited to'' the data elements listed in the definition of Customer Attributes. If the Participants intend to require additional data elements to be reported to the CAT, such changes must be filed with the Commission and would be subject to public notice and comment, and need to be approved by the Commission before becoming effective. *See* 17 CFR 240.19b–4; *see also* 17 CFR 242.608(a).

[178] A relationship identifier is used when an Industry Member does not have an account number available to its order handling and/or execution system at the time of order receipt, but can provide an identifier representing the client's trading. When a relationship identifier is used instead of a parent account number, and an Industry Member places an order on behalf of the client, any executed trades will be kept in a firm account until they are allocated to the proper subaccount(s). Relationship identifiers would be reported as Firm Designated IDs pursuant to the Firm Designated ID amendment in this situation.

[179] The proposed definition of Account Attributes would retain the alternative data elements that an Industry Member can report in the circumstances in which the Industry Member has established a trading relationship with an institution but has not established an account with that institution. *See* CAT NMS Plan *supra* note 3 at Article I, Section 1.1 ''Customer Account Information.''

[180] *See* PII Exemption Order, *supra* note 164, at 16156; *see also* Identify Theft Resource Center 2018 End of Year Breach Report, pg. 13, *https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-YearAftermath_FINAL_V2_combinedWEB.pdf.*

[181] *See* proposed definition of ''Account Attributes'' in proposed Section 1.1.

[182] *See* PII Exemption Order, *supra* note 164, at 16156.

The Commission also preliminarily believes that it is appropriate to delete the term ''PII'' from the CAT NMS Plan and replace that term with ''Customer and Account Attributes'' as that would more accurately describe the attributes that must be reported to the CAT, now that ITINs/SSNs, dates of birth and account numbers would no longer be required to be reported to the CAT pursuant to the amendments being proposed by the Commission. Thus, the Commission proposes to eliminate the term ''PII'' in Article VI, Sections 6.2(b)(v)(F) and 6.10(c)(ii); and Appendix D, Sections 4.1; 4.1.2; 4.1.4; 6.2; 8.1.1; 8.1.3; 8.2; and 8.2.2.

The Commission requests comment on the proposed amendments that would adopt revised Industry Member reporting requirements to reflect that ITINs/SSNs, dates of birth and account numbers will not be reported to the CAT. Specifically, the Commission solicits comment on the following:

64. The proposed amendments define ''Customer and Account Attributes'' as meaning the data elements in Account Attributes and Customer Attributes. Do commenters believe these definitions should be modified to add or delete data elements? If so, what elements?

2. Establish a Process for Creating Customer-ID(s) in Light of Revised Reporting Requirements

The creation of a Customer-ID by the Plan Processor that accurately identifies a Customer continues to be a requirement under the CAT NMS Plan. The Commission preliminarily believes that it is appropriate to amend the CAT NMS Plan to set forth the process for how the Plan Processor would create Customer-IDs in the absence of the requirement that SSNs/ITINs, dates of birth and account numbers be reported to and collected by the CAT, consistent with the PII Exemption Order.[183] As further discussed below, however, the amendments proposed by the Commission deviate from the PII Exemption Order by requiring that a Customer's EIN would also be transformed by the CCID Transformation Logic, along with SSNs/ITINs, so that the same process for creating Customer-IDs for natural persons also would apply to the creation of Customer-IDs for legal entities.[184]

Accordingly, the Commission proposes the following amendments to the CAT NMS Plan: Section 9 of Appendix D, would be renamed ''CAIS, the CCID Subsystem and the Process for Creating Customer-IDs'';[185] a new Section 9.1 would be added to Appendix D, entitled ''The CCID Subsystem,'' which would describe the operation of the CCID Subsystem and the process for creating Customer-IDs; Section 9.2, would be revised to describe the Customer and Account Attributes reported to and collected in the CAIS[186] and Transformed Values;[187] Section 9.3 would be amended to reflect the revised reporting requirements that require the reporting of a Transformed Value and Customer and Account Attributes by Industry Members; and Section 9.4 would be amended to specify the error resolution process for the CCID Subsystem and CAIS, and the application of the existing validation process required by Section 7.2 of Appendix D applied to the Transformed Value, Customer-IDs, the CCID Subsystem. The proposed amendments to each of these provisions is described below.

The Commission proposes to describe the CCID Subsystem and the process for creating Customer-IDs for both natural person and legal entity Customers through the CCID Subsystem in Section 9.1 of Appendix D. The proposed amendments provide that Customer-IDs would be generated through a two-phase transformation process. In the first phase, a Customer's ITIN/SSN/EIN would be transformed into a Transformed Value using the CCID Transformation Logic provided by the Plan Processor. The Transformed Value, and not the ITIN/SSN/EIN of the Customer, would then be submitted to the CCID Subsystem, a separate subsystem within the CAT System,[188] along with any other information and additional events (*e.g.,* record number) as may be prescribed by the Plan Processor that would enable the final linkage between the Customer-ID and the Customer Account Attributes. The CCID Subsystem would perform a second transformation to create a globally unique Customer-ID for each Customer. From the CCID Subsystem, the Customer-ID for the natural person and legal entity Customer would be sent to the CAIS[189] separately from any other CAT Data required to be reported by Industry Members to identify a Customer, which would include the Customer and Account Attributes.[190] In CAIS, the Customer-ID would be linked to the Customer and Account Attributes associated with that Customer-ID, and linked data would be made available to Regulatory Staff for queries in accordance with Appendix D, Section 4.1.6 (Customer Identifying Systems Workflow) and Appendix D, Section 6 (Data Availability). The proposed amendments would make clear that the Customer-ID may not be shared with an Industry Member.

The proposed amendments also would require the Plan Processor to provide the CCID Transformation Logic to Industry Members and Participants pursuant to the provisions of Appendix D, Section 4.1.6 (Customer Identifying Systems Workflow).[191] For Industry Members, the proposed amendments would provide that the CCID Transformation Logic would be embedded in the CAT Reporter Portal or used by the Industry Member in machine-to-machine processing.[192]

For Regulatory Staff, the Commission proposes to amend Appendix D, Section 9.1 to first reflect the fact that, unlike Industry Members who receive ITIN(s)/SSN(s)/EIN(s) from their Customers as part of the process of identifying their Customers for purposes of reporting to the CAT, Regulatory Staff may receive ITIN(s)/SSN(s)/EIN(s) of Customers from outside sources (*e.g.,* via regulatory data, a tip, complaint, or referral).[193] Therefore, the proposed amendments would provide that for Regulatory Staff, the Plan Processor would embed the CCID Transformation Logic in the CAIS/CCID Subsystem Regulator Portal for manual CCID Subsystem Access.[194] For

[183] *See* proposed Appendix D, Section 9.

[184] *See* proposed Appendix D, Section 9.1. In addition, a legal entity Customer would continue to be required to report its EIN to the CAT pursuant to the CAT NMS Plan because such EIN is an attribute included in Customer and Account Attributes. *See* proposed Appendix D, Section 9.2. Thus, a legal entity's EIN would be transformed by the CCID Transformation Logic into a Transformed Value and submitted to the CCID Subsystem, as well as reported to the CAT as an element of Customer and Account Attributes.

[185] Currently, Section 9 of Appendix D is entitled ''CAT Customer and Customer Account Information.''

[186] ''CAIS'' refers to the Customer and Account Information System within the CAT System that collects and links Customer-ID(s) to Customer and Account Attributes and other identifiers for queries by Regulatory Staff. *See* proposed Section 1.1 ''CAIS''.

[187] ''Transformed Value,'' would be defined to mean ''the value generated by the CCID Transformation Logic as set forth in proposed Section 6.1(v) and Appendix D, Section 9.1 of the CAT NMS Plan. *See infra* note 190 for a discussion of this proposed definition.

[188] *See* proposed Section 1.1 ''CCID Subsystem.'' *See also* proposed Appendix D, Section 9.1 (The CCID Subsystem).

[189] *See infra* note 203 for a discussion of this proposed definition.

[190] A legal entity's EIN, which is an attribute included in Customer and Account Attributes, also would be sent directly to CAIS, as further discussed below.

[191] *See* proposed Appendix D, Section 9.1 (The CCID Subsystem).

[192] *See id.*

[193] *See id.*

[194] For a full discussion of Manual CCID Access, *see infra* Part II.F.4. As further discussed in Part

Continued

Programmatic CCID Subsystem Access by Regulatory Staff, Participants approved for Programmatic CCID Subsystem Access would use the CCID Transformation Logic in conjunction with an API provided by the Plan Processor.[195]

Given the need to safeguard the security of the CCID Subsystem, the Commission also proposes to amend the CAT NMS Plan to provide that the CCID Subsystem must be implemented using network segmentation principles to ensure traffic can be controlled between the CCID Subsystem and other components of the CAT System, with strong separation of duties between it and all other components of the CAT System.[196] The proposed amendments would furthermore state that the design of the CCID Subsystem will maximize automation of all operations of the CCID Subsystem to prevent, if possible, or otherwise minimize human intervention with the CCID Subsystem and any data in the CCID Subsystem.

Finally, as proposed, the CAT NMS Plan's existing requirement that the Participants ensure the timeliness, accuracy, completeness, and integrity of CAT Data would apply to the Transformed Value(s) and the overall performance of the CCID Subsystem to support the creation of a Customer-ID that uniquely identifies each Customer.[197] The proposed amendments would also require that the annual Regular Written Assessment required by Article VI, Section 6.6(b)(i)(A) assess the overall performance and design of the CCID Subsystem and the process for creating Customer-ID(s).[198] The proposed amendments would clarify that because the CCID Subsystem is part of the CAT System, all provisions of the CAT NMS Plan that apply to the CAT System would also apply to the CCID Subsystem.[199]

In order to implement these proposed amendments, the Commission proposes to adopt several new definitions, as follows: ''CCID Subsystem'' would be defined to mean the ''subsystem within the CAT System which will create the Customer-ID from a Transformed Value(s),'' as set forth in proposed Section 6.1(v) and Appendix D, Section 9.1 of the CAT NMS Plan.[200] ''Transformed Value,'' would be defined to mean ''the value generated by the CCID Transformation Logic as set forth in proposed Section 6.1(v) and Appendix D, Section 9.1 of the CAT NMS Plan.'' [201] ''CCID Transformation Logic'' would be defined to mean the mathematical logic identified by the Plan Processor that accurately transforms an ITIN/SSN/EIN into a Transformed Value(s) for submission to the CCID Subsystem as set forth in Appendix D, Section 9.1.[202] ''CAIS,'' would be defined to mean the ''Customer and Account Information System within the CAT System that collects and links Customer-ID(s) to Customer and Account Attributes and other identifiers for queries by Regulatory Staff.'' [203] ''Customer Identifying Systems'' would be defined to mean both the CAIS and the CCID Subsystem.[204] Finally, the ''CAIS/CCID Subsystem Regulator Portal'' would be defined to mean the online tool enabling Manual CAIS access and Manual CCID Subsystem access.[205]

The Commission preliminarily believes that it is appropriate to amend the CAT NMS Plan to establish the process for creating Customer IDs using Transformed Values. This approach would preserve and facilitate the creation of a unique Customer-ID for all Customers and would track orders from, or allocations to, any Customer or group of Customers over time, regardless of what brokerage account was used without requiring the submission of the ITIN/SSN to the CAT.

As noted above, the proposed amendments would require that the EIN for a Customer that is a legal entity be submitted to the CCID Transformation Logic to create the legal entity's Customer-ID; as such, the creation of a legal entity's Customer-ID would undergo the same transformation by the CCID Transformation Logic as a natural person Customer's ITIN/SSN. The Commission believes that this requirement is appropriate in order to leverage the operational efficiency that can be gained by requiring the same process for creating Customer-IDs for both natural person Customers and Customers that are legal entity Customers. The Commission also believes that requiring a legal entity's EIN to undergo the same transformation by the CCID Transformation Logic should also facilitate the ability of the Plan Processor to check the accuracy of the Customer-ID creation process since the Plan Processor can confirm that the same Customer-ID is created for the same EIN.

The Commission also preliminarily believes that these proposed amendments appropriately specify and describe the two systems within the CAT System that would ingest the various pieces of information that identify a Customer: (1) The CCID Subsystem, which would ingest the Transformed Value(s), along with any other information and additional events as may be prescribed by the Plan Processor that would enable the final linkage between the Customer-ID and the Customer Account Attributes, and (2) CAIS, which would collect the Customer and Account Attributes and other identifiers (*e.g.,* Industry Member Firm Designated IDs and record numbers) and link this data with the Customer-ID(s) created by the CCID Subsystem. The creation of the CCID Subsystem would facilitate the ability to create Customer-IDs in a process that is separate from the process that would require Industry Members to report Customer and Account Attributes to CAIS, but would ultimately link the Customer-IDs of Customers with the associated Customer and Account Attributes, so that Customers could be identified by Regulatory Staff when appropriate.

The Commission preliminarily believes that it is appropriate for the CAT NMS Plan to address the manner in which the CCID Transformation Logic is provided by the Plan Processor because the manner differs as between Industry Members on the one hand and Regulatory Staff on the other hand.

II.F.4, Manual CCID Subsystem Access would be used when Regulatory Staff require the conversion of fifty or fewer ITIN(s)/SSN(s)/EIN(s). *See* proposed Section 4.1.6.

[195] For a full discussion of Programmatic CCID Access, *see infra* Part II.F.7. As further discussed in Part II.F.7, Programmatic CCID Subsystem 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). *See* proposed Appendix D, Section 4.1.6.

[196] *See* proposed Appendix D, Section 9.1 (The CCID Subsystem).

[197] *See id. See also* CAT NMS Plan 4.12(b)(ii).

[198] *See id.*

[199] *See id.*

[200] *See* proposed Section 1.1.

[201] *See* proposed Section 1.1 ''Transformed Value.''

[202] *See* proposed Section 1.1 ''CCID Transformation Logic.''

[203] *See* proposed Section 1.1 ''CAIS.''

[204] *See* proposed Section 1.1 ''Customer Identifying Systems.''

[205] *See infra* Part II.F.3 for s discussion on Manual CAIS access and Manual CCID Subsystem access.

With respect to Industry Members, the manner in which the CCID Transformation Logic would be implemented depends on the submission method chosen by the Industry Member—*e.g.,* CAT Reporter Portal [206] or machine-to-machine submission [207] (*e.g.,* SFTP upload).[208] Because the CAT Reporter Portal is provided by the Plan Processor, the CCID Transformation Logic would have to be embedded in the CAT Reporter Portal for use by the Industry Member. However, if the Industry Member were to connect to the CAT through a machine-to-machine interface, the Industry Member would have to embed the CCID Transformation Logic into its own reporting processes. In both cases, transformation of the Customer ITIN/SSN would be done by the Industry Member in its own environment.

With respect to the provision of the Transformation Logic to Regulatory Staff, the Commission preliminarily believes it is appropriate to first note in the proposed amendments that Regulatory Staff may receive ITIN(s)/SSN(s)/EIN(s) from outside sources such as through regulatory data, tips, complaints, or referrals. Regulatory Staff also would be using the CCID Transformation Logic to convert ITIN(s)/SSN(s)/EIN(s) for regulatory and oversight purposes, unlike Industry Members.[209] Similar to Industry Members, however, Regulatory Staff would need to convert such ITIN(s)/SSN(s)/EIN(s) into Customer-IDs, using the CCID Transformation Logic provided by the Plan Processor. Therefore, the Commission believes that it is appropriate to specify that the CCID Transformation Logic for Regulatory Staff will be based on the type of access to the CCID Subsystem sought by Regulatory Staff. For Manual CCID Subsystem Access, the Plan Processor would embed the CCID Transformation Logic in the client-side code of the CAIS/CCID Subsystem Regulator Portal; [210] for Programmatic CCID Subsystem Access, Participants would use the CCID Transformation Logic with an API provided by the Plan Processor.[211] Providing the CCID Transformation Logic in this manner would facilitate ITIN(s) and SSN(s) not being submitted to the CAT.[212]

The Commission preliminarily believes that the proposed amendments addressing the structure and operation of the CCID Subsystem are appropriate. Requiring that the CCID Subsystem be implemented using network segmentation principles to ensure traffic can be controlled between the CCID Subsystem and other components of the CAT System will facilitate the CCID Subsystem being designed, deployed, and operated as a separate and independent system within the CAT system. Strong separation of duties also will add an additional level of protection against unlawful access to the CCID Subsystem, CAIS, or any other component of the CAT System. Minimizing the need for human intervention in the operation of the CCID Subsystem and any data in the CCID Subsystem should also help minimize the introduction of human data-entry errors into the operation of the CCID Subsystem.

Finally, the existing CAT NMS Plan requires that the Participants provide to the SEC a Regular Written Assessment pursuant to Article VI, Section 6.6(b)(i)(A). As proposed, the Participants must include in this assessment an assessment of the overall performance and design of the CCID Subsystem and the process for creating Customer-ID(s).[213] The Commission believes these amendments are appropriate because the assessment required by Article VI, Section 6.6.(b)(i)(A) includes an assessment of the CAT System, and the overall performance and design of the CCID Subsystem and the process for creating Customer-ID(s) are elements of the CAT System.[214]

The Commission requests comment on the proposed amendments that would serve to describe the process for creating Customer-ID(s) in light of the revised reporting requirements. Specifically, the Commission solicits comment on the following:

65. The proposed amendments define the ''CAIS'' as the Customer and Account Information System within the CAT System that collects and links Customer-IDs to Customer and Account Attributes and other identifiers for queries by Regulatory Staff. Are there other data elements that should be included in CAIS, and if so, what are they and why would it be appropriate to include them? How would adding these data elements to the CAIS impact regulatory value? Please explain.

66. The proposed amendments define the ''CAIS/CCID Subsystem Regulator Portal'' as the online tool enabling Manual CAIS access and Manual CCID Subsystem access. Is the term ''online tool'' in the proposed definition sufficient to describe the manner of access, or would it be beneficial to provide more detail regarding the access mechanism? Please explain.

67. The proposed amendments define the ''CCID Subsystem'' as the subsystem within the CAT System that will create the Customer-ID from a Transformed Value, as set forth in Section 6.1(v) and Appendix D, Section 9.1. Would it be beneficial to provide more information about how the CCID Subsystem functions based on the substance of Section 6.1(v) and Appendix D, Section 9.1 in the proposed definition? If so, what additional information would be helpful?

68. The proposed amendments define ''CCID Transformation Logic'' as the mathematical logic identified by the Plan Processor that accurately transforms an individual taxpayer

[206] The Industry Member CAT Reporter Portal is a web-based tool that allows CAT Reporters to monitor and manage data submissions to the CAT. *See* Industry Member CAT Reporter Portal User Guide, Version 1.0 (dated April 20, 2020) at 4, available at *https://www.catnmsplan.com/sites/default/files/2020-04/IM%20Reporter%20Portal%20User%20Guide_04202020.pdf.*

[207] The machine-to-machine interface is available via the CAT Secure File Transfer Protocol (''SFTP'') Accounts, which enable Industry Members and CAT Reporting Agents to create a machine-to-machine connection to securely transmit data to CAT and receive related feedback. *See* FINRA CAT Industry Member Onboarding Guide, Version 1.9 (dated April 15, 2020) at 17, available at *https://www.catnmsplan.com/sites/default/files/2020-04/FINRA%20CAT%20Onboarding%20Guide%20v1.9.pdf.*

[208] *See* proposed Appendix D, Section 9.1 (The CCID Subsystem).

[209] SEC staff shall have the same access to and functionalities of the CAT as Regulatory Staff. For example, in the case of ITIN(s) and SSN(s), SEC would receive these data elements from sources outside of the CAT and use the CCID Transformation Logic for Regulatory Staff to convert such data elements into Customer-IDs. *See* proposed Section 4.1.6 of Appendix D, Manual CCID Subsystem Access and Programmatic CCID Subsystem Access.

[210] *See infra* Part II.F.4 for a discussion on Manual CCID Subsystem access.

[211] *See infra* Part II.F.; *see also* proposed Appendix D Section 4.1.6. EINs are published in publicly available documents and will continue to be submitted to the CAT as Customer Attributes.

[212] Manual CCID Subsystem access would only be used when Regulatory Staff or SEC staff already have the ITIN(s)/SSN(s)/EIN(s) associated with a Customer of regulatory interest through regulatory efforts that have taken place outside of the CAT. *See* proposed Section 4.1.6 of Appendix D, Manual CCID Subsystem Access.

[213] *See* CAT NMS Plan *supra* note 3, Section 6.6.

[214] Article VI, Section 6.6(b)(i)(A) provides that ''annually, or more frequently in connection with any review of the Plan Processor's performance under this Agreement pursuant to Section 6.1(n), the Participants shall provide the SEC with a written assessment of the operation of the CAT that meets the requirements of SEC Rule 613, Appendix D, and this Agreement.'' *See* CAT NMS Plan *supra* note 3, Article VI, Section 6.6(b)(i)(A). The ''CAT System'' is defined to mean ''all data processing equipment, communications facilities, and other facilities, including equipment, utilized by the Company or any third parties acting on the Company's behalf in connection with operation of the CAT and any related information or relevant systems pursuant to this Agreement,'' which would include the CCID Subsystem. *See* CAT NMS Plan Section 1.1 ''Cat System.''

identification number, SSN, or EIN into a Transformed Value for submission into the CCID Subsystem, as set forth in Appendix D, Section 9.1. Would it be beneficial to provide more information in the proposed definition about how the CCID Transformation Logic functions based on the substance of Appendix D, Section 9.1? If so, what additional information would be helpful?

69. The proposed amendments define the ''Transformed Value'' as the value generated by the CCID Transformation Logic, as set forth in proposed Section 6.1(v) and Appendix D, Section 9.1. Would it be beneficial to provide more information in the proposed definition about how the Transformed Value is used, based on the substance of proposed Section 6.1(v) and Appendix D, Section 9.1? If so, what additional information would be helpful?

70. The proposed amendments contain a description of how the Plan Processor would generate a Customer-ID, which would be made available to Regulatory Staff for queries, by using a two-phase transformation process that does not require ITINs, SSNs, or EINs to be reported to the CAT. Is the description of this process sufficient for a clear understanding of the process? Is the description of the process sufficient for a clear understanding of the process for generating a Customer-ID for a Customer that does not have an ITIN/SSN (*e.g.,* a non-U.S. citizen Customer)? Would additional detail be beneficial for understanding the process? If so, please explain what kind of detail would be helpful.

71. The proposed amendments state that Industry Members or Regulatory Staff will transform the ITINs, SSNs, or EINs of a Customer using the CCID Transformation Logic into a Transformed Value, which will be submitted to the CCID Subsystem with any other information and additional elements required by the Plan Processor to establish a linkage between the Customer-ID and Customer and Account attributes. Are there other factors that would impact the ability of Industry Members or Regulatory Staff to execute the transformation process as described and to submit Transformed Values to the CCID Subsystem? If so, please explain.

72. For Industry Members, the proposed amendments state that the CCID Transformation Logic will be either embedded in the CAT Reporter Portal or used by the Industry Member in machine-to-machine processing. Would additional detail be helpful for understanding the process? Do commenters understand what is meant by machine-to-machine processing? Please explain what kind of additional detail would be helpful.

73. Do commenters agree that requiring the CCID Subsystem to be implemented using network segmentation principles to ensure that traffic can be controlled between the CCID Subsystem and other components of the CAT System, with strong separation of duties between it and all other elements of the CAT System, would be an effective mechanism to provide protection against unlawful access to the CCID Subsystem and any other component of the CAT System? Would additional requirements be beneficial? If so, please specify and explain why it would be appropriate to include them.

74. As proposed, the Participants would be required to meet certain standards with respect to the process for creating Customer-IDs, *i.e.,* ensuring the timeliness, accuracy, completeness, and integrity of a Transformed Value, and ensuring the accuracy and overall performance of the CCID Subsystem. Do commenters agree that these standards would serve to accomplish the purpose of accurately attributing order flow to a Customer-ID? If not, please specify how the standards could be modified to achieve their intended goal and explain why it would be appropriate to impose these modified standards.

75. As proposed, the Participants are required to assess both (1) the overall performance and design of the CCID Subsystem, and (2) the process for creating Customer-IDs annually as part of each annual Regular Written Assessment. Are there other specific aspects of the CCID Subsystem or the Customer-ID creation process that might benefit from regular assessment? If so, please specify and explain why it would be appropriate to include them.

3. Plan Processor Functionality To Support the Creation of Customer-ID(s)

The CCID Subsystem needs to function appropriately and be sufficiently secure. Therefore, the Commission proposes amendments to Article VI, Section 6 to add a new Section 6.1(v) that would require the Plan Processor to develop, with the prior approval of the Operating Committee, specific functionality to implement the process for creating a Customer-ID(s), consistent with both Section 6.1 and Appendix D, Section 9.1.[215] With respect to the CCID Subsystem specifically, the proposed amendments would also require the Plan Processor to develop functionality to: Ingest Transformed Value(s) and any other required information and convert the Transformed Value(s) into an accurate Customer-ID(s); validate that the conversion from the Transformed Value(s) to the Customer-ID(s) is accurate and reliable; and transmit the Customer-ID(s), consistent with Appendix D, Section 9.1, to CAIS or a Participant's SAW.[216]

The Commission also preliminarily believes that it is appropriate to require the Plan Processor to develop the functionality by the CCID Subsystem to ingest the Transformed Value(s), along with any other information and additional events as may be prescribed by the Plan Processor that would enable the final linkage between the Customer-ID and the Customer Account Attributes and convert the Transformed Value(s) into an accurate and reliable Customer-ID(s); to validate that the conversion from the Transformed Value(s) to the Customer-ID(s) is accurate and reliable; and to transmit the Customer-ID(s) to CAIS or a Participant's SAW because these are the critical operational phases that must be performed by the CCID Subsystem in order to facilitate the creation of accurate Customer-IDs.

The Commission requests comment on the proposed amendments that would serve to impose specific obligations on the Plan Processor that will support the revised reporting requirements and creation of Customer-ID(s). Specifically, the Commission solicits comment on the following:

76. The proposed amendments require the Plan Processor to develop, with the prior approval of the Operating Committee, the functionality to implement the process for creating Customer-IDs consistent with this section and Appendix D, Section 9.1. Are the details provided in relation to developing this functionality between this section and Appendix D, Section 9.1 sufficient for purposes of implementation? Would additional detail be beneficial? If so, please explain.

77. With respect to the CCID Subsystem, the proposed amendments require the Plan Processor to develop functionality to (1) ingest Transformed Values and any other required information to convert the Transformed Values into an accurate and reliable Customer-IDs, (2) validate that that conversion from the Transformed Values to the Customer-IDs is accurate, and (3) transmit the Customer-IDs, consistent with Appendix D, Section 9.1, to CAIS or a Participant's SAW. Should the proposed amendments be

[215] *See* proposed Section 6.1(v) (Plan Processor).

[216] *See* proposed Section 6.1(v).

more specific about what kind of functionality must be provided by the Plan Processor? If so, please explain what kinds of details would be helpful.

4. Reporting Transformed Value

The Commission proposes to amend Article VI, Section 6.4 of the CAT NMS Plan to adopt Article VI, Section 6.4(d)(ii)(D) to require Industry Members to report on behalf of all Customers that have an ITIN/SSN/EIN the Transformed Value for that Customer's ITIN/SSN/EIN.[217] The Commission preliminarily believes these amendments are appropriate because they reflect the fact that Industry Members will be required to report the Transformed Value for their Customers in order to create the Customer-IDs for natural person and legal entity Customers, rather than the ITIN/SSN/EIN of such a Customer.

The Commission requests comment on the proposed amendments that relate to reporting required Industry Member Data in Section 6.4(d)(ii). Specifically, the Commission solicits comment on the following:

78. The proposed amendments require Industry Members to report on behalf of all Customers that have an ITIN/SSN/EIN the Transformed Value for that Customer's ITIN/SSN/EIN. Are there any factors that could impact the ability of Industry Members to report the Transformed Value? Please explain.

5. Data Availability Requirements

Appendix D, Section 6.2 (Data Availability Requirements) of the CAT NMS Plan generally addresses the processing of information identifying Customers that is reported by Industry Members to the CAT, the reporting timeframes for such information that must be met by Industry Members, and the availability of such information to regulators.[218] The Commission proposes to amend this section to require that (i) Industry Members submit Customer and Account Attributes and Transformed Values to the CCID Subsystem and CAIS, which are a part of the Central Repository, by the same deadline already required by the CAT NMS Plan (no later than 8:00 a.m. Eastern Time on T+1); [219] (ii) the CAT NMS Plan's validation; generation of error reports; processing and resubmission of data; correction of data; and resubmission of corrected data requirements in Appendix D, Section 6.2 apply to the CCID Subsystem and CAIS, which are part of the Central Repository, and (iii) Customer and Account Attributes and Customer-IDs be available to regulators immediately upon receipt of initial data and corrected data, pursuant to security policies for retrieving Customer and Account Attributes and Customer-IDs.[220] Finally, the Commission proposes to replace references to the term ''PII'' in this section with references to ''Customer and Account Attributes.''

In order to provide Regulatory Staff with access to Customer and Account Attributes in a timely manner, the Commission believes it is appropriate for the proposed amendments to set forth the requirements for (i) processing Customer and Account Attributes and Transformed Value(s) that are reported by Industry Members to the CAT, (ii) the reporting timeframes for such information identifying a Customer(s) that must be met by Industry Members, and (iii) the availability of such information to regulators.

6. Customer and Account Attributes in CAIS and Transformed Values

Appendix D, Section 9.1 of the CAT NMS Plan (Customer and Customer Account Information Storage) generally addresses the attributes identifying a Customer that are required to be reported to and collected by the Plan Processor; the validation, maintenance and storage of such attributes; the creation and use of a Customer-ID; and the manner in which attributes identifying a Customer should initially be reported to the Central Repository.[221] Appendix D, Section 9.2 generally lists the account attributes that would be reported to and collected by the Central Repository.[222] The Commission proposes to combine those sections into one section that would comprehensively list all the Customer and Account Attributes that Industry Members must report to CAT and clarify existing requirements in the CAT NMS Plan. Accordingly, Section 9.2 will reflect the entire list of Customer and Account Attributes and other identifiers associated with a Customer (*e.g.,* Firm Designated IDs) that must be reported by Industry Members. The Commission also proposes that for the name field, the first, middle, and last name must be reported; and for the address field, the street number, street name, street suffix and/or abbreviation (*e.g.,* road, lane, court, etc.), city, state, zip code, and country must be provided.[223] The Commission also proposes changes that would organize the attributes reported by Industry Members so that all attributes identifying a Customer would be grouped together and all attributes identifying an account would be grouped together (including any attributes currently listed in Sections 9.1 and 9.2 of the CAT NMS Plan).

The proposed amendments also would address the storage of Customer Account Attributes by requiring that ''[t]he CAT must collect and store Customer and Account Attributes in a secure database physically separated from the transactional database'' and would require that ''[t]he Plan Processor must maintain valid Customer and Account Attributes for each trading day and provide a method for Participants' Regulatory Staff and SEC staff to easily obtain historical changes to Customer-IDs, Firm Designated IDs, and all other Customer and Account Attributes.'' [224] The proposed amendments also would require that Industry Members initially submit full lists of Customer and Account Attributes, Firm Designated IDs, and Transformed Values for all active accounts and submit updates and changes on a daily basis.[225] In addition, the proposed amendments would require that the Plan Processor must have a process to periodically receive updates, including a full refresh of all Customer and Account Attributes, Firm Designated IDs, and Transformed Values to ensure the completeness and

[217] *See* proposed Section 6.4(d)(ii)(D); *see also infra* Part II.K (Firm Designated ID and Allocation Reports) for a discussion that addresses another proposed amendment to Section 6.4(d)(ii), specifically a proposed amendment that would require Customer and Account Attributes and Firm Designated IDs associated with Allocation Reports to be reported.

[218] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 6.2.

[219] *See* proposed Appendix D, Section 6.2.

[220] Previously, this section of Section 6.2 of Appendix D required that PII must be must be available to regulators immediately upon receipt of initial data and corrected data, pursuant to security policies for retrieving PII. *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 6.2. Raw unprocessed data that has been ingested by the Plan Processor must be available to Participants' regulatory staff and the SEC prior to 12:00 p.m. Eastern Time on T+1. Access to all iterations of processed data must be available to Participants' regulatory staff and the SEC between 12:00 p.m. Eastern Time on T+1 and T+5. *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 6.2. Processing timelines start on the day the order event is received by the Central Repository for processing. Most events must be reported to the CAT by 8:00 a.m. Eastern Time the Trading Day after the order event occurred, which is referred to as the transaction date. *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 6.1.

[221] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 9.1. The Central Repository includes the CAIS system. The CAT NMS Plan defines ''Central Repository'' to mean ''the repository responsible for the receipt, consolidation, and retention of all information reported to the CAT pursuant to SEC Rule 613 and this Agreement.'' *See* CAT NMS Plan, *supra* note 3 at Section 1.1.

[222] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 9.2.

[223] *See* proposed Appendix D, Section 9.2.

[224] *See id.*

[225] *See id.*

accuracy of the data in CAIS, and would require that the Central Repository must support account structures that have multiple account owners and associated Customer and Account Attributes, and must be able to link accounts that move from one Industry Member to another.[226] Finally, the proposed amendments would delete the requirement that previous name and previous address be reported to the CAT.[227]

The Commission preliminarily believes that the proposed amendments to Section 9.2 of Appendix D are appropriate because the CAT NMS Plan currently includes an incomplete list of all the Customer and Account Attributes that must be reported to the CAT. The proposed amendments would provide a list of all of the Customer and Account Attributes that Industry Members must report and would retain existing requirements in the CAT NMS Plan related to the availability of historical changes and the assignment of Customer-IDs, as well as reflect new definitions and reporting requirements (*e.g.,* the requirement to report the Transformed Value to the CCID Subsystem). The proposed amendments also would update the CAT NMS Plan's requirement regarding the initial submission of full lists of Customer and Account Attributes and subsequent updates and refreshes of such information to reflect that these requirements would apply to Customer and Account Attributes, Firm Designated IDs, and associated Transformed Values.

The Commission also believes that it is appropriate to amend the CAT NMS Plan to require that the name field for Customers include the Customer's first name, middle name, and last name, and that the address field include the street number, street name, street suffix and/or abbreviation (*e.g.,* road, lane, court, etc.), city, state, zip code, and country.[228] The Commission understands that such specificity is already collected by broker-dealer databases identifying individuals and believes that this level of specificity is required to facilitate regulatory or surveillance efforts, and could diminish the need to conduct broader searches of CAIS in order to identify an individual of regulatory interest because such specificity would enable more focused searches of CAT Customer and Account Attributes. Deleting the requirement for previous name and previous address fields to be reported is also appropriate because such information can be determined by the Plan Processor when providing historical information for the name and address attributes, as required by the proposed amendments to this section.

The Commission requests comment on the proposed amendments that would combine Sections 9.1 and 9.2 of Appendix D of the CAT NMS Plan and the proposed revisions therein. Specifically, the Commission solicits comment on the following:

79. For natural persons, Appendix D, Section 9.1 requires a name attribute to be captured and stored. For implementation purposes, the proposed amendments would specify that all of the aspects of the ''Name'' attribute must be captured, including first, middle, and last name, as separate fields within the attribute. Do commenters agree that adding specificity to the ''Name'' attribute would aid in facilitating regulatory or surveillance efforts by enhancing the ability for regulators to search the data? Would it be helpful to add more specificity to any other attributes in proposed Appendix D, Section 9.1 for implementation purposes? For example, would it be helpful to add a name suffix (*e.g.,* Jr.)?

80. For both natural persons and legal entities, Appendix D, Section 9.1 requires an address attribute to be captured and stored. For implementation purposes, the proposed amendments would specify that all of the aspects of the ''Address'' attribute must be captured, including street number, street name, street suffix and/or abbreviation (*e.g.,* road, lane, court, etc.), city, state, zip code, and country, as separate fields within the attribute. Do commenters agree that adding specificity to the ''Address'' attribute would aid in facilitating regulatory or surveillance efforts by enhancing the ability for regulators to search the data? Alternatively, could this search capability be a function of the CAIS/CCID Subsystem Regulator Portal rather than a reporting requirement for Industry Members?

81. Would it be helpful to add more specificity to any other attributes in proposed Appendix D, Section 9.2 for implementation purposes? For example, would it be helpful to add the last four digits to the zip code in the address attribute, so that the full nine digit zip code would be captured? Please identify what separate fields could be included within the attribute, and why it would be appropriate to include them.

82. Appendix D, Section 9.1 requires full account lists for all active accounts and subsequent updates and changes to be submitted to the Plan Processor. As part of the process for periodically receiving updates, the proposed amendments would require the Plan Processor to have a process to periodically receive updates, rather than full account lists, which could include a full refresh of all Customer and Account Attributes, Firm Designated IDs, and Transformed Values. Would it be appropriate to require the Plan Processor to have a process to periodically receive a full refresh update?

7. Customer-ID Tracking

Appendix D, Section 9.3 (Customer-ID Tracking) generally describes the creation, linking, and persistence of a Customer-ID for use by regulators.[229] The Commission proposes to amend this section to require that Customer-IDs would be created based on the Transformed Value, rather than the ITIN/SSN of a natural person Customer, and that the Customer-ID for a legal entity would be based on the EIN for the legal entity Customer, as discussed above.[230] The Commission also proposes to amend the CAT NMS Plan to require the Plan Processor to resolve discrepancies in the Transformed Values.[231] The Commission preliminarily believes these amendments are appropriate because they reflect the fact that ITINs/SSNs will no longer be reported to the CAT but that Transformed Values will be reported to and collected by the CAT, and that existing requirements regarding Customer-IDs and their function will continue to be required for natural person Customers and Customers that are legal entities under the amendments proposed by the Commission. In addition, the CAT NMS Plan currently requires that the Participants and the SEC must be able to use the unique CAT-Customer-ID to track orders from any Customer or group of Customers, regardless of what brokerage account was used to enter the order. The Commission proposes to amend this section to explicitly require that Participants and the SEC be able to use

[226] *See id.*

[227] *See id.*

[228] *See* proposed Appendix D, Section 9.2.

[229] Currently, Section 9.3 of Appendix D provides that ''The Plan Processor will assign a CAT-Customer-ID for each unique Customer. The Plan Processor will determine a unique Customer using information such as SSN and DOB for natural persons or entity identifiers for Customers that are not natural persons and will resolve discrepancies. Once a CAT-Customer-ID is assigned, it will be added to each linked (or unlinked) order record for that Customer. Participants and the SEC must be able to use the unique CAT-Customer-ID to track orders from any Customer or group of Customers, regardless of what brokerage account was used to enter the order.'' *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 9.3.

[230] *See supra* Part II.E.2.

[231] *See* proposed Appendix D, Section 9.3.

the unique Customer-ID to track allocations to any Customer or group of Customers over time, regardless of what brokerage account was used to enter the order as well. The Commission believes these changes are appropriate so that regulators can track Customer-IDs over time.

The Commission requests comment on the proposed amendments to Appendix D, Section 9.3 (Customer-ID Tracking) of the CAT NMS Plan. Specifically, the Commission solicits comment on the following:

83. Are there any factors that could impact the ability of the Plan Processor to resolve discrepancies in the Transformed Values?

8. Error Resolution for Customer Data

Appendix D, Section 9.4 (Error Resolution for Customer Data) currently addresses the Plan Processor's general obligations with respect to errors, and minor and material inconsistencies.[232] Section 9.4 of Appendix D requires the Plan Processor to design and implement procedures and mechanisms to handle both minor and material inconsistencies in Customer information, and to accommodate minor data discrepancies such as variations in road name abbreviations in searches.[233] This section of the CAT NMS Plan further provides that material inconsistencies such as two different people with the same SSN must be communicated to the submitting CAT Reporters and resolved within the established error correction timeframe as detailed in Section 8.[234] Regarding the audit trail showing the resolution of all errors, this provision also requires that the audit trail include certain information including, for example, the CAT Reporter; the initial submission date and time; data in question or the ID of the record in question; and the reason identified as the source of the issue.[235]

The Commission preliminarily believes that it is appropriate to apply the error resolution process to the CCID Subsystem and CAIS; to provide details as to how the existing validation requirements of Section 7.2 of Appendix D relate to the CCID Subsystem and CAIS; and to amend the existing audit trail requirements addressing the resolution of all errors to take into account the revised reporting requirements that would require the submission of Transformed Values by Industry Members and Participants.

Accordingly, the proposed amendments to Section 9.4 would require that the CCID Subsystem and CAIS support error resolution functionality which includes the following components: Validation of submitted data, notification of errors in submitted data, resubmission of corrected data, validation of corrected data, and a full audit trail of actions taken to support error resolution.[236] The proposed amendments also would require, consistent with Section 7.2, the Plan Processor to design and implement a robust data validation process for all ingested values and functionality including, at a minimum: The ingestion of Transformed Values and the creation of Customer-IDs through the CCID Subsystem; the transmission of Customer-IDs from the CCID Subsystem to CAIS or a Participant's SAW; and the transmission and linking of all Customer and Account Attributes and any other identifiers (*e.g.,* Industry Member Firm Designated ID) required by the Plan Processor to be reported to CAIS.[237] The proposed amendments also provide that at a minimum, the validation process should identify and resolve errors with an Industry Member's submission of Transformed Values, Customer and Account Attributes, and Firm Designated IDs including where there are identical Customer-IDs associated with significantly different names, and identical Customer-IDs associated with different years of birth, or other differences in Customer and Account Attributes for identical Customer-IDs.[238] The Commission also proposes to amend Section 9.4 to require that the proposed validations must result in notifications to the Industry Member to allow for corrections, resubmission of corrected data and revalidation of corrected data, and to note that as a result of this error resolution process there will be accurate reporting within a single Industry Member as it relates to the submission of Transformed Values and the linking of associated Customer and Account Attributes reported.[239]

Timely, accurate, and complete CAT Data is essential so that Regulatory Staff and SEC staff can rely on CAT Data in their regulatory and oversight responsibilities.[240] Therefore, the Commission preliminarily believes that these proposed amendments addressing how the Plan Processor must address errors in data reported to CAIS and the CCID Subsystem are appropriate. The proposed amendments also set out the key components that such error resolution functionality must address, namely the validation of submitted data; notification of error in submitted data, resubmission of corrected data, validation of corrected data, and an audit trail of actions taken to support error resolution. Error resolution for each of these key functionalities will help ensure that CAT Data is timely, accurate and complete.

Section 7.2 of Appendix D already requires that CAT Data be validated.[241] The proposed amendments to Section 9.4 provide detail as to how the existing validation process in Section 7.2 of Appendix D should apply to the revised reporting requirements applicable to Industry Members and the process for creating Customer-IDs through the CCID Subsystem. As proposed, the amendments specify that the validation process must address the ingestion of Transformed Values and the creation of Customer-IDs through the CCID Subsystem; the transmission of Customer-IDs to CAIS or the Participant's SAW; and the linking between the Customer-IDs and the Customer and Account Attributes within CAIS.[242] Each of those requirements addresses key reporting requirements and operations that must be validated by the Plan Processor as part of the validation process of CAT Data as required by Section 7.2 of Appendix D. The Commission also believes that the examples of what the validation process should, at a minimum, address is appropriate because these examples relate to the new reporting requirements related to Transformed Values and Customer and Account Attributes, and therefore were not discussed in the CAT NMS Plan. The Commission also preliminarily believes that it is appropriate to amend the CAT NMS Plan to require that the Plan Processor notify Industry Members of errors so that they can correct them. This notification facilitates a process for reporting corrected data to the CAT.

Finally, the Commission also believes that it is appropriate to modify the existing CAT NMS Plan requirement that the Central Repository have an audit trail showing the resolution of all errors, including material inconsistencies, occurring in the CCID Subsystem and CAIS. Article VI, Section 6.5(d) of the CAT NMS Plan requires that CAT Data be accurate, which would

[232] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 9.4.

[233] *See id.*

[234] *See id.*

[235] *See id.*

[236] *See id.*

[237] *See id.*

[238] *See id.*

[239] *See id.*

[240] *See* CAT NMS Plan Approval Order, *supra* note 3, at Part III.19 ''Error Rates.''

[241] *See* CAT NMS Plan, *supra* note 3, Appendix D Section 7.2.

[242] *See* proposed Appendix D Section 9.4.

include data that is reported to the CCID Subsystem and CAIS.[243] The Commission is proposing that there be an audit trail showing the resolution of all errors, including material inconsistencies, occurring in the CCID Subsystem and CAIS because tracking error resolution will assist in identifying compliance issues with CAT Reporters, and therefore help ensure that CAT Data is accurate.

84. The proposed amendments would require the Plan Processor to design and implement a robust data validation process for all ingested values and functionality, consistent with Appendix D, Section 7.2. Are the minimum requirements set forth for inclusion in this data validation process sufficiently detailed for the purposes of implementing such a process? Should the proposed amendments be more specific about what kind of capability must be provided by the Plan Processor? If so, please explain what kinds of details would be helpful.

85. The proposed amendments would require the CCID Subsystem and CAIS to support error resolution functionality which includes the following components: Validation of submitted data, notification of errors in submitted data, resubmission of corrected data, validation of corrected data, and an audit trail of actions taken to support error resolution. Do the proposed amendments set forth the components of the error resolution functionality that must be supported by the CCID Subsystem and CAIS with an appropriate amount of detail? If not, should other details be added or are some not necessary?

86. Appendix D, Section 9.4 requires the Central Repository to have an audit trail showing the resolution of all errors. The proposed amendments would require the audit trail to show the resolution of all errors, including material inconsistencies, occurring in the CCID Subsystem and CAIS. Do the proposed amendments set forth the components of the audit trail requirements with an appropriate amount of detail? If not, what details should be added or are some not necessary?

87. Should the proposed amendments address error resolution requirements with respect to Transformed Values and Customer and Account Attributes, and reporting Transformed Values to the CCID Subsystem and Customer and Account Attributes to CAIS? If error resolution requirements are not applied to Transformed Values and Customer and Account Attributes, and reporting Transformed Values to the CCID Subsystem and Customer and Account Attributes to CAIS, how would errors in those data elements be identified and corrected? Please be specific in your response.

9. CAT Reporter Support and CAT Help Desk

Currently, Appendix D, Section 10.1 of the CAT NMS Plan addresses the technical, operational, and business support being offered by the Plan Processor to CAT Reporters as applied to all aspects of reporting to CAT, and Section 10.3 of Appendix D addresses the responsibilities of the CAT Help Desk to support broker-dealers, third party CAT Reporters, and Participant CAT Reporters with questions and issues regarding reporting obligations and the operation of the CAT.[244] The Commission proposes to amend the CAT NMS Plan to add the requirements that (i) the Plan Processor would also provide CAT Reporter Support and Help Desk support for issues related to the CCID Transformation Logic and reporting required by the CCID Subsystem, and (ii) the Plan Processor would have to develop tools to allow each CAT Reporter to monitor the use of the CCID Transformation Logic, including the submission of Transformed Values to the CCID Subsystem.[245] The Commission believes these amendments are appropriate so that all CAT Reporters who must submit Transformed Values to the CCID Subsystem can get the assistance that they need should any problems arise with their efforts to report the required data to the CAT.

The Commission requests comment on the proposed amendments that would amend Appendix D, Sections 10.1 and 10.3 of the CAT NMS Plan. Specifically, the Commission solicits comment on the following:

88. With respect to CAT Reporter support, the proposed amendments would require the Plan Processor to develop functionality that allows each CAT Reporter to monitor the use of the CCID Transformation Logic including the submission of Transformed Values to the CCID Subsystem. Should the proposed amendments be more specific about what kind of functionality must be provided by the Plan Processor? If so, please explain what kinds of details would be helpful.

89. The proposed amendments would require the CAT Help Desk to support responding to questions from and providing support to CAT Reporters regarding all aspects of the CCID Transformation Logic and CCID Subsystem. Are there any specific aspects that should be enumerated in relation to CAT Help Desk support?

F. Customer Identifying Systems Workflow

The CAT NMS Plan currently requires Industry Members to report PII[246] to the CAT, and states that such ''PII can be gathered using the 'PII workflow' described in Appendix D, Data Security, PII Data Requirements.''[247] However, the ''PII workflow'' was neither defined nor established in the CAT NMS Plan.[248] While the modifications proposed by the Commission in Part II.E no longer require a Customer's ITIN(s)/SSN(s), account number and date of birth be reported to and collected by the CAT, Customer and Account Attributes, as described in Part II.E., are still reported to and collected by the CAT and could be used to attribute order flow to a single Customer across broker-dealers.[249] The collection of Customer and Account Attributes and access to such attributes will facilitate the ability of Regulatory Staff to carry out their regulatory and oversight obligations.[250] Therefore, the Commission is proposing to amend the CAT NMS Plan to define the Customer Identifying Systems Workflow for accessing Customer and Account Attributes, and to establish restrictions governing such access. Accordingly, the Commission proposes to amend the CAT NMS Plan to (1) specify how existing data security requirements apply to Customer and Account Attributes; (2) define the Customer Identifying Systems; (3) establish general requirements that must be met by Regulatory Staff before accessing the Customer Identifying Systems, which access will be divided between two types of access—manual access and programmatic access; and (4) establish the specific requirements for each type of access to the Customer Identifying Systems.[251]

[243] *See* CAT NMS Plan, *supra* note 3, Article VI, Section 6.5(d).

[244] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Sections 10.1 and 10.3.

[245] *See* proposed Appendix D, Sections 10.1 and 10.3.

[246] *See supra* note 10.

[247] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 4.1.6.

[248] *Id.*

[249] *See supra* Part II.E; *see also* proposed Section 1.1 for the proposed definition of ''Customer and Account Attributes.''

[250] *See supra* Part II.E for a discussion of the changes to the data collected by the CAT that would identify an individual or legal entity, and the associated defined term ''Customer and Account Attributes.''

[251] *See* proposed Appendix D, Section 4.1.6 (Customer Identifying Systems Workflow).

1. Application of Existing Plan Requirements to Customer and Account Attributes and the Customer Identifying Systems

Appendix D, Section 4.1.6 of the CAT NMS Plan currently requires that PII must be stored separately from other CAT Data, and that PII must not be accessible from public internet connectivity.[252] The CAT NMS Plan also states that PII data must not be included in the result set(s) from online or direct query tools, reports, or bulk data extraction; instead, results are to display existing non-PII unique identifiers (*e.g.,* Customer-ID or Firm Designated ID).[253] The PII corresponding to these identifiers can be gathered using a ''PII workflow.'' [254] The CAT NMS Plan also provides that by default, users entitled to query CAT Data are not authorized for PII access, and that furthermore the process by which someone becomes entitled to PII access, and how they then go about accessing PII data, must be documented by the Plan Processor.[255] The chief regulatory officer, or other such designated officer or employee at each Participant must review and certify that people with PII access have the appropriate level of access for their role at least annually.[256] The CAT NMS Plan also provides that a full audit trail of PII access (*i.e.,* who accessed what data, and when) must be maintained, and that the Chief Compliance Officer and the Chief Information Security Officer must have access to daily PII reports that list all users who are entitled to PII access, as well as the audit trail of all PII access that has occurred for the day being reported upon.[257] In other sections of the CAT NMS Plan, PII data is also required to be ''masked'' unless a user has permission to view it.[258]

The Commission proposes to amend these provisions to replace the term ''PII'' with ''Customer and Account Attributes'' and to reflect that Customer Identifying Systems, including CAIS, would now contain the information that identifies a Customer.[259] Accordingly, the proposed amendments to Appendix D, Section 4.1.6 would provide that Customer and Account Attributes data must be stored separately from other CAT Data within the CAIS, that Customer and Account Attributes cannot be stored with the transactional CAT Data in the Central Repository, and that Customer and Account Attributes must not be accessible from public internet connectivity. Similarly, the proposed amendments would provide that Customer and Account Attributes must not be included in the result set(s) from online or direct query tools, reports, or bulk data extraction tools used to query transactional CAT Data. Instead, query results of transactional CAT Data would display unique identifiers (*e.g.,* Customer-ID or Firm Designated ID) and the Customer and Account Attributes corresponding to these identifiers could be gathered by accessing CAIS in accordance with the ''Customer Identifying Systems Workflow,'' as described in the proposed amendments and discussed below. The proposed amendments would provide that, by default, users entitled to query CAT Data would not be authorized to access Customer Identifying Systems, and the process by which someone becomes entitled to Customer Identifying Systems and how an authorized person then could access Customer Identifying Systems, would have to be documented by the Plan Processor. The proposed amendments also would modify the CAT NMS Plan to require that a similarly designated head(s) of regulation or the designee of the chief regulatory officer or such similarly designated head of regulation must, at least annually, review and certify that people with Customer Identifying Systems access have the appropriate level of access for their role, in accordance with the Customer Identifying Systems Workflow, as discussed and described below.[260]

The proposed amendments also would modify the requirement related to maintaining a full audit trail to require that the audit trail must reflect access to the Customer Identifying Systems by each Participant and the Commission (*i.e.,* who accessed what data, and when), and to require that the Plan Processor provide to each Participant and the Commission the audit trail for their respective users on a monthly basis. In addition, the proposed amendments would require that the Chief Compliance Officer and Chief Information Security Officer have access to daily reports that list all users who are entitled to Customer Identifying Systems access, and that such reports must be provided to the Operating Committee on a monthly basis.[261]

The Commission believes that the proposed amendments are appropriate because storing Customer and Account Attributes separately from other CAT Data would aid in protecting the confidentiality of Customer identifying information that is reported to and collected by the CAT, and would reflect what the CAT NMS Plan currently requires for PII.[262] Moreover, Customer and Account Attributes should neither be stored with transactional CAT Data nor be accessible by public internet in order to further aid in protecting this information. Similarly, to help safeguard Customer and Account Attributes, such attributes should not be included in result set(s) obtained from online or direct query tools or bulk extraction tools. The proposed amendments that would permit a designated head of regulation similar to the chief regulatory officer, or his or her designee, to at least annually review and certify that people with Customer Identifying Systems Access have the appropriate level of access for their role in accordance with the Customer Identifying Systems Workflow are appropriate because this change will serve to ease any potential delays in the annual review and certification process. The proposed amendments would accomplish this by expanding the pool of individuals that are authorized to conduct such reviews and certifications.

In addition, the proposed amendments deleting ''masked'' Customer and Account Attributes are appropriate because ''masked'' Customer and Account Attributes implies that certain Customer and Account Attributes (*i.e.,* ''masked'' Customer and Account Attributes) would be made available to certain Regulatory Staff outside of the access requirements set forth in these proposed amendments. The Commission believes that if Regulatory Staff do not meet the requirements to be entitled to access Customer and Account Attributes, then Regulatory Staff should not be allowed to access those Customer and Account Attributes, even if such data were to be masked.

The Commission preliminarily believes it is appropriate to require the Plan Processor to provide the audit trail of access to Customer Identifying Systems by each Participant and the Commission (who accessed what data and when), and to require the Plan

[252] *See* CAT NMS Plan, *supra* note 3, Appendix D, Section 4.1.6.

[253] *See id.*

[254] *See id.*

[255] *See id.*

[256] *See id.*

[257] *See id.*

[258] *See* CAT NMS Plan, *supra* note 3, at Section 6.10(c)(ii) and Appendix D, Section 8.2.2.

[259] *See supra* Part II.E.1; *see also* proposed Appendix D, Section 4.1.6.

[260] Other provisions of the CAT NMS Plan that refer to PII are also proposed to be similarly modified to remove the term ''PII'' and instead refer to ''Customer and Account Attributes'' or ''Customer Identifying Systems'' as appropriate. *See, e.g.,* Appendix D, Sections 4.1.6 and 8.2.2.

[261] *See* proposed Appendix D, Section 4.1.6.

[262] The CAT NMS Plan presently requires PII to be stored separately from other CAT Data. *See* Appendix D, Section 4.1.6.

Processor to provide to each Participant and the Commission the audit trail for their respective users on a monthly basis because providing such information may increase the accountability and transparency into the justification(s) for each Participant's access to Customer Identifying Systems. The benefit of providing the audit trail of Customer Identifying Systems access to each Participant is that it would enable each Participant to monitor use in accordance with their data confidentiality policies, procedures, and usage restriction controls. Similarly, the Commission could use such data in support of their internal policies governing access to Customer Identifying Systems.[263] The Commission also believes that providing the daily reports of all users entitled to access the Customer Identifying Systems to the Operating Committee on a monthly basis would enable Participants and the Operating Committee to verify that only Regulatory Staff who are entitled to access Customer Identifying Systems have such access.

The Commission requests comment on the continued application of existing provisions of Appendix D, Section 4.1.6 to help ensure the security and confidentiality of the information reported to and collected by the Customer Identifying Systems. Specifically, the Commission solicits comment on the following:

90. Existing provisions of the CAT NMS Plan address the security and confidentiality of CAT Data by requiring that PII must be stored separately from other CAT Data. These provisions also specifically require that PII cannot be stored with transactional CAT Data and that PII must not be accessible from public internet connectivity. Should the existing provisions of Appendix D, Section 4.1.6 continue to apply so as to require: (i) That Customer and Account Attributes data are stored separately from other CAT Data within the CAIS, (ii) that Customer and Account Attributes cannot be stored with the transactional CAT Data in the Central Repository, and (iii) that Customer and Account Attributes must not be accessible from public internet connectivity? Why or why not? Please explain with specificity why such provisions should or should not apply.

91. Should existing provisions of Appendix D, Section 4.1.6 continue to apply so as to require that Customer and Account Attributes must not be included in the result set(s) from online or direct query tools, reports, or bulk data extraction tools used to query transactional CAT Data? In addition, is it appropriate to amend the CAT NMS Plan to require that query results of transactional CAT Data will display unique identifiers (*e.g.,* Customer-ID or Firm Designated ID)? If such unique identifiers are not displayed, what should be provided in result set(s) from online or direct query tools, reports, or bulk data extraction tool queries?

92. Is it appropriate to amend the CAT NMS Plan to state that by default, users entitled to query CAT Data are not authorized to access Customer Identifying Systems? Why or why not? Please explain with specificity why this provision should or should not apply and what other process would be appropriate to ensure that only authorized users access the Customer Identifying systems.

93. The existing CAT NMS Plan requires that the Chief Regulatory Officer or another such designated officer or employee at each Participant must at least annually review and certify that people with PII access have the appropriate level of access in light of their respective roles. The proposed amendments state that the review and certification must be made by the Chief Regulatory Officer or similarly designated head(s) of regulation, or his or her designee, at each Participant, and that the Chief Regulatory Officer or similarly designated head(s) of regulation, or his or her designee must, at least annually, review the list of people who have access to Customer Identifying Systems at their organization, the role of each person on the list and the level of access of each person. Based on that review, the Chief Regulatory Office must certify that people with Customer Identifying Systems access have the appropriate level of access for their role, in accordance with the Customer Identifying Systems Workflow. Is it appropriate to continue to facilitate oversight regarding who has access to the Customer Identifying Systems by applying these requirements to the Customer Identifying Systems Workflow? Why or why not? Please explain with specificity why such provisions should or should not apply.

94. Appendix D, Section 4.1.6 of the CAT NMS Plan requires a full audit trail of access to PII (who accessed what data, and when) to be maintained. Should the proposed amendments require that the Plan Processor maintain a full audit trail of access to Customer Identifying Systems by each Participant and the Commission (who accessed what data and when), and require that the Plan Processor provide to each Participant and the Commission the audit trail for their respective users on a monthly basis? Furthermore, should the proposed amendments require that the Chief Compliance Officer and the Chief Information Security Officer l have access to daily reports that list all users who are entitled to Customer Identifying Systems access, and for such reports to be provided to the Operating Committee on a monthly basis? Why or why not? Is there another means of providing information to the Participants and the Operating Committee to facilitate their review of access to Customer Identifying Systems? If so, please identify this means and explain why it would be an appropriate way to facilitate review of access to Customer Identifying Systems.

2. Defining the Customer Identifying Systems Workflow and the General Requirements for Accessing Customer Identifying Systems

Given that Regulatory Staff may seek to access both CAIS and the CCID Subsystem (collectively, the Customer Identifying Systems) in order to carry out their regulatory and oversight responsibilities, the Commission preliminarily believes that it is appropriate to establish access requirements that would apply to both systems. Accordingly, the Commission proposes to amend Section 4.1.6 of Appendix D to require that access to Customer Identifying Systems be subject to the following restrictions, many of which already exist in the CAT NMS Plan today, as discussed below.[264]

First, only Regulatory Staff may access Customer Identifying Systems and such access would have to follow the ''least privileged'' practice of limiting access to Customer Identifying Systems as much as possible.[265] Second, using the role based access control (''RBAC'') model described in the CAT NMS Plan, access to Customer and Account Attributes would have to be configured at the Customer and Account Attributes level.[266] Third, all queries of Customer Identifying Systems would have to be based on a ''need to know''

[263] *See also* Part II.N. *infra,* for a discussion of how the proposed amendments would apply to Commission staff. The Commission understands that a full audit trail of all access to Customer Identifying Systems is required by NIST 800–53.

[264] *See* proposed Appendix D, Section 4.1.6 (Customer Identifying Systems Workflow, Access to Customer Identifying Systems).

[265] The CAT NMS Plan currently states that ''[u]sing the RBAC model described above, access to PII data shall be configured at the PII attribute level, following the 'least privileged' practice of limiting access as much as possible.'' *See* CAT NMS Plan, *supra* note 3, Appendix D, Section 4.1.6 (PII Data Requirements).

[266] *See* proposed Appendix D, Section 4.1.6.

the data[267] in the Customer Identifying Systems, and queries must be designed such that the query results would contain only the Customer and Account Attributes that Regulatory Staff reasonably believes will achieve the regulatory purpose of the inquiry or set of inquiries, consistent with Article VI, Section 6.5(g) of the CAT NMS Plan.[268] Fourth, Customer Identifying Systems would have to be accessed through a Participant's SAW.[269] Fifth, access to Customer Identifying Systems would be limited to two types of access: Manual access (which would include Manual CAIS Access and Manual CCID Subsystem Access, as further discussed below) and programmatic access (which would include Programmatic CAIS Access and Programmatic CCID Subsystem Access, as further discussed below). Lastly, authorization to use Programmatic CAIS Access or Programmatic CCID Subsystem Access would have to be requested and approved by the Commission, pursuant to the process as further described in the proposed amendments below.[270]

The Commission preliminarily believes that the proposal to establish rules applicable to all forms of access to the Customer Identifying Systems by all Participants would facilitate the application of the same requirements and standards across all Regulatory Staff at each Participant seeking access to Customer Identifying Systems. Furthermore, restricting access to Regulatory Staff is appropriate because such staff are required to report directly to the Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation), or to persons within the Participant's Chief Regulatory Officer's (or similarly designated head(s) of regulation's) reporting line, and because such staff must be specifically identified and approved in writing by the Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation).[271] Thus, the proposed amendments would help to ensure that the Participant's staff accessing Customer and Account Attributes and other identifying information about a Customer are doing so for regulatory—not commercial—purposes, and that sufficient oversight of such access by the Participant's Chief Regulatory Officer exists.[272] In addition, by allowing a similarly designated head(s) of regulation to also approve such access, the Commission preliminarily believes that any operational issues in obtaining such approval should be minimized.

The Commission also preliminarily believes that it is appropriate to limit access to Customer Identifying Systems to the minimum level of access that will achieve the Participant's regulatory purposes.[273] For example, a regulator investigating alleged fraud against senior investors may only need the year of birth to investigate such matters; thus, under the ''least privileged practice'' model, such Regulatory Staff would only be entitled to view year of birth from CAIS in response to queries, and would only access the minimum amount of CAT Data, including Customer and Account Attributes, that would be required to conduct their investigation.

The RBAC model, which is already an access requirement contained in the CAT NMS Plan, requires that the Plan Processor grant permission to access certain CAT Data based on the user's regulatory role.[274] The Commission believes it is appropriate to apply the same RBAC model to access to Customer and Account Attributes because not all Regulatory Staff will need to access Customer and Account Attributes, and limitations on such access should be based on the role that such Regulatory Staff fill for the Participant.

The Commission also preliminarily believes that it is appropriate to require that all queries of the Customer Identifying Systems be based on a regulator's ''need to know'' the data in the Customer Identifying Systems, and to require that queries be designed such that query results contain only the Customer and Account Attributes that Regulatory Staff reasonably believes will achieve the regulatory purpose of the inquiry or set of inquiries, consistent with Article VI, Section 6.5(g) of the CAT NMS Plan.[275] The Participants stated that they intended the CAT NMS Plan to require that a regulator ''need to know'' the Customer and Account Attributes, and thus only those users who have ''need to know'' the Customer and Account Attributes will be granted access to the Customer and Account Attributes.[276] The Commission believes that incorporating the ''need to know'' standard in the proposed amendments would require Regulatory Staff to articulate their reasons for needing access to search CAIS or use the CCID Subsystem. These proposed amendments also would help to limit the results of queries to containing only the Customer and Account Attributes that Regulatory Staff reasonably believes will achieve the regulatory purpose of the inquiry or set of inquiries that are being pursued by Regulatory Staff, which would be consistent with the requirements set forth in Article VI, Section 6.5(g) of the CAT NMS Plan.[277]

The Commission believes that the proposed amendments would result in Regulatory Staff continually assessing whether there is a need to know the volume of Customer and Account Attributes that may be returned in response to a query in light of the regulatory purpose of the query being submitted, and whether the query results contain only the Customer and Account Attributes that Regulatory Staff reasonably believes will achieve the regulatory purpose of the Regulatory Staff's inquiry or set of inquiries. The same requirement applies when Regulatory Staff utilizes programmatic access; to the extent applications to query Customer and Account Attributes are developed as part of programmatic access, such applications must support a design that limits Customer and Account Attributes to only those which Regulatory Staff reasonably believes are needed to achieve the regulatory purpose of the inquiry or set of inquiries. The Commission also expects that this assessment would operate as a useful check on the scope of the queries being submitted by Regulatory Staff, and that this requirement would complement the proposed amendments

[267] The Participants stated that they ''anticipate that access to PII will be limited to a 'need-to-know' basis. Therefore, it is expected that access to PII associated with customers and accounts will have a much lower number of registered users, and access to this data will be limited to Participants' staff and the SEC who need to know the specific identity of an individual.'' *See* CAT NMS Plan, *supra* note 3, Appendix C, Section A.4.(b). The Plan also states that ''[t]he Participants are requiring multi-factor authentication and Role Based Access Control for access to PII, separation of PII from other CAT Data, restricted access to PII (only those with a 'need to know' will have access), and an auditable record of all access to PII data contained in the Central Repository.'' *See* CAT NMS Plan Appendix C, Section D.12.(e).

[268] *See id.*

[269] *See id.* For a discussion of the requirements related to SAWs, see *infra* Part II.C.

[270] *See* proposed Appendix D, Section 4.1.6 (Customer and Accounts Attributes Data Requirements).

[271] *See* proposed Section 6.5(g).

[272] *See* Part II.H.1, *infra,* for a discussion of proposed amendments related to restricting access to CAT Data solely for regulatory purposes. Access to Customer and Account Attributes, which are a subset of CAT Data, would be subject to these restrictions.

[273] *See* CAT NMS Plan Approval Order, *supra* note 3 at note 1299.

[274] *See* CAT NMS Plan, *supra* note 3, Appendix D, Section 4.1.4 (Data Access).

[275] *See* proposed Appendix D, Section 4.1.6 (Customer Identifying Systems Workflow, Access to Customer Identifying Systems).

[276] *See* CAT NMS Plan, *supra* note 3, Appendix C, Section A.4(b); *see also* CAT NMS Plan Appendix C, Section D.12.(e).

[277] *See* proposed Appendix D, 4.1.6 (Customer Identifying Systems Workflow).

that address access-level requirements, as discussed above (*i.e.,* that only Regulatory Staff may access Customer Identifying Systems and such access must follow the ''least privileged'' practice of limiting access to Customer Identifying Systems as much as possible).[278]

The Commission also believes that it is appropriate to require that Customer Identifying Systems must be accessed through a Participant's SAW.[279] As described above in Part II.C.3., each Participant's SAW is a secure analytic environment that would be part of the CAT System and therefore subject to the CISP.[280] This provision together with Proposed Section 6.13(a)(i)(A) establishes the SAW as the only means of accessing and analyzing Customer and Account Attributes and applies the security safeguards implemented in a Participant's SAW 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.[281] Requiring access through a Participant's SAW also would enable the Plan Processor to capture information about CAT Data usage by Participants, which would assist Participants in analyzing such usage to determine whether CAT Data is being used for legitimate regulatory or oversight purposes.

The Commission also preliminarily believes that it is appropriate to limit access to the Customer Identifying Systems to two types of access—manual and programmatic.[282] As noted above, the CAT NMS Plan currently follows the ''least privileged'' practice of limiting access to information identifying a Customer to the greatest extent possible.[283] The Commission believes that applying this same security focused, minimum access approach to the data in the Customer Identifying systems is appropriate in order to safeguard the Customer information contained in each system from bad actors who obtain such information through a data breach. The Commission believes that the ''least privileged practice'' approach also means that only Regulatory Staff will be permitted to access Customer Identifying Systems.[284] Accordingly, the Commission is proposing to limit access to those systems to two methods: Manual access (which would include Manual CAIS Access and Manual CCID Subsystem Access) and programmatic access (which would include Programmatic CAIS Access and Programmatic CCID Subsystem Access), which would be subject to an approval process, as further described below, and only granted if certain circumstances are met.[285]

Finally, the Commission preliminarily believes that Programmatic CAIS Access and Programmatic CCID Subsystem Access, as further detailed below, should only be used by Participants if requested and approved by the Commission.[286] Indeed, the Participants represented in the CAT NMS Plan that ''general queries can be carried out using the Customer-ID without the need to know specific, personally-identifiable information (*i.e.,* who the individual Person or legal entity associated with the Customer-ID is). The Customer-ID will be associated with the relevant accounts of that Person; thus, the use of Customer-ID for querying will not reduce surveillance.'' [287] Thus, the Commission preliminarily believes that it is appropriate to require Regulatory Staff to use manual access to Customer Identifying Systems in order to carry out their regulatory responsibilities because such access should meet the regulatory purpose of their inquiry or set of inquiries—and only access CAIS and the CCID Subsystem programmatically if authorized by the Commission.[288]

The Commission requests comment on the proposed amendments to define the Customer Identifying Systems Workflow and the requirements for accessing Customer Identifying Systems. Specifically, the Commission solicits comment on the following:

95. Do Commenters agree that it is necessary to define and set forth the requirements for the Customer Identifying Systems Workflow? If not, what provisions of the CAT NMS Plan apply to govern access to Customer Identifying Systems? Please be specific about those provisions and explain how they protect the information reported to and collected by the Customer Identifying Systems.

96. Is there a different set of requirements that should be applied to the proposed Customer Identifying Systems Workflow? If yes, please describe with specificity what those requirements are and how they would operate to support the security and confidentiality of the information reported to and collected by the Customer Identifying Systems.

97. The proposed amendments require that only Regulatory Staff may access Customer Identifying Systems and such access must follow the ''least privileged'' practice of limiting access to Customer Identifying Systems as much as possible. What are the advantages to limiting access to the Customer Identifying Systems in this manner? Are there other standards of access to Customer Identifying Systems that would be appropriate? If so, what are those standards? Please be specific in your response.

98. The proposed amendments require that access to Customer and Account Attributes shall be configured at the Customer and Account Attributes level using the Role Based Access Model in the Customer Identifying Systems Workflow. Is there another more appropriate way to configure access to Customer and Account Attributes? Should access to identifiers in the transaction database (*e.g.,* Customer-ID(s) or Industry Member Firm Designated ID(s)) be permitted, or entitled, separately such that Regulatory Staff would need specific permissions to access these identifiers? If so, how would regulatory use of CAT Data still be accomplished? Please discuss implementation details addressing both security and usability.

99. The proposed amendments require that all queries of Customer Identifying Systems must be based on a ''need to know'' data in the Customer Identifying Systems. Is there a different standard that should apply to queries of the Customer Identifying Systems and if so, why is that standard more appropriate? Please be specific in your response.

100. The proposed amendments state that the standard for assessing the Customer and Account Attributes that can be returned in response to a query is what Regulatory Staff reasonably believes will achieve the regulatory purpose of the inquiry or set of inquiries in the Customer Identifying Systems Workflow. Is this standard appropriate?

[278] Similar to the requirement that applications developed in connection with programmatic access must support a design that limits the Customer and Account Attributes to only that which Regulatory Staff reasonably believes are needed to achieve the regulatory purpose of the inquiry or set of inquiries as discussed above, these applications also must support all elements of the Customer Identifying Systems Workflow (*e.g.,* following the ''least privileged'' practice of limiting access to Customer Identifying Systems as much as possible).

[279] *See* Part II.C. *supra* for a discussion of the proposed SAWs.

[280] *See* proposed Section 6.13.

[281] *See* proposed Appendix D, Section 4.1.6 (Customer Identifying Systems Workflow).

[282] *See* proposed Appendix D, Section 4.1.6 (Customer Identifying Systems Workflow).

[283] *See supra* note 273.

[284] *See also* Part II.H.1, *infra,* for a discussion of proposed amendments requiring need for regulatory purpose for access to Customer and Account Attributes.

[285] *See* proposed Appendix D, Section 4.1.6.

[286] *See infra* Part II.F.5.

[287] *See* CAT NMS Plan Approval Order, *supra* note 3, at 84983 note 826.

[288] *See* proposed Appendix D, Section 4.1.6 (Customer Identifying Systems Workflow).

Why or why not? If there is another standard that should apply, what should that standard be? Please be specific in your response.

101. The proposed amendments require that Customer Information Systems must be accessed through a Participant's SAW in the Customer Identifying Systems Workflow. Should the proposed amendments permit access other than through a Participant's SAW? If so, is there another way to subject the accessing and analyzing of Customer and Account Attributes to the CISP?

102. The proposed amendments state that access to Customer Identifying Systems will be limited to two types of access: Manual access (which would include Manual CAIS Access and Manual CCID Subsystem Access) and programmatic access (which would include Programmatic CAIS Access and Programmatic CCID Subsystem Access). Are these methods of access appropriate for facilitating the ability of Regulatory Staff to fulfill their regulatory and oversight obligations? Please explain.

103. The proposed amendments require that authorization to use Programmatic CAIS Access or Programmatic CCID Subsystem Access must be requested and approved by the Commission pursuant to the Customer Identifying Systems Workflow. Do Commenters agree that it is appropriate to require Commission authorization to use Programmatic Access to the CAIS and the CCID Subsystem?

3. Introduction to Manual and Programmatic Access

As noted above, the proposed amendments would limit access to Customer Identifying Systems to two general methods of access—manual and programmatic access. Accordingly, the Commission is proposing amendments to the CAT NMS Plan that would define and set forth the requirements for (1) Manual CAIS Access and Manual CCID Subsystem Access; and (2) Programmatic CAIS Access and Programmatic CCID Subsystem Access. A description of the requirements applicable to each method of access follows.

4. Manual CAIS Access

The Commission proposes to amend the CAT NMS Plan to define Manual CAIS Access to mean ''[w]hen used in connection with the Customer Identifying Systems Workflow, as defined in Appendix D, shall mean the Plan Processor functionality to manually query CAIS, in accordance with Appendix D, Data Security, and the Participants' policies as set forth in Section 6.5(g).'' [289] Under the proposed amendments, if Regulatory Staff have identified a Customer(s) of regulatory interest through regulatory efforts and require additional information from the CAT regarding such Customer(s), then they may use Manual CAIS Access.[290] The proposed amendments also would provide that additional information about Customer(s) may be accessed through Manual CAIS Access by (1) using identifiers available in the transaction database (*e.g.,* Customer-ID(s) or Industry Member Firm Designated ID(s)) to identify Customer and Account Attributes associated with the Customer-ID(s) or Industry Member Firm Designated ID(s), as applicable; or (2) using Customer Attributes in CAIS to identify a Customer-ID(s) or Industry Member Firm Designated ID(s), as applicable, associated with the Customer Attributes, in order to search the transaction database.[291] The proposed amendments would not permit open-ended searching of parameters not specific to a Customer(s).[292]

In addition, the Commission proposes to amend the CAT NMS Plan to require that Manual CAIS Access must provide Regulatory Staff with the ability to retrieve data in CAIS via the CAIS/CCID Subsystem Regulator Portal with query parameters based on data elements including Customer and Account Attributes and other identifiers available in the transaction database (*e.g.,* Customer-ID(s) or Industry Member Firm Designated ID(s)).[293]

Finally, the proposed amendments would require that the performance requirements for Manual CAIS Access be consistent with the criteria set out in Appendix D, Functionality of the CAT System, Online Targeted Query Tool Performance Requirements.[294]

These proposed amendments reflect a principle that underlies the required use of manual access to CAIS (and manual access to the CCID Subsystem, as further discussed below) that if Regulatory Staff have already identified a Customer(s) of interest based on their regulatory efforts and Regulatory Staff have a ''need to know'' additional identifying information about the Customer(s), then manual access may be used to obtain such information.[295] For example, manual access would be appropriate if Regulatory Staff have the Customer-ID of a Customer or the Industry Member Firm Designated ID of Customer as a result of a search of the transactional CAT database in furtherance of a regulatory purpose, and Regulatory Staff require additional Customer and Account Attributes associated with that Customer (*e.g.,* the name and address associated with that Customer-ID). Manual CAIS Access also would be appropriate if Regulatory Staff have identifying information that are Customer and Account Attributes (*e.g.,* name or address of a natural person Customer) and have a regulatory ''need to know'' that Customer's Customer-ID in order to search the transactional CAT Data.[296]

The Commission preliminarily believes these proposed amendments are appropriate because they describe the specific circumstances under which Regulatory Staff may use Manual CAIS Access. In accordance with the proposed amendments, if Regulatory Staff have already identified a Customer of regulatory interest, Manual CAIS Access may be used. If a Customer of regulatory interest has been identified, Regulatory Staff could access CAIS manually to seek additional information about that identified Customer. CAIS would contain Customer and Account Attributes and other identifiers associated with a Customer (*e.g.,* Customer-ID and Industry Member Firm Designated ID).

Consistent with this approach, the proposed amendments permit wildcard searches based on multiple spellings of the known Customer's name (*e.g.,* Jone or Jones) or multiple spellings of a street associated with a known Customer's name (*e.g.,* the name ''Sally Jones'' could be searched with ''Fis?her Street'' to identify individuals with that name that live on either ''Fisher'' or ''Fischer'' Street). However, open-ended searching of parameters that are not specific to an identified Customer would be prohibited. Similarly, Regulatory Staff without additional Customer identifying information would not be permitted to search for all people sharing a common zip code, birth year or street. The Commission preliminarily believes this proposed provision is appropriate

[289] *See* proposed Section 1.1.

[290] *See* proposed Appendix D, Section 4.1.6 (Customer Identifying Systems Workflow).

[291] *See id.*

[292] *See id.*

[293] *See id.*

[294] *See id.* ''Performance requirements'' refers to the response times Online Targeted Queries. *See* CAT NMS Plan, *supra* note 3, Appendix D Section 8.1.2. Pursuant to Appendix D, Section 8.1.2, the performance requirement for Manual CAIS Access must generally be in increments of less than one minute. *Id.*

[295] *See* Part II.G.2., *infra* for a discussion of policies and procedures relating to access to and use of CAT Data.

[296] Manual CAIS Access is distinct from Programmatic CAIS Access and Programmatic CCID Subsystem Access, as discussed *infra* Part II.F.6 (Programmatic CAIS Access) and Part II.F.7 (Programmatic CCID Subsystem Access).

because it extends the principle that Regulatory Staff must already have identified a Customer of regulatory interest pursuant to regulatory efforts before Manual CAIS Access will be permitted.

The Commission also preliminarily believes that the proposed amendments requiring that Manual CAIS Access be provided by the Plan Processor via the CAIS/CCID Subsystem Regulator Portal are appropriate because they set forth access and use restrictions, while at the same time facilitating regulatory use. Specifically, the proposed requirement specifies how such manual access must be implemented (*i.e.,* through the CAIS/CCID Subsystem Regulatory Portal) by the Plan Processor for access by Regulatory Staff. The CAIS/CCID Subsystem Regulator Portal must facilitate query parameters based on data elements in Customer and Account Attributes and other identifiers available in the transaction database (*e.g.,* Customer-ID(s) or Industry Member Firm Designated ID(s)).[297]

Finally, the Commission preliminarily believes that it is appropriate to amend the CAT NMS Plan to adopt performance requirements for Manual CAIS Access so that there is a baseline performance metric to assess the operation of Manual CAIS Access, and to facilitate the return of query results within a timeframe that facilitates the usefulness of the data obtained by Regulatory Staff from CAIS. Further, the Commission also believes that it is appropriate to base the Manual CAIS Access performance requirements on the Online Targeted Query Tool Performance Requirements because the Online Targeted Query Tool enables Regulatory Staff to retrieve transactional CAT Data using an on-line query screen and includes the ability to choose from a variety of pre-defined selection criteria, which is similar in operation to Manual CAIS Access.

The Commission requests comment on the proposed amendments to define Manual CAIS Access and the requirements for using Manual CAIS Access. Specifically, the Commission solicits comment on the following:

104. The proposed amendments require Manual CAIS Access to be used if Regulatory Staff, having identified Customers of regulatory interest through regulatory efforts, require additional information from the CAT regarding such Customers. Are the circumstances in which Manual CAIS Access will be used clearly defined? If not, what additional detail would be helpful? Are there any other circumstances in which Manual CAIS Access might be appropriate? Please be specific in your response.

105. The proposed amendments establish that additional information about Customers may be accessed through Manual CAIS Access by (1) using identifiers available in the transaction database to identify Customer and Account Attributes associated with the Customer-IDs or industry member Firm Designated IDs, as applicable; or (2) using Customer Attributes in CAIS to identify Customer-IDs or industry member Firm Designated IDs, as applicable, associated with the Customer Attributes, in order to search the transaction database. Should requirements be added in relation to accessing additional information about Customers through Manual CAIS Access, *e.g.,* limiting the number of records that may be accessed? What limitation would be appropriate? Please be specific and describe the impact that any limitation on record numbers would have on regulatory value.

106. The proposed amendments prohibit open-ended searching of parameters not specific to Customers in Manual CAIS Access. Is it clear to Commenters what an open-ended search is? Please explain what commenters understand the term to mean. Should open-ended searches be limited by other conditions in addition to the condition that it be specific to a Customer? Please be specific in your response and explain why any change to the proposed prohibition on open-ended searching would be appropriate.

107. The proposed amendments require Manual CAIS Access to provide Regulatory Staff with the ability to retrieve data in CAIS via the CAIS/CCID Subsystem Regulator Portal. Is the CAIS/CCID Subsystem Regulator Portal an appropriate mechanism by which to require Regulatory Staff to retrieve data in CAIS? Are there any other appropriate means of providing Manual CAIS Access? If so, please explain how those other means would operate and be implemented.

108. The proposed amendments require query parameters for Manual CAIS Access to be based on data elements including Customer and Account Attributes and other identifiers available in the transaction database (*e.g.,* Customer-IDs or Firm Designated IDs). Should the query parameters for Manual CAIS Access be based on these data elements? If not, why not? Are there other query parameters that are more appropriate? If so, why? Please be specific in your response.

109. The proposed amendments require the Performance Requirements for Manual CAIS Access to be consistent with the criteria set out in Appendix D, Functionality of the CAT System, Online Targeted Query Tool Performance Requirements. Is there another more appropriate performance requirement in the CAT NMS Plan that should apply to Manual CAIS Access? Why would alternative performance requirements more appropriate? Please be specific in your response.

5. Manual CCID Subsystem Access

The Commission also proposes to amend the CAT NMS Plan to include requirements for manual access to the CCID Subsystem. ''Manual CCID Subsystem Access'' would be defined to mean ''when used in connection with the Customer Identifying Systems Workflow, as defined in Appendix D, shall mean the Plan Processor functionality to manually query the CCID Subsystem, in accordance with Appendix D, Data Security, and the Participants' policies as set forth in Section 6.5(g).'' [298] In addition, the Commission proposes to amend the CAT NMS Plan to state that if Regulatory Staff have the ITIN(s)/SSN(s)/EIN(s) of a Customer(s) of regulatory interest identified through regulatory efforts outside of the CAT and now require additional information from the CAT regarding such Customer(s), then they may use Manual CCID Subsystem Access.[299] The proposed amendments also state that Manual CCID Subsystem Access must allow Regulatory staff to convert ITIN(s)/SSN(s)/EIN(s) into Customer-ID(s) using the CCID Subsystem, and that Manual CCID Subsystem Access will be limited to 50 ITIN(s)/SSN(s)/EIN(s) per query.[300] The Commission also proposes to amend the CAT NMS Plan to state that Manual CCID Subsystem Access must allow Regulatory Staff to retrieve data from the CCID Subsystem via the CAIS/CCID Subsystem Regulator Portal based on ITIN(s)/SSN(s)/EIN(s) [301] where the CCID Transformation Logic is embedded in the client-side code of the CAIS/CCID Regulator Portal.[302] The Commission also proposes to require that the performance requirements for the conversion of ITIN(s)/SSN(s)/EIN(s) to Customer-ID(s) shall be consistent with the criteria set out in Appendix D,

[297] *See supra* Part II.E.1; *see also* proposed Appendix D, Section 4.1.6 (Manual CAIS Access).

[298] *See* proposed Section 1.1.

[299] *See* proposed Appendix D, Section 4.1.6 (Manual CCID Subsystem Access).

[300] *See id.*

[301] *Id.*

[302] *See* proposed Appendix D, Section 4.1.6 (Manual CCID Subsystem Access).

Functionality of the CAT System, Online Targeted Query Tool Performance Requirements.[303]

The Commission preliminarily believes the proposed amendments to adopt Manual CCID Subsystem Access are appropriate because such access would provide a way for Regulatory Staff that have the ITIN(s)/SSN(s)/EIN(s) of a natural person or legal entity Customer as a result of regulatory efforts outside of the CAT (*e.g.,* from regulatory data, a tip, complaint, referral, or from other data in the possession of Regulatory Staff) to transform such ITIN(s)/SSN(s)/EIN(s) into Customer-ID(s) and subsequently obtain other information identifying a Customer that is associated with the Customer-ID, if that is in furtherance of a regulatory purpose. The Commission also preliminarily believes that limiting Manual CCID Subsystem Access to the submission of 50 SSN(s)/ITIN(s)/EIN(s) per query is appropriate because in the Commission's experience, 50 SSN(s)/ITIN(s)/EIN(s) is sufficient to accommodate the needs of most regulatory examinations or investigations involving SSN(s)/ITIN(s)/EIN(s).

The Commission also preliminarily believes that it is appropriate to specify, as the proposed amendments would, that Manual CCID Subsystem access must be enabled through the CAIS/CCID Subsystem Regulatory Portal, and that Transformation Logic must be embedded in the client-side code of the CAIS/CCID Subsystem Regulator Portal. By embedding the Transformation Logic in the client-side code of the CAIS/CCID Subsystem Regulator Portal, the proposed amendments would help to prevent the ITIN/SSIN/EIN of a Customer from entering any component of the CAT System.

Finally, the Commission is amending the CAT NMS Plan to adopt performance requirements for Manual CCID Subsystem Access so that there is a baseline performance metric to assess the operation of Manual CCID Subsystem Access, and to facilitate the return of query results within a timeframe that facilitates the usefulness of the data obtained by Regulatory Staff from the CCID Subsystem.[304] The Manual CCID Subsystem Access performance requirements are based on the Online Targeted Query Tool Performance Requirements because the Online Targeted Query Tool, which provides Regulatory Staff with the ability to retrieve transactional CAT Data using an on-line query screen and includes the ability to choose from a variety of pre-defined selection criteria, is most similar in operation to Manual CCID Subsystem Access. In addition, the Commission believes that the query performance requirement for the Online Targeted Query Tool is a reasonable performance requirement for Manual CCID Subsystem Access because that the Online Targeted Query Tool performance requirement of a one minute query response time is drawn from targeted queries that return less than 1 million rows of data based on a dataset covering less than a day for a single CAT Reporter whereas the Manual CCID Subsystem Access is transforming no more than 50 ITIN(s)/SSN(s)/EIN(s) per query.

The Commission requests comment on the proposed amendments to define Manual CCID Subsystem Access and the requirements for using Manual CCID Subsystem Access. Specifically, the Commission solicits comment on the following:

110. The proposed amendments require that Manual CCID Subsystem Access will be used when Regulatory Staff have the ITIN(s)/SSN(s)/EIN(s) of a Customer(s) of regulatory interest obtained through regulatory efforts outside of CAT and now require additional information from CAT regarding such Customer(s). Are the circumstances in which Manual CCID Subsystem Access will be used clearly defined? If not, what additional detail would be helpful? Are there any other circumstances in which Manual CCID Subsystem Access might be appropriate? Please be specific in your response.

111. The proposed amendments require that Manual CCID Subsystem Access will be limited to 50 ITIN(s)/SSN(s)/EIN(s) per query. Is this limitation appropriate? If not, what number limitation would be appropriate and why? Please be specific in your response and please explain how a different threshold would not compromise the security of the CCID Transformation Logic algorithm.

112. The proposed amendments require that Manual CCID Subsystem Access must provide Regulatory Staff with the ability to retrieve data from the CCID Subsystem via the CAIS/CCID Subsystem Regulator Portal with the ability to query based on ITIN(s)/SSN(s)/EIN(s) where the CCID Transformation Logic is embedded in the client-side code of the CAIS/CCID Subsystem Regulator Portal. Are there any other appropriate means of providing Manual CCID Subsystem Access that also would not require ITIN(s)/SSN(s) being reported to CAT? Please be specific in your response.

113. For Manual CCID Subsystem Access, should the CCID Transformation Logic be embedded in the client-side code of the CAIS/CCID Subsystem Regulator Portal? If not, where should it be embedded and how would that prevent the reporting and collection of ITIN(s)/SSN(s) to CAT?

114. Is it appropriate to require that the performance requirements for Manual CCID Subsystem Access be consistent with the criteria set out in the Online Targeted Query Tool Performance Requirements set out in Appendix D, Functionality of the CAT System? Is there another more appropriate performance requirement in the CAT NMS Plan that should apply to Manual CCID Subsystem Access? Why is that alternative performance requirement more appropriate? Please be specific in your response.

6. Programmatic Access—Authorization for Programmatic CAIS Access and Programmatic CCID Subsystem

While the Commission believes that manual access to both CAIS and the CCID Subsystem will satisfy the vast majority of Participant use cases, the Commission preliminarily believes that certain regulatory inquiries based on the investigation of potential rule violations and surveillance patterns depend on more complex queries of Customer and Account Attributes and transactional CAT Data. Such inquiries could involve regulatory investigations of trading abuses and other practices proscribed by Rule 10b–5 under the Exchange Act,[305] Section 17(a) of the Securities Act,[306] Rule 30(a) of Regulation SP [307] and Rule 201 of Regulation S–ID,[308] and Sections 206 and 207 of the Advisers Act.[309] Detecting and investigating trading based on hacked information in violation of Rule 10b–5 and Section 17(a) of the Exchange Act, for example, will often require the inclusion of transactional and customer criteria in misconduct detection queries with transactional and customer attributes in query result sets. With CAT Data, determining the scope and nature of hacking and associated trading misconduct could depend on tailored programmatic access to transactional CAT Data and information identifying a Customer collected in the CAT. Similar forms of complex queries and query result sets also will facilitate detection

[303] *See id.*

[304] *See supra* note 294.

[305] 17 CFR 240.10b–5.

[306] 15 U.S.C.77q.

[307] 17 CFR 248.30(a).

[308] 17 CFR 248.201.

[309] 15 U.S.C.80b–6; 15 U.S.C.80b–7.

and investigation of insider trading, including identifying potential illegal tippers. Complex query result sets that include transactional data and customer attributes also can advance regulatory investigations of unfair trade allocation practices (''cherry-picking''). In order to address these needs, the Commission preliminary believes it is appropriate to require the Plan Processor to provide programmatic access to the Customer Identifying Systems, as further described below.

In order to enable Regulatory Staff to carry out the regulatory responsibilities to enforce the statutes and rules noted above, among others, and to be consistent with and extend the ''least privileged'' practice of limiting access to Customer and Account Attributes, the Commission preliminarily believes it is appropriate to limit use of programmatic access to CAIS and the CCID Subsystem only to those Participants that receive Commission approval for programmatic access to those systems. Accordingly, the Commission is proposing to amend Appendix D, Section 4.1.6 of the CAT NMS Plan to require a Participant to submit an application, approved by the Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation) to the Commission for authorization to use Programmatic CAIS Access or Programmatic CCID Subsystem Access if a Participant requires programmatic access.[310]

The application would seek three sets of information: (1) Identification of the system for which programmatic access is being requested (*i.e.,* Programmatic CAIS Access and/or Programmatic CCID Subsystem Access); (2) discussion of the need for programmatic access; and (3) specifics on the regulatory purpose and systems that require programmatic access, including: (a) The Participant's rules that require programmatic access for surveillance and regulatory purposes; (b) the regulatory purpose of the inquiry or set of inquires requiring programmatic access; [311] (c) a detailed description of the functionality of the Participant's system(s) that will use data from CAIS or the CCID Subsystem; (d) a system diagram and description indicating architecture and access controls to the Participant's system that will use data from CAIS or the CCID Subsystem; and (e) the expected number of users of the Participant's system that will use data from CAIS or the CCID Subsystem.

The Commission also proposes amendments that would provide the process for Commission consideration of the application for Programmatic CAIS Access or Programmatic CCID Subsystem Access. Specifically, the Commission proposes that SEC staff shall review the application and may request supplemental information to complete the review prior to Commission action.[312] Once the application is completed, the proposed amendments would provide that the Commission shall approve Programmatic CAIS Access or Programmatic CCID Subsystem Access if it finds that such access is generally consistent with one or more of the following standards: That such access is designed to prevent fraudulent and manipulative acts and practices; to promote just and equitable principles of trade; to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in, securities; to remove impediments to and perfect the mechanism of a free and open market and a national market system; and, in general, to protect investors and the public interest.[313] The proposed amendments further would provide that the Commission shall issue an order approving or disapproving a Participant's application for Programmatic CAIS Access or Programmatic CCID Subsystem Access within 45 days of receipt of a Participant's application, which can be extended for an additional 45 days if the Commission determines that such longer period of time is appropriate and provides the Participant the reasons for such determination.[314]

The Commission preliminarily believes that each requirement proposed for the application would elicit the essential information that the Commission needs in order to assess whether to grant programmatic access to CAIS or the CCID Subsystem, as further discussed below. As such, the application requirements are designed to require each Participant that applies for programmatic access to provide detailed and thorough information that is tailored to explain why programmatic access is required by such Participant in order to achieve that Participant's unique regulatory and surveillance purposes, and why such access to transactional CAT Data and Customer and Account Attributes will be responsive to a Participant's inquiry or set of inquiries. These requirements are designed to set a high bar for granting an application for programmatic access so that such access is only granted when there is a demonstrated need and ability to use such access responsibly.

The Commission preliminarily believes that approval of the application process by the Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation) is appropriate because the Participant's Chief Regulatory Officer has the best understanding of how programmatic access to CAIS or the CCID Subsystem fits into the overall regulatory program and surveillance needs of the Participant. Approval by the Chief Regulatory Officer also would help to ensure that the need for programmatic access is assessed without any undue business pressures or concerns.[315]

Because there are two systems that contain information identifying Customers, the Commission also preliminarily believes that it is appropriate to require the Participant to indicate whether it is seeking Programmatic CAIS Access and/or Programmatic CCID Subsystem Access. Such identification would also enable the Commission to assess whether the type of access being requested by the Participant is consistent with the regulatory purpose of the inquiry or set of inquiries being pursued by the Participant's Regulatory Staff. The Commission preliminarily believes that given the different functionality of the two systems, separate applications and demonstrations of need and the ability to secure the data are required.

As previously discussed, the CAT NMS Plan adheres to the ''least privileged'' practice of limiting access to Customer Identifying Systems as much as possible. Therefore, the Commission believes that it is appropriate to require the Participant's application for programmatic access to indicate why manual access to CAIS and the CCID Subsystem cannot achieve the regulatory purpose of an inquiry or set of inquiries being pursued by Regulatory Staff before permitting programmatic access to CAIS and the CCID Subsystem. Requiring this information also would help the Participant's Chief Regulatory Officer (or similarly designated head(s) of

[310] *See* proposed Appendix D, Section 4.1.6.

[311] *Id.* While the application addresses the inquiries or set of inquiries that will be performed using programmatic access, the Customer Identifying Systems Workflow applies at the query level. Each query must be designed such that query results would contain only the Customer and Account Attributes that Regulatory Staff reasonably believes will achieve the regulatory purpose of the inquiry or set of inquiries.

[312] *Id.*

[313] *Id.*

[314] *Id.*

[315] Importantly, the Chief Regulatory Office is subject to oversight by the Regulatory Oversight Committee, which provides a governance structure for the Chief Regulatory Officer.

regulation) to conduct a fulsome analysis of his or her Regulatory Staff's need for programmatic access. The Commission preliminarily believes manual access will be sufficient in many cases and that need for programmatic access must be justified based on current and intended practices.

The Commission also preliminarily believes that it is appropriate to require the Participant's application to identify the Participant's specific rules that necessitate Programmatic Access for surveillance and regulatory purposes. For example, programmatic access to CAIS might be reasonable if the investigation into the potential violation of such rule would require knowledge of Customer and Account Attributes and transactional CAT Data to identify misconduct. The Participants should be specific in their justification for Programmatic Access; generally stating that programmatic access is required for member regulation, for example, would not be sufficient to justify Programmatic Access. The Participants must identify the nature of the specific rules or surveillance patterns that they believe require programmatic access. The Commission preliminarily believes that many forms of misconduct can be addressed using manual access and that programmatic access will not be necessary.

After considering the specific rule(s) that the Participant represents necessitates programmatic access, the Commission preliminarily believes that the next logical step in the assessment of whether programmatic access should be granted is to consider the regulatory purpose of the inquiry or set of inquires being conducted by Regulatory Staff; if a regulatory purpose for the inquiry or set of inquiries cannot be articulated, programmatic access cannot be justified. Therefore, the Commission preliminarily believes that a clear statement by a Participant that explicitly articulates the reasons that access should be granted and for what purposes, in light of the Participant's rule(s) that required programmatic access, is appropriate. If SEC staff believes that sufficient detail is lacking, staff may request additional information, as described below.

While all access and analysis of Customer and Account Attributes must occur within the SAW, the Commission must be assured that Customer and Account Attributes will be incorporated securely into the Participant's system before granting programmatic access. Therefore, the Commission also preliminarily believes that sufficient information about how a Participant intends to incorporate data from the Customer Identifying Systems into the Participant's system is needed in order to assess whether programmatic access should be granted. The Commission preliminarily believes that in addition to detailed description of functionality, requiring a system diagram and description indicating architecture and access controls at the Participant's system would provide a sufficient starting point to assess whether access should be granted; if needed, SEC staff would request additional information from the Participant. The Commission preliminarily believes that only Participants who demonstrate they have the surveillance and technical expertise to use programmatic access in a secure manner may be granted programmatic access.

While the Commission does not believe there is a number of users that is appropriate for all Participants and all regulatory inquiries, the number of users at a Participant that are performing inquiries can be relevant to data security concerns (*i.e.,* the ability to protect the data in the Customer Identifying Systems can be affected by the number of users with access to the data in the Customer Identifying Systems). Therefore, the Commission preliminarily believes that information about the expected number of users for the Participant's system that would use data from CAIS or the CCID Subsystem is an appropriate data point to solicit from the Participants.

The Commission also believes it is appropriate to amend the CAT NMS Plan to provide that SEC staff may request supplemental information to complete the review prior to Commission action. Given the scope of data that can be accessed from the Customer Identifying Systems under programmatic access, the Commission believes that it is vital to the approval process that the Participant clearly assess and articulate its need for programmatic access, and that the Commission receive and understand the Participant's need for programmatic access. The information solicited by the application process would help to ensure that programmatic access follows the ''least privileged'' practice of limiting access to Customer Identifying Systems as much as possible, is based on a ''need to know'' the data in the Customer Identifying Systems, and contains only the data from the Customer Identifying Systems that Regulatory Staff reasonably believes will achieve the regulatory purpose of the inquiry or set of inquiries; however, should SEC staff require additional information, the Commission believes that the CAT NMS Plan should allow SEC staff to request additional information about the programmatic application from the submitting Participant.[316]

As proposed, Programmatic CAIS Access and Programmatic CCID Subsystem Access would be used by certain approved Regulatory Staff in the Participant's SAW, subject to specific conditions, and focused on a defined regulatory purpose of an inquiry or set of inquiries. A Participant's application would be approved if it is generally consistent with one or more of the criteria. The Commission believes that this approval standard allows for flexibility and the ability to tailor access to specific regulatory needs.

The Commission also believes that requiring the Commission to issue an order approving or disapproving a Participant's application for programmatic access within 45 days is appropriate in order to facilitate a timely decision on the application. However, it is also appropriate to allow for an extension of time for Commission action if the Commission needs more time to consider whether the application is appropriate and provides its reasons for the extension to the Participant. Allowing extensions of time should help to facilitate a thorough review of the application by the Commission.

The Commission understands that a Participant's programmatic access may evolve over time. As such, the Commission believes that it is appropriate to require that policies be reasonably designed to implement and satisfy the Customer and Account Attributes data requirements of Section 4.1.6 of Appendix D, such that Participants must be able to demonstrate that a Participant's ongoing use of programmatic access adheres to the restrictions of the Customer Identifying Systems Workflow, as set forth in a Participant's Data Confidentiality Policies governing programmatic access, as required by Section 6.5(g)(i)(I) of the CAT NMS Plan, described below.[317] Such policies also are subject to an annual independent examination, which will help ensure ongoing effectiveness of a Participant's Data Confidentiality Policies as they relate to that Participant's programmatic

[316] Should a Participant receive approval for Programmatic Access, such Participant would not be precluded from incorporating in its analytical tools the ability to manually query CAIS and the CCID Subsystem.

[317] *See infra* Part II.G.3.c (Policies and Procedures Relating to Customer and Account Attributes).

access.[318] In addition and as described above, other proposed amendments to the Plan will also protect transactional CAT Data and Customer and Account Attributes accessed through programmatic access; notably, access would be within the SAW and governed by the CISP, the organization-wide and system-specific controls and related policies and procedures required by NIST SP 800–53 and applicable to all components of the CAT System. Such requirements will enable ongoing oversight of each approved Participant's programmatic access by the Plan Processor and the Commission, and will help limit programmatic access to appropriate use cases initially and on an ongoing basis.

The Commission requests comment on the proposed amendments to set forth the approval process for Programmatic CAIS and Programmatic CCID Subsystem Access. Specifically, the Commission solicits comment on the following:

115. The proposed amendments require that the Participant's application for programmatic access be approved by the Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation). Is the Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation) the appropriate person to approve the application? If not, why not? Is there another person or entity that should approve the Participant's application?

116. Is it appropriate for the application to require the Participant to indicate which programmatic access is being requested: Programmatic CAIS Access and/or Programmatic CCID Subsystem Access? Why or why not?

117. The proposed amendments require the Participant to detail in an application to the Commission why Programmatic CAIS Access or Programmatic CCID Subsystem is required, and why Manual CAIS Access or Manual CCID Subsystem Access cannot achieve the regulatory purpose of an inquiry or set of inquiries. Is this information sufficient to explain why programmatic access is required? Should Participants have to provide more than an explanation of why manual access cannot achieve the regulatory purpose or an inquiry or set of inquiries? What other information should be solicited? Please be specific in your response.

118. The proposed amendments require that the application explain the Participant's rules that require Programmatic Access for surveillance and regulatory purposes. Should any other aspect of the Participant rules to be explained in the application? If so, please explain.

119. The proposed amendments require that the application explain the regulatory purpose of the inquiry or set of inquiries requiring programmatic access. Is there additional detail that could be added to this standard? If so, what provisions could be added to clarify this standard? Please be specific in your response.

120. The proposed amendments require that an application to the Commission provide a detailed description of the functionality of the Participant's system(s) that will use data from CAIS or the CCID Subsystem. Is there anything in addition to the functionality of the Participant's system(s) that will use the data from CAIS and the CCID Subsystem that should be provided by the Participant? Please provide detail about why this additional information is necessary and how it would be appropriate for the Commission to consider in its assessment of whether to provide programmatic access to the Participant.

121. The proposed amendments require that the application provide a system diagram and description indicating architecture and access controls to the Participant's system that will use data from CAIS or the CCID Subsystem. Is there any other information regarding the Participant's system and the architecture and access controls that should be provided? Please describe that additional information in detail and explain how this will be useful in the Commission's assessment of whether to provide programmatic access to the Participant.

122. The proposed amendments require the application to indicate the expected number of users of the Participant's system that will use data from CAIS or the CCID Subsystem. Is there any other information about users in the Participants' system that will use the data that should be required? Please be specific and explain why it would be appropriate to add such a requirement.

123. The proposed amendments provide that the Commission shall approve Programmatic CAIS Access or Programmatic CCID Subsystem Access if it finds that such access is generally consistent with one or more of the following standards: That such access is designed to prevent fraudulent and manipulative acts and practices; to promote just and equitable principles of trade; to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in, securities; to remove impediments to and perfect the mechanism of a free and open market and a national market system; and, in general, to protect investors and the public interest. Are there other standards that should be used by the Commission to assess whether to grant a Participant's application for Programmatic CAIS Access or Programmatic CCID Subsystem Access? Please be specific and explain why such other standards would be more appropriate.

124. Under the proposed amendments, the Commission shall issue an order approving or disapproving a Participant's application for programmatic access within 45 days, which can be extended by the Commission for an additional 45 days, if the Commission determines that such longer period of time is appropriate and provides the Participant with the reasons for such determination. Do commenters believes that 45 days is an appropriate amount of time for Commission action? Is another time period for Commission action more appropriate? Is another time period for the extension of time for Commission action more appropriate? If so, what time would that be? Please be specific and explain why a different time period would be more appropriate.

125. Once Commission approval of an application is granted, an approved Participant would be permitted to use programmatic access subject to the ongoing restrictions identified in Appendix D, Section 4.1.6 and Article VI, Section 6.5(g), as well as those related to use of a SAW; however, the proposed amendments would not require an approved Participant to submit updated applications as its use of programmatic access evolves. Should updates to application materials be required in order for Participants to maintain their programmatic access, or should Participants have to re-apply to maintain their programmatic access? Or is it sufficient that the policies and procedures in Section 6.5(g)(i) require the Participants to establish, maintain and enforce their policies and procedures? If Participants were required to re-apply to maintain their programmatic access, what criteria should be used for requiring re-application? For example, should approval for programmatic access expire after a set amount of time, so that Participants would have to re-apply at regular intervals in order to maintain their programmatic access? If so, what time period would be reasonable? For example, should Participants be required to re-apply every two years to maintain their programmatic access?

[318] *See infra* Part II.G.4.

Alternatively, should Participants be required to re-apply for programmatic access only if there is a material change in their use of programmatic access?

7. Programmatic CAIS Access

The Commission believes that it is appropriate to set forth the circumstances and requirements for Programmatic CAIS Access. The proposed amendments will define Programmatic Access, when used in connection with the Customer Identifying Systems Workflow, to mean the Plan Processor functionality to programmatically query, and return results that include, data from the CAIS and transactional CAT Data, in support of the regulatory purpose of an inquiry or set of inquiries, in accordance with Appendix D, Data Security, and the Participants' policies as set forth in Section 6.5(g).[319] The Commission proposes to amend the CAT NMS Plan to state that Programmatic CAIS Access may be used when the regulatory purpose of the inquiry or set of inquiries by Regulatory Staff requires the use of Customer and Account Attributes and other identifiers (*e.g.,* Customer-ID(s) or Industry Member Firm Designated ID(s)) to query Customer and Account Attributes and transactional CAT Data.[320] In addition, the Commission proposes to require that the Plan Processor provide Programmatic CAIS Access by developing and supporting an API that allows Regulatory Staff to use analytical tools and ODBC/JDBC drivers to access the data in CAIS, and that the Performance Requirements for Programmatic CAIS Access shall be consistent with the criteria set out in Appendix D, Functionality of the CAT System, User-Defined Direct Query Performance Requirements.[321]

The Commission preliminarily believes that these proposed amendments are appropriate because they set forth the parameters for Programmatic CAIS access, which would permit a programmatic interface that facilitates the submission of complex queries for both the transactional CAT Database and the Customer Identifying Systems. For example, if the regulatory purpose of an inquiry or set of inquiries being pursued by Regulatory Staff involved insider trading before a company news release, Programmatic CAIS Access could be an appropriate method for accessing CAIS because Regulatory Staff could search the transactional CAT Database for consistently profitable trading activity and filter the data using the parameters of name and zip code—part of Customer and Account Attributes—to find Customer-IDs or other information identifying Customers that might be responsive to the inquiry or set of inquiries.

As discussed above, Programmatic CAIS Access must be within the SAW, adhere to the ''least privileged'' practice of limiting access to Customer Identifying Systems as much as possible, is based on a ''need to know'' the data in the Customer Identifying Systems, and must contain only the data from the Customer Identifying Systems that Regulatory Staff reasonably believes will achieve the regulatory purpose of the inquiry or set of inquiries. In addition, as required by Article VI, Section 6.5(g)(i)(I), the policies of the Participants must be reasonably designed to implement and satisfy the Customer and Account Attributes data requirements of Section 4.1.6 of Appendix D such that Participants must be able to demonstrate that a Participant's ongoing use of Programmatic CAIS and/or CCID Subsystem access is in accordance with the Customer Identifying Systems Workflow, which will enable an ongoing analysis of whether Programmatic CAIS Access is being used by an approved Participant appropriately.[322] Therefore, the Commission believes that these are appropriate limitations on Programmatic CAIS Access.

Finally, the Commission preliminarily believes that it is appropriate to amend the CAT NMS Plan to adopt performance requirements for Programmatic CAIS Access so that there is a baseline performance metric to assess the operation of such access, and to facilitate the return of query results within a timeframe that facilitates the usefulness of the data obtained by Regulatory Staff from CAIS. The Commission also believes that it is appropriate to base the Programmatic CAIS Access performance requirements on the User-Defined Direct Query Performance Requirements because User-Defined Direct Queries are the most similar to Programmatic CAIS Access and thus would provide Regulatory Staff with programmatic interfaces that would enable and support, for example, complex queries, including the ability to provide query results that are extractable/downloadable, multistage queries; and concurrent queries.

The Commission requests comment on the proposed amendments to define and set forth the requirements for Programmatic CAIS Access. Specifically, the Commission solicits comment on the following:

126. The proposed amendments establish that Programmatic CAIS Access may be used when the regulatory purpose of the inquiry or set of inquiries by Regulatory Staff requires the use of Customer and Account Attributes and other identifiers (*e.g.,* Customer-ID(s) or Firm Designated ID(s)) to query the Customer and Account Attributes and transactional CAT Data. Are the circumstances in which Programmatic CAIS Access may be used clearly defined? If not, what additional detail would be helpful? Are there any other circumstances in which Programmatic CAIS Access might be appropriate? Please be specific in your response.

127. The proposed amendments require the Plan Processor to provide Programmatic CAIS Access by developing and supporting an API that allows Regulatory Staff to use analytical tools and ODBC/JDBC drivers to access the data in CAIS. Is there another more appropriate method to allow Regulatory Staff to access the data in CAIS? Please be specific in your response.

128. The proposed amendments require that the performance requirements for Programmatic CAIS Access be consistent with the criteria in the User-Defined Direct Query Performance Requirements set out in Appendix D, Functionality of the CAT System. Is there another more appropriate performance requirement in the CAT NMS Plan that should apply to Programmatic CAIS Access? Why is that alternative performance requirement more appropriate? Please be specific in your response.

8. Programmatic CCID Subsystem Access

The Commission believes that it is appropriate to amend the CAT NMS Plan to set forth the circumstances and requirements for Programmatic CCID Subsystem Access. The proposed amendments would define CCID Subsystem Access when used in connection with the Customer Identifying Systems Workflow, to mean the Plan Processor functionality to programmatically query the CCID Subsystem to obtain Customer-ID(s) from Transformed Value(s), in support of the regulatory purpose of an inquiry or set of inquiries, in accordance with Appendix D, Data Security, and the Participants' policies as set forth in

[319] *See* CAT NMS Plan, Section 6.5(g)(1).

[320] *See* proposed Appendix D, Section 4.1.6 (Programmatic CAIS Access).

[321] *See id.*

[322] *See* Part II.G.3.c, *infra,* for a discussion of the policies relating to Customer and Account Attributes.

Section 6.5(g).[323] The Commission proposes to amend the CAT NMS Plan to state that Programmatic CCID Subsystem Access allows Regulatory Staff to submit multiple ITIN(s)/SSN(s)/EIN(s) [324] for a Customer(s) of regulatory interest identified through regulatory efforts outside of the CAT to obtain Customer-ID(s) in order to query CAT Data regarding such Customer(s).[325] The Commission also proposes to amend the CAT NMS Plan to explicitly state that the Plan Processor must provide Programmatic CCID Subsystem Access by developing and supporting the CCID Transformation Logic and an API to facilitate the submission of Transformed Values to the CCID Subsystem for the generation of Customer-ID(s).[326] The proposed amendments would also state that Performance Requirements for the conversion of ITIN(s)/SSN(s)/EIN(s) to Customer-ID(s) shall be consistent with the criteria set out in Appendix D, Functionality of the CAT System, User-Defined Direct Query Performance Requirements.[327]

The 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 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). In addition, as required by Article VI, Section 6.5(g)(i)(I), the policies of the Participants must be reasonably designed to implement and satisfy the Customer and Account Attributes data requirements of Section 4.1.6 of Appendix D such that Participants must be able to demonstrate that a Participant's ongoing use of Programmatic CAIS and/or CCID Subsystem access is in accordance with the Customer Identifying Systems Workflow, which will enable an ongoing analysis of whether Programmatic CCID Subsystem Access is being used by an approved Participant appropriately. Finally, the Commission believes that it is appropriate to amend the CAT NMS Plan to adopt the performance requirements applicable to User-Defined Direct queries because such queries provide Regulatory Staff with programmatic interfaces to enable complex queries in a manner most similar to Programmatic CCID Subsystem Access.

The Commission requests comment on the proposed amendments to define and set forth the requirements for Programmatic CCID Subsystem Access. Specifically, the Commission solicits comment on the following:

129. The proposed amendments require the Plan Processor to provide Programmatic CCID Subsystem Access by developing and supporting the CCID Transformation Logic and an API to facilitate the submission of Transformed Values to the CCID Subsystem for the generation of Customer-ID(s). Is there another more appropriate method to facilitate the development and support for the Programmatic CCID Subsystem Access? Please be specific in your response.

130. The proposed amendments require Programmatic CCID Subsystem access to allow Regulatory Staff to submit multiple ITIN(s)/SSN(s)/EIN(s) of a Customer(s) of regulatory interest identified through regulatory efforts outside of CAT to obtain Customer-ID(s) in order to query CAT Data regarding such Customer(s). Is this an appropriate way to facilitate Regulatory Staff obtaining Customer-IDs in order to query CAT Data? If not, is there another more appropriate way to facilitate obtaining Customer-IDs for Regulatory Staff?

131. The proposed amendments that require the performance requirements for Programmatic CCID Subsystem Access be consistent with the criteria in the User-Defined Direct Query Performance Requirements set out in Appendix D, Functionality of the CAT System. Is there another more appropriate performance requirement in the CAT NMS Plan that should apply to Programmatic CCID Subsystem Access? Why would an alternative performance requirement more appropriate? Please be specific in your response.

G. Participants' Data Confidentiality Policies

1. Data Confidentiality Policies

When adopting Rule 613, the Commission recognized the importance of maintaining the confidentiality of all CAT Data reported to the Central Repository.[328] The Commission noted at the time that the purpose and efficacy of the CAT would be compromised if the Commission, the SROs, and their members could not rely on the integrity, confidentiality, and security of the information stored in the Central Repository, noting that the Central Repository would contain confidential and commercially valuable information.[329] Rule 613 required the CAT NMS Plan to include policies and procedures that are designed to ensure implementation of the privacy protections that are necessary to assure regulators and market participants that the CAT NMS Plan provides for rigorous protection of confidential information reported to the Central Repository.[330] Furthermore, Rule 613 required the Participants and their employees to agree to not use CAT Data for any purpose other than surveillance and regulatory purposes, provided that a Participant is permitted to use the data that it reports to the Central Repository for regulatory, surveillance, commercial, or other purposes as otherwise permitted by applicable law, rule or regulation.[331]

The CAT NMS Plan has several provisions designed to protect the confidentiality of CAT Data. Specifically, Section 6.5(f)(ii) of the CAT NMS Plan requires Participants to adopt and enforce policies and procedures that: (1) Implement ''effective information barriers'' between the Participant's regulatory and non-regulatory staff with regard to access and use of CAT Data stored in the Central Repository; (2) permit only persons designated by Participants to have access to the CAT Data stored in the Central Repository; and (3) impose penalties for staff non-compliance with any of its or the Plan Processor's policies or procedures with respect to information security. Section 6.5(f)(iii) of the CAT NMS Plan requires each Participant to, as promptly as reasonably practicable, and in any event

[323] *See* proposed Section 1.1.

[324] The CCID Subsystem will contain the functionality to facilitate the efficient and accurate conversion of multiple legal entity's EIN(s) into a Transformed Value(s) and a subsequent Customer-ID. However, because an EIN(s) will be reported to CAIS as a Customer Attribute for association with a Customer-ID, the need for Regulatory Staff to utilize the CCID Subsystem to convert multiple EIN(s) into a Transformed Value and a subsequent Customer-ID will be minimized.

[325] *See* proposed Appendix D, Section 4.1.6 (Programmatic CCID Subsystem Access).

[326] *See id.*

[327] *See id.*

[328] *See e.g.,* Rule 613 Adopting Release, *supra* note 2, at 45781–83.

[329] *See id.* at 45783.

[330] 17 CFR 242.613(e)(4)(i).

[331] 17 CFR 242.613(e)(4)(i)(A). In addition, the CAT NMS Plan specifies that usage of the CAT Data is provided to Participants solely for the purpose of performing their respective regulatory and oversight responsibilities pursuant to federal securities laws, rules and regulations or any contractual obligations. CAT NMS Plan Section 6.5(g). As noted in the CAT NMS Plan Approval Order, regulatory purposes include, among other things, analysis and reconstruction of market events, market analysis and research to inform policy decisions, market surveillance, examinations, investigations, and other enforcement functions. *See* CAT NMS Plan Approval Order, *supra* note 3, at 84724 note 586.

within 24 hours, report to the Chief Compliance Officer, in accordance with the guidance provided by the Operating Committee, any instance, of which such Participant becomes aware, of: (1) Noncompliance with the policies and procedures adopted by such Participant pursuant to Section 6.5(e)(ii); or (2) a breach of the security of the CAT. Section 6.5(g) requires the Participants to establish, maintain, and enforce written policies and procedures reasonably designed to: (1) Ensure the confidentiality of the CAT Data obtained from the Central Repository; and (2) limit the use of CAT Data obtained from the Central Repository solely for surveillance and regulatory purposes. The CAT NMS Plan further requires each Participant to periodically review the effectiveness of the policies and procedures required by Section 6.5(g), and to take prompt action to remedy deficiencies in such policies and procedures.[332]

The Commission believes that while the existing provisions discussed above are designed to protect the security and confidentiality of CAT Data, the CAT NMS Plan should be modified and supplemented to provide additional specificity concerning data usage and confidentiality policies and procedures, and to strengthen such policies and procedures with expanded and new requirements designed to protect the security and confidentiality of CAT Data.

First, the Commission proposes to combine the existing CAT NMS Plan provisions applicable to Participants discussed above, specifically Sections 6.5(f)(ii), (f)(iii) and (g), into a single section of the CAT NMS Plan.[333] The Commission also proposes to modify these provisions so that they would apply to the Proposed Confidentiality Policies and procedures and usage restriction controls [334] in accordance with these policies, as required by proposed Section 6.5(g)(i).[335] This single section, Section 6.5(g)(i), would set forth the provisions that must be included in each Participant's confidentiality and related policies (''Proposed Confidentiality Policies''). Provisions that are applicable to Participants would be contained in one place and separated from those applicable to the Plan Processor. As proposed, Section 6.5(f) of the CAT NMS Plan would continue to relate to data confidentiality and related policies and procedures of the Plan Processor, while Section 6.5(g) would relate to data confidentiality and related policies and procedures of the Participants.

Second, the Commission proposes to amend the CAT NMS Plan to require the Proposed Confidentiality Policies to be identical across Participants, which would result in shared policies that govern the usage of CAT Data by Participants and apply to all Participants equally. Currently, the CAT NMS Plan requires each individual Participant to establish, maintain, and enforce policies and procedures relating to the usage and confidentiality of CAT Data. The Commission preliminarily believes that having policies that vary across Participants could result in the creation of policies that differ substantively even for the same regulatory role. For example, pursuant to Section 6.5(f)(ii) of the CAT NMS Plan, a Participant could establish policies that grant broad access to CAT Data to regulatory staff that are assigned to a particular regulatory role, even if such broad access is not necessary for that regulatory role, while another Participant could more appropriately establish policies limiting access to CAT Data for the same regulatory role to CAT Data necessary to perform the role. The Commission preliminarily believes that to the extent SROs have regulatory staff with roles that serve a consistent purpose across SROs, that SROs generally should be accessing CAT Data pursuant to identical policies. The Commission further believes that requiring one identical set of policies would allow for input and expertise of all Participants to be used in the development of such policies, and should reasonably be expected to result in more comprehensive Proposed Confidentiality Policies that incorporate the full range of regulatory activities performed by the SROs and are designed in a manner that is consistent with how SROs operate in practice.[336] As proposed, while the Proposed Confidentiality Policies would be identical across Participants, the policies would incorporate different regulatory and surveillance roles and goals of the Participants and would apply to the whole scope of CAT Data usage by Participants, including use within a SAW, excepted non-SAW environment, or any other Participant environment.[337]

The Commission recognizes, though, that the internal organization structures, reporting lines, or other operations may differ across the Participants. Accordingly, the Commission preliminarily believes that it is appropriate to permit Participants to develop their own procedures relating to the Proposed Confidentiality Policies. In this regard, proposed Section 6.5(g)(i) would require each Participant to establish, maintain, and enforce procedures in accordance with the policies required by proposed Section 6.5(g)(i). The Commission also preliminarily believes that it is not necessary to subject such Participant procedures to the same requirements as those policies that are discussed below, including the requirements that such procedures are approved by the CAT Operating Committee and subject to annual examination and publication, because Participant procedures will differ based on individual Participants' organizational, technical, and structural uniqueness.[338]

2. Access to CAT Data and Information Barriers

As noted above, current Sections 6.5(f)(ii)(A) and (B) of the CAT NMS Plan require each Participant to adopt and enforce policies and procedures that implement effective information barriers between such Participant's

[332] *See* CAT NMS Plan, *supra* note 3, at Section 6.5(g).

[333] Specifically, the Commission proposes to move Sections 6.5(f)(ii)(A) and (C), to Sections 6.5(g)(i)(D) and (H) respectively, and Section 6.5(f)(iii) to Section 6.5(g)(iii). Section 6.5(f)(ii)(B) would be deleted and replaced by a new provision regarding access to CAT Data in proposed Section 6.5(g)(i)(C), as discussed below. *See infra* Part II.G.2.a. Due to the proposed deletions, paragraphs (f)(iv) and (f)(v) in Section 6.5 would be re-designated as (f)(ii) and (f)(iii).

[334] *See, infra,* Part II.G.3.a.

[335] Revising these provisions to cover the Proposed Confidentiality Policies would apply these existing safeguards to the identical Proposed Confidentiality Policies. For example, proposed Section 6.5(g)(iii) would be modified to reference the policies, procedures and usage restriction controls required by Section 6.5(g)(i) instead of Section 6.5(e)(ii). The Commission believes the provision is supposed to reference Section 6.5(f)(ii), because there is no Section 6.5(e)(ii) and because Participant policies and procedures are addressed in Section 6.5(f)(ii). In addition, the Commission proposes to revise the language of some of these provisions for clarity. Proposed Section 6.5(g)(iii) would thus require Participants to, as promptly as reasonably practicable, and in any event within 24 hours of becoming aware, report to the Chief Compliance Officer, in accordance with the guidance provided by the Operating Committee: (A) Any instance of noncompliance with the policies, procedures and usage restriction controls adopted by such Participant pursuant to Section 6.5(g)(i); or (B) a breach of the security of the CAT.

[336] The Commission understands that the Participants have established policies and procedures pursuant to Section 6.5(f)(ii), and preliminarily believes that Participants can use these existing policies and procedures in order to help prepare, review, and approve the policies and procedures required by proposed Section 6.5(g)(i). The Commission also understands Participants have policies and procedures outside of CAT, such as insider trading policies and non-public data policies, which could be used to help develop both the Proposed Confidentiality Policies and the related procedures.

[337] *See infra* Part II.G.2.

[338] *See infra* Part II.G.4.

regulatory and non-regulatory staff with regard to access and use of CAT Data stored in the Central Repository and permit only persons designated by Participants to have access to CAT Data stored in the Central Repository.[339]

a. Regulatory Staff and Access to CAT Data

Current Section 6.5(f)(ii)(A) and (B) do not impose specific restrictions or requirements for Participants in determining which staff are considered regulatory staff. The existing provisions also do not address whether there may be limited instances in which non-regulatory staff—particularly technical staff—may have legitimate reasons to access CAT Data for regulatory purposes. The Commission believes that providing specificity regarding which staff are considered regulatory staff in the current CAT NMS Plan, and thus may have access to CAT Data, and specific limitations on access to CAT Data by both regulatory and non-regulatory staff may help better protect CAT Data and result in it being accessed and used appropriately.

To address these issues, the Commission proposes to replace existing Section 6.5(f)(ii)(B)[340] with Section 6.5(g)(i)(C) to the CAT NMS Plan. Section 6.5(g)(i)(C) would limit access to CAT Data to persons designated by Participants, which persons must be: (1) Regulatory Staff; or (2) technology and operations staff that require access solely to facilitate access to and usage of CAT Data stored in the Central Repository by Regulatory Staff. In contrast to existing Section 6.5(f)(ii)(B), the proposed requirement in Section 6.5(g)(i)(C) would apply more broadly to CAT Data, rather than ''CAT Data stored in the Central Repository,'' and the Commission preliminarily believes that this expansion is appropriate because access to CAT Data should be limited to appropriate Participant personnel whether or not the data is being accessed directly from the Central Repository. The Commission further believes that deleting Section 6.5(f)(ii)(B) is appropriate because proposed Section 6.5(g)(i)(C) provides greater clarity and more specificity on which Participant staff are permitted to access CAT Data.

The Commission proposes to define ''Regulatory Staff,'' for the purposes of the Proposed Confidentiality Policies and the CAT NMS Plan. Specifically, ''Regulatory Staff'' would be defined in Section 1.1 of the CAT NMS Plan as the Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation) and staff within the Chief Regulatory Officer's (or similarly designated head(s) of regulation's) reporting line.[341] In addition, the proposed definition would require that Regulatory Staff be specifically identified and approved in writing by the Chief Regulatory Officer (or similarly designated head(s) of regulation). In addition to creating the definition, the Commission proposes to amend references throughout the CAT NMS Plan that refer to ''Participant regulatory staff'' or ''Participants' regulatory staff'' to ''Participants' Regulatory Staff,'' in Sections 6.5(b)(i) and 6.5(f)(iv)(B) and in Appendix D, Sections 6.1, 6.2, 8.1, 8.2.1, 8.3, 9.1, 10.2 and 10.3 of the CAT NMS Plan.[342]

The Commission preliminarily believes that the proposed definition of Regulatory Staff is reasonably designed to result in the identification of those with a legitimate regulatory role and such staff would be the only Participant staff that are generally provided access to CAT Data. The Commission preliminary believes considering a Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation) as Regulatory Staff is appropriate because generally that role with a Participant is regulatory in function and reports directly to a Participant's board of directors and/or a Participant's Regulatory Oversight Committee.[343] The Commission is including staff within the Chief Regulatory Officer's (or similarly designated head(s) of regulation's) reporting line because the Commission believes that such Participant staff will have a primarily regulatory function. By contrast, Participant staff with other reporting lines and who primarily perform other functions for Participants, such as commercial or business functions generally should not have access to CAT Data. The Commission further believes that requiring the Chief Regulatory Officer (or similarly designated head(s) of regulation) to identify and approve which personnel are considered Regulatory Staff should help prevent staff with primarily non-regulatory obligations from being categorized as Regulatory Staff. A Chief Regulatory Officer (or similarly designated head(s) of regulation) may determine that some Regulatory Staff should not have access to CAT Data. The Commission believes that this proposal would further clarify which Participant staff can access CAT Data outside of the CAT infrastructure. For example, in addition to the staff who are directly accessing CAT Data inside the CAT infrastructure, Participant regulatory staff assisting examination staff in analyzing data extracted by a Participant for a particular examination or participating in an enforcement matter would be accessing CAT Data and thus would need to be identified and approved for access to CAT Data.

Participants may have staff with the technical or operational expertise necessary to implement systems to access CAT Data within other departments or that otherwise fall outside of the proposed definition of Regulatory Staff. Limiting access solely to Regulatory Staff could make it difficult for Participants to adequately develop, monitor, test, improve, or fix technical and operational systems developed or designed to access, review, or analyze CAT Data. Accordingly, the Commission proposes to require that the Proposed Confidentiality Policies allow technology and operations staff access to CAT Data only insofar as it is necessary to facilitate access by Regulatory Staff. To better protect CAT Data however, the Commission believes that such staff should not be granted access to CAT Data as a matter of course, and further believes that such staff should be subject to affidavit and training requirements and other requirements applicable to regulatory users of CAT Data.

The Commission understands that with regard to CAT responsibilities, certain Participants may choose to enter into regulatory services agreements (''RSAs'') or allocate regulatory responsibilities pursuant to Rule 17d–2 (through ''17d–2 agreements'') to other Participants to operate their surveillance and regulatory functions, and in

[339] *See supra* Part II.G.1.

[340] Current Section 6.5(f)(ii)(B) of the CAT NMS Plan states that each Participant shall adopt and enforce policies and procedures that: ''Permit only persons designated by Participants to have access to the CAT Data stored in the Central Repository.'' The Commission believes that proposed Section 6.5(g)(i)(C) more clearly defines what Participant staff may have access to CAT Data.

[341] *See* proposed CAT NMS Plan Section 1.1.

[342] The term ''regulatory staff'' appears in other existing provisions of the CAT NMS Plan, and in particular Appendix C, and the Commission is not proposing to amend these references. The Commission is not changing references to ''regulatory staff'' which clearly refer to both Participant and Commission staff, in Section 6.10 of the CAT NMS Plan. In addition, the Commission is not amending the term in Appendix C because, as discussed in Part II.L below, Appendix C was not intended to be continually updated once the CAT NMS Plan was approved.

[343] The Commission is proposing to allow ''similarly designated head(s) of regulation'' to act as the Chief Regulatory Officer in the proposed definition because certain Participants do not have a ''Chief Regulatory Officer.'' With respect to FINRA, the Commission understands that it does not have a Chief Regulatory Officer and that it may have multiple Executive Vice Presidents that fit within for the definition.

particular cross-market regulation and surveillance.[344] Under an RSA an SRO contracts to perform certain regulatory functions on behalf of another SRO, but the outsourcing SRO maintains ultimate legal responsibility for the regulation of its members and market. In contrast, under a Commission approved plan for the allocation of regulatory responsibilities pursuant to Rule 17d–2, the SRO does not maintain ultimate legal responsibility.[345] The amendment would not prohibit the outsourcing SRO from permitting its Regulatory Staff to access CAT Data to carry out their regulatory responsibilities. In addition, 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.

The Commission further believes that restricting access to CAT Data as proposed above would not foreclose 17d–2 agreements and RSAs, but that the Proposed Confidentiality Policies, 17d–2 agreements and RSAs would address access to CAT Data in light of these agreements. For example, the Commission preliminarily believes that the role of the relevant SROs' Chief Regulatory Officers, and designation of employees who may access CAT Data, may depend on the nature of the arrangement between the SROs. However, the proposed amendment would not foreclose SROs from considering both the outsourcing SRO's and the counterparty SRO's Chief Regulatory Officer (or similarly designated head(s) of regulation) as a relevant Chief Regulatory Officer (or similarly designated head(s) of regulation) for purposes of proposed Sections 1.1 and 6.5(g)(i), and thus allowing each Chief Regulatory Officer (or similarly designated head(s) of regulation) to identify Regulatory Staff in a manner consistent with the Proposed Confidentiality Policies.

b. Information Barriers

Current Section 6.5(f)(ii)(A) of the CAT NMS Plan requires Participants to adopt and enforce policies and procedures that implement effective information barriers between such Participant's regulatory and non-regulatory staff with regard to access and use of CAT Data stored in the Central Repository. The Commission proposes to move this requirement to Section 6.5(g)(i)(D), and modify the provision to replace the references to ''regulatory and non-regulatory staff,'' with the new defined term to state ''Regulatory Staff and non-Regulatory Staff,'' and correct the grammar of the provision.

Because the CAT is intended to be a regulatory system, the Commission continues to believe that requiring effective information barriers between regulatory and non-regulatory Staff is appropriate. The Commission believes that proposed Section 6.5(g)(i)(D) improves upon existing Section 6.5(f)(ii) by requiring such information barriers to be implemented in the identical set of policies required by Section 6.5(g)(i), and because it more clearly defines between which types of staff effective information barriers must be established. Regulatory Staff, depending on their roles and regulatory responsibilities, will have access to transactional data and/or access to CAIS or CCID Subsystem data, and there should be effective information barriers that prevent disclosure of such data to non-Regulatory Staff. Effective information barriers would help restrict non-Regulatory Staff access to CAT Data to the limited circumstances in which such staff could access CAT Data, as described below.

c. Access by Non-Regulatory Staff

The Commission understands that there might be limited circumstances in which non-Regulatory Staff access to CAT data may be appropriate. Accordingly, the Commission proposes new Section 6.5(g)(i)(E), which would require that the Confidentiality Policies limit non-Regulatory Staff access to CAT Data to limited circumstances in which there is a specific regulatory need for such access and a Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation), or designee, provides written approval for each instance of access by non-Regulatory Staff.[346]

The Commission believes that it is appropriate to provide this specific exception to allow for access to CAT Data by non-Regulatory Staff where there is a specific regulatory need. The Commission preliminarily believes there could be circumstances that justify allowing non-Regulatory Staff to view limited CAT Data. For example, in the case of a market ''flash crash,'' Regulatory Staff may need to brief an exchange's Chief Executive Officer (who may not otherwise be considered Regulatory Staff) regarding the causes of such an event or share raw CAT Data about specific orders and trades. Another example in which non-Regulatory Staff access could be appropriate is if major market participant misconduct warrants a briefing to a Participant's board of directors because it presents a risk to the continued operation of an exchange. The Commission believes requiring approval and documentation of such approval by the Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation) should obligate the Chief Regulatory Officer (or similarly designated head(s) of regulation) to determine whether a specific regulatory need exists. As proposed, and described further below, such approval and the access of CAT Data by non-Regulatory Staff would be subject to an annual examination.[347]

d. Training and Affidavit Requirements

The CAT NMS Plan currently has provisions relating to training and affidavit requirements for individuals who access CAT Data, enforced by the Plan Processor. Section 6.1(m) of the CAT NMS Plan requires the Plan Processor to develop and, with the prior approval of the Operating Committee, implement a training program that addresses the security and confidentiality of all information accessible from the CAT, as well as the operational risks associated with accessing the Central Repository. The training program must be made available to all individuals who have access to the Central Repository on behalf of the Participants or the SEC, prior to such individuals being granted access to the Central Repository. Section 6.5(f)(i)(B) states that the Plan Processor shall require all individuals who have access to the Central Repository (including the respective employees and consultants of the Participants and the Plan Processor, but excluding employees and Commissioners of the SEC) to execute a personal ''Safeguard of Information Affidavit'' in a form approved by the Operating Committee

[344] *See* 15 U.S.C. 78q(d)(1) and 17 CFR 240.17d–2.

[345] See Section 17(d)(1) of the Act and Rule 17d–2 thereunder, 15 U.S.C. 78q(d)(1) and 17 CFR 240.17d–2. Section 17(d)(1) of the Act allows the Commission to relieve an SRO of certain responsibilities with respect to members of the SRO who are also members of another SRO. Specifically, Section 17(d)(1) allows the Commission to relieve an SRO of its responsibilities to: (i) Receive regulatory reports from such members; (ii) examine such members for compliance with the Act and rules and regulations thereunder, and the rules of the SRO; or (iii) carry out other specified regulatory responsibilities with respect to such members.

[346] The Commission notes that this would not apply to certain technology and operations staff pursuant to proposed Section 6.5(g)(i)(C) discussed above.

[347] *See infra* Part II.G.4.

providing for personal liability for misuse of data.[348]

The Commission proposes in new Section 6.5(g)(i)(F) that the Proposed Confidentiality Policies require all Participant staff who are provided access to CAT Data to: (1) Sign a ''Safeguard of Information'' affidavit as approved by the Operating Committee pursuant to Section 6.5(f)(i)(B); and (2) participate in the training program developed by the Plan Processor that addresses the security and confidentiality of information accessible in the CAT pursuant to Section 6.1(m), provided that Participant staff may be provided access to CAT Data prior to meeting these requirements in exigent circumstances.[349] This affidavit and training requirement is already required by the Plan Processor before individuals can access the Central Repository, pursuant to Sections 6.1(m) and 6.5(f)(i)(B) of the CAT NMS Plan, but this proposal would require the Proposed Confidentiality Policies to access to CAT Data.

The Commission preliminarily believes it is important that any Participant staff with access to CAT Data, whether or not that staff has access to the Central Repository itself, should undergo appropriate training and sign the Safeguard of Information affidavit.[350] The Commission further believes that an exception for exigent circumstances is appropriate to provide for the rare circumstance where non-Regulatory Staff, who has not yet completed the training and affidavit requirements required by Section 6.5(g)(i)(F), must receive access to limited CAT Data to address an exceptional emergency. Examples might include the Chief Executive Officer of a securities exchange receiving a briefing relating to a sudden market-wide emergency or technical or operations staff being called upon to address an unanticipated threat to the continued functioning of a Participant's system. Under proposed Section 6.5(g)(i)(F), any Participant staff who does receive access to CAT Data prior to satisfying the requirements of proposed Section 6.5(g)(i)(F), due to exigent circumstances, would have to fulfill such requirements thereafter.

3. Additional Policies Relating to Access and Use of CAT Data and Customer and Account Attributes

The Commission also proposes several additional requirements to the Proposed Confidentiality Policies to expand upon existing provisions as described below. The Commission preliminarily believes that these additional requirements, and providing a comprehensive list of requirements for the Proposed Confidentiality Policies, would help result in policies that are sufficiently robust to protect CAT Data and to effectively regulate Participant usage of such data.

a. Limitations on Extraction and Usage of CAT Data

Rule 613 and the CAT NMS Plan limit the usage of CAT Data solely to surveillance and regulatory purposes.[351] In this regard, the CAT NMS Plan requires Participants to adopt policies and procedures that are reasonably designed to limit the use of CAT Data obtained from the Central Repository solely for surveillance and regulatory purposes.[352] In order to broaden the scope of such policies, the Commission proposes to add Sections 6.5(g)(i)(B) to require that the policies limit the extraction of CAT Data to the minimum amount necessary to achieve a specific surveillance or regulatory purpose.[353] The Commission recognizes the potential security risks that result from the extraction of CAT Data. At the same time, the Commission recognizes that there may be legitimate regulatory needs to extract CAT Data. Accordingly, the Commission believes that it is important for the CAT NMS Plan and the Participants' policies to require that only the minimum amount of CAT Data necessary to achieve surveillance or regulatory purposes shall be downloaded. Such a 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. The 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.

b. Individual Roles and Usage Restrictions

The Commission proposes to add Section 6.5(g)(i)(F) to the CAT NMS Plan to require the Proposed Confidentiality Policies to define the individual roles and regulatory activities of specific users, including those users requiring access to Customer and Account Attributes, of the CAT. This provision would require Participants to define roles and responsibilities on an individual level. For example, the policies could provide for a role in which a regulatory analyst accesses CAT Data to determine whether industry members complied with specific laws or SRO or Commission rules. The policies would be expected to define all individual roles and regulatory activities of users that Participants require to perform their regulatory and surveillance functions. For example, this would include roles and regulatory activities related to CAIS and CCID Subsystem access. The Commission also proposes to require in

[348] Although Commission personnel would be excluded from provisions such as Section 6.5(f)(i)(B), the rules and policies applicable to the Commission and its personnel will be comparable to those applicable to the Participants and their personnel. *See* CAT NMS Plan Approval Order, *supra* note 3, at 84765.

[349] The Commission notes that the Safeguard of Information affidavit approved by the Operating Committee pursuant to Section 6.5(f)(i)(B) must provide for personal liability for the misuse of data.

[350] In the CAT NMS Plan Approval Order, the Commission stated that it believed existing CAT NMS Plan provisions, including Section 6.1(m), ''indicate that the Plan Processor will require that all persons that have access to CAT Data will be required to complete training prior to accessing CAT Data, and expects that only those persons that have been adequately trained will have access to CAT Data.'' *See* CAT NMS Plan Approval Order, *supra* note 3, at 84755. The Commission believes that proposed Section 6.5(g)(i)(F) clarifies and affirms that these expectations regarding training should apply to all Participant staff with access to CAT Data, regardless of whether or not directly accessed through the Central Repository.

[351] *See, e.g.,* Rule 613(e)(4)(i)(A) and CAT NMS Plan, *supra* note 3, at Section 6.5(f)(i)(A), 6.5(g). However, a Participant may use data that *it* reports to the Central Repository for regulatory, surveillance, commercial, or other purposes as otherwise not prohibited by applicable law, rule or regulation. *See* CAT NMS Plan, *supra* note 3, at 6.5(h).

[352] *See* CAT NMS Plan, *supra* note 3, at Section 6.5(g). As proposed, the policies required by the Proposed Confidentiality Policies would still require this. *See* proposed Section 6.5(g)(i)(A). The Commission also proposes to modify this provision to state that the Proposed Confidentiality Policies must ensure the confidentiality of CAT Data and limit the use of CAT Data to solely surveillance and regulatory purposes, and not ''CAT Data obtained from the Central Repository,'' to avoid potential confusion and to make clear that requirements related to the Proposed Confidentiality Policies extend to CAT Data outside of the Central Repository.

[353] This provision is consistent with proposed Section 6.13(a)(i)(C). *See, supra* Part II.C.2. This provision of the Proposed Confidentiality Policies, as well as the others, will be subject to an annual examination of compliance by an independent auditor, which should help ensure that the provision is adhered to by Participants. *See, infra* Part II.G.4.

Section 6.5(f)(i) of the CAT NMS Plan that each Participant shall establish, maintain, and enforce usage restriction controls (*e.g.,* data loss prevention controls within any environment where CAT Data is used) in accordance with the Proposed Confidentiality Policies.

The Commission preliminarily believes that requiring the Participants to define the individual roles and regulatory activities of specific users, including those requiring access to Customer and Account Attributes, will encourage the Participants to thoroughly consider the roles and regulatory activities that individual users at Participants will be engaged in when using CAT Data and to consider what roles and regulatory activities require CAT Data to accomplish Participants' regulatory goals. Clearly defined roles and regulatory activities for individual users would help Participants better develop appropriate policies, procedures and controls to appropriately limit access to CAT Data on an individual level, and in particular, to establish appropriate Participant-specific procedures and usage restriction controls as required by proposed Section 6.5(g)(i). Over time, if Participants develop new roles and regulatory activities, or modify existing roles and regulatory activities, the Participants would be required to update the Proposed Data Confidentiality Policies, and related procedures and usage restriction controls, as appropriate. The Commission also preliminarily believes that requiring the Participants to define individual roles and regulatory activities of specific users should provide clarity and transparency with regard to the use of CAT Data to achieve specific regulatory and surveillance roles and goals of the Participants.[354]

In particular, the Commission preliminarily believes that this provision would help provide clarity with regard to individual roles in the context of regulatory coordination. In addition, the provision would add accountability for Regulatory Staff based on their individual roles. Some individual roles that are appropriate for some Participants may not be appropriate for others, because of differences between markets and the functions of the SROs. For example, FINRA may need to define individual roles and regulatory responsibilities that would not be applicable to exchange SROs. Or, an SRO with a trading floor may have to define individual roles that specifically relate to regulation and surveillance of trading floor activity. An SRO that has entered into an RSA with another SRO may need to define an individual role or roles for Regulatory Staff responsible for overseeing and monitoring the another SRO's performance under the RSA.

The Commission believes that requiring the establishment of usage restriction controls should help achieve the goal that individuals with access to CAT Data are using only the amount of CAT Data necessary to accomplish that individual's regulatory function. For example, Regulatory Staff with a regulatory role that only requires access to transactional data should not be given manual access to CAIS or CCID Subsystem. Additionally, limiting the access of an individual to only the specific data elements required for his or her surveillance or regulatory function reduces the potential of inappropriate receipt and misuse of CAT Data. The Commission believes that this requirement also leverages existing requirements of the CAT NMS Plan.[355] The Commission further believes that the CAT NMS Plan's logging requirements would provide information that would help Participants to establish and refine usage restriction controls.[356]

c. Policies Relating to Customer and Account Attributes

Currently, the policies and procedures required by Section 6.5(f)(ii) of the CAT NMS Plan and (g) do not directly address PII or Customer and Account Attributes, CAIS or the CCID Subsystem. The Commission believes that requiring Participants to incorporate policies relating to the access of Customer and Account Attributes, Programmatic CAIS Access, and Programmatic CCID Subsystem Access in the Proposed Confidentiality Policies would help protect the security and confidentiality of Customer and Account Attributes and CCIDs.

Specifically, the Commission proposes Section 6.5(g)(i)(I) of the CAT NMS Plan, which would require that the Proposed Confidentiality Policies be reasonably designed to implement and satisfy the Customer and Account Attributes data requirements of proposed Section 4.1.6 of Appendix D such that Participants must be able to demonstrate that a Participant's ongoing use of Programmatic CAIS and/or CCID Subsystem access is in accordance with the Customer Identifying Systems Workflow.[357] As discussed above in Part II.F, the Commission is proposing to amend Section 4.1.6 of Appendix D to more clearly define a Customer Identifying Systems Workflow, which sets forth explicit restrictions designed to limit the access and usage of Customer and Account Attributes only to the extent necessary to accomplish surveillance and regulatory purposes. The Commission believes that requiring the Proposed Confidentiality Policies to incorporate and implement the proposed Customer Identifying Systems Workflow would result in consistent application of the Customer Identifying Systems Workflow because all Participants would be subject to the policies which apply to Customer and Account Data usage both within and outside of a SAW. Together with Participant-specific procedures and usage restriction controls, these policies would help protect the security and confidentiality of Customer and Account Attributes, which would yield insight into a specific Customer's trading activity if coupled with transaction data, and would be collected and maintained by the CAT system.[358] These policies would also be subject to the approval, publication, and examination provisions discussed below.

The Commission also believes that it is appropriate to amend the CAT NMS Plan to highlight that the restrictions to a Participant's access to Customer and Account Attributes and Customer Identifying Systems through programmatic access continue to apply even after a Participant is initially approved for programmatic access. Thus, the proposed amendments state that the Proposed Confidentiality Policies must be reasonably designed to implement and satisfy the Customer and

[354] *See infra* Part II.E.4.

[355] Pursuant to the CAT NMS Plan, the CAT System must support an arbitrary number of roles with access to different types of CAT Data, down to the attribute level. *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 4.14. In addition, the administration and management of roles must be documented by the Plan Processor. *Id.* As noted below, the Commission proposing to amend Appendix D, Section 4.14 to clarify what ''arbitrary number'' means, *see, infra,* note 380.

[356] For example, the CAT NMS Plan requires the online targeted query tool to log ''submitted queries and parameters used in the query, the user ID of the submitter, the date and time of the submission, as well as the delivery of results. The Plan Processor will use this logged information to provide monthly reports to each Participant and the SEC of its respective metrics on query performance and data usage of the online query tool. The Operating Committee must receive all monthly reports in order to review items, including user usage and system processing performance.'' *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 8.1.1.

[357] *See supra* Part II.E and Part II.F.

[358] In addition, the Commission believes that the logging and reports required by Appendix D, Section 8.1.1 of the CAT NMS Plan would help Participants review whether the requirements of Section 4.1.6 of Appendix D are being followed. *See, supra* note 356.

Account Attributes data requirements of Section 4.1.6 of Appendix D such that Participants must be able to demonstrate that a Participant's ongoing use of Programmatic CAIS and/or CCID Subsystem access is in accordance with the Customer Identifying Systems Workflow and the restrictions noted therein. As a result of these policies, Participants must be able to demonstrate that their ongoing use of programmatic access continues to be in compliance with the restrictions to Customer and Account Attributes. For example, a Participant could document the changes to the Participant's evolving use of the programmatic access, noting in particular how the Participant's programmatic access continues to comply with the restrictions around access to Customer and Account Attributes since the Commission's initial approval of the Participant's programmatic access.[359] In light of this requirement, each Participant would be in a position to continually assess whether such ongoing programmatic access adheres to the restrictions of the Customer Identifying Systems Workflow. For example, if the functionality of a Participant's programmatic access changed to address a new regulatory purpose, the Participant must be able to demonstrate that the changed functionality remains consistent with all of the restrictions of the Customer Identifying Systems Workflow including (1) that the ''least privileged'' practice of limiting access to Customer Identifying Systems has been applied but that programmatic access to achieve the new regulatory purpose is still required; (2) that Regulatory Staff accessing Customer and Account Attributes through programmatic access is limited to only those individuals that maintain the appropriate regulatory role for such access; (3) that queries submitted by Regulatory Staff using programmatic access are based on a ''need to know'' data in the Customer Identifying Systems; and (4) that queries have been designed such that query results contain only the Customer and Account Attributes that Regulatory Staff reasonably believes will achieve the regulatory purpose of the inquiry or set of inquiries. The Commission preliminarily believes that these requirements, in conjunction with other requirements of the Proposed Confidentiality Policies discussed above, including monitoring, usage restriction controls and definitions of individual roles and regulatory activities of specific users, would help restrict Manual and Programmatic CAIS and/or CCID Subsystem Access to narrowly tailored circumstances when initially approved by the Commission and on an ongoing basis.

4. Approval, Publication, Review and Annual Examinations of Compliance

Currently, Section 6.5(g) of the CAT NMS Plan requires Participants to periodically review the effectiveness of the policies and procedures required by Section 6.5(g), and take prompt action to remedy deficiencies in such policies and procedures. However, the Commission believes that the highly sensitive nature of CAT Data and the importance of confidentiality warrants further oversight of the Proposed Confidentiality Policies, and in particular, the Commission believes it is appropriate to require approval of the Proposed Confidentiality Policies; require publication of these policies; provide specifics regarding Participant review of policies, procedures, and usage restriction controls; and require an annual examination of compliance with the Proposed Confidentiality Policies by independent accountants.

First, the Commission proposes to require that both the CISO and CCO of the Plan Processor be required to review the Proposed Confidentiality Policies.[360] In addition, the Commission proposes to require that the CCO of the Plan Processor obtain assistance and input from the Compliance Subcommittee,[361] and require that the policies required by proposed Section 6.5(g)(i) of the CAT NMS Plan be subject to review by the Operating Committee, after review by the CISO and CCO.[362] Currently, no specific individual is responsible for reviewing or approving the Participant policies and procedures required by Section 6.5(f)(ii) or 6.5(g) of the CAT NMS Plan. The Commission preliminarily believes that these requirements will further help result in Proposed Confidentiality Policies that are consistent with the requirements of the CAT NMS Plan and proposed changes herein, while providing for multiple opportunities for feedback and input while the Proposed Confidentiality Policies are being developed. It would allow the Plan Processor to have input in the creation of the Proposed Confidentiality Policies and would encourage consistency with policies and procedures created by the Plan Processor itself. The Commission preliminarily believes that it is appropriate to require the CCO to receive the assistance of the Compliance Subcommittee for broad input into the process of developing the Proposed Confidentiality Policies.[363] The Commission believes that it is reasonable to require the Operating Committee to review and approve the Proposed Confidentiality Policies after review by the CCO and CISO to prevent such policies from going into effect until these relevant parties have had the opportunity to review and provide feedback if necessary. Similarly, it is important for the Operating Committee, CCO and CISO to review updates to the Proposed Confidentiality Policies, as Participants make changes over time, because such parties can provide feedback and identify any inconsistencies with requirements of the CAT NMS Plan.

Second, the Commission believes that public disclosure of the Proposed Confidentiality Policies would be beneficial to investors and the public. Currently, the policies and procedures created by Participants pursuant to Section 6.5(f)(ii) and (g) are not required to be publicly disseminated. The Commission believes that public disclosure could help encourage the Participants to thoroughly consider the Proposed Confidentiality Policies and encourage the Participants to create robust Proposed Confidentiality Policies because they will be subject to public scrutiny. Thus, the Commission proposes new Section 6.5(g)(iv) which would require the Participants to make the Proposed Confidentiality Policies publicly available on each of the Participants' websites, or collectively on the CAT NMS Plan website, redacted of sensitive proprietary information.[364]

[359] The Commission generally believes that such documentation should at minimum have the same level of detail as the initial application material for programmatic access and should highlight how the Participant's programmatic access has changed over time.

[360] *See* proposed Sections 6.2(a)(v)(R) and 6.2(b)(viii).

[361] *See* proposed Section 6.2(a)(v)(R). The CAT NMS Plan requires the Operating Committee to maintain a compliance Subcommittee (the ''Compliance Subcommittee'') whose purpose shall be to aid the Chief Compliance Officer as necessary. *See* CAT NMS Plan, *supra* note 3, at Section 4.12(b).

[362] *See* proposed Section 6.5(g)(vi). The Commission anticipates that the Participants will provide the draft Proposed Confidentiality Policies to the CISO and CCO sufficiently in advance of the Operating Committee vote to permit review.

[363] Members of the Advisory Committee, composed of members that are not employed by or affiliated with any Participant or any of its affiliates or facilities, are currently on the Compliance Subcommittee. *See* CAT NMS Plan, *supra* note 3, at Section 4.13.

[364] *See supra* note 362. As proposed, publication of the policies could occur on either each of the Participant websites or on the CAT NMS Plan website. The CAT NMS Plan website was created by the Participants shortly after the adoption of Rule 613 and has been used as a means to communicate information to the industry and the

The Commission also believes that such a requirement would allow other Participants, broker-dealers, investors, and the public to better understand and analyze the Proposed Confidentiality Policies that govern Participant usage of and the confidentiality of CAT Data, and, when updated by Participants, any changes to these policies. The Commission preliminarily believes that broker-dealers and investors that generate the order and trade activity that is reported to CAT should be able to access the policies governing usage of CAT Data. In addition, due to the sensitivity and importance of CAT Data, which may contain personally identifiable information, trading strategies, and other valuable or sensitive information, it is important for broker-dealers, investors and the public to understand how CAT Data will be used and confidentiality maintained by the Participants, and to know the policies that Participants are bound to follow to protect the confidentiality of such data. The Commission believes that this may be particularly important for policies relating to access to Customer Account Attributes, as well policies relating to Manual and Programmatic CAIS and/or CCID Subsystem Access, which will allow customer attribution of order flow. The Commission is proposing an exception for sensitive proprietary information in the Proposed Confidentiality Policies because certain information in the policies required in the Proposed Confidentiality Policies may jeopardize the security of CAT Data if publicly disclosed. However, the Commission preliminarily does not believe that the proposed requirements for the Proposed Confidentiality Policies would require the disclosure of any substantial amount of sensitive proprietary information, and expects that there would be no redactions of information specifically required in the Proposed Confidentiality Policies, such as the identification of the individual roles and regulatory activities of specific users. The Commission believes that Participant-specific procedures and usage restriction controls, that would not be required to be made public, are more likely to contain the type of sensitive information that is inappropriate for public disclosure.

Currently, the CAT NMS Plan requires Participants to periodically review the effectiveness of the policies and procedures required by Section 6.5(g), maintain such policies and procedures, and take prompt action to remedy deficiencies in such policies and procedures, without further specifics regarding how this review is to occur. The Commission proposes changes to strengthen the review of the Proposed Confidentiality Policies in proposed Sections 6.5(g)(i)(J), 6.5(g)(ii) and 6.5(g)(v).

Proposed Section 6.5(g)(i)(J) would require that the Proposed Confidentiality Policies document monitoring and testing protocols that will be used to assess Participant compliance with the policies (*e.g.,* protocols monitoring CAT Data movement within any environment where CAT Data is used and associated testing to determine that such protocols are effective at identifying data leakage). In conjunction with this provision, proposed Section 6.5(g)(ii) would require the Participant to periodically review the effectiveness of the policies, procedures, and usage restriction controls required by Section 6.5(g)(i), including by using the monitoring and testing protocols documented within the policies pursuant to Section 6.5(g)(i)(J), and taking prompt action to remedy deficiencies in such policies, procedures and usage restriction controls.[365]

The Commission believes that these requirements are appropriate and should result in Proposed Confidentiality Policies, and Participant-specific procedures and usage restriction controls developed pursuant to the Proposed Confidentiality Policies, that are effective and complied with by each Participant across all environments where CAT Data is used. The Commission believes that review of implementation is important since even robust confidentiality policies could be circumvented or violated due to poor or improper implementation. Such periodic review will also help assure broker-dealers, investors and the public that the Participants are complying with the publicly disclosed Proposed Confidentiality Policies and related procedures and usage restriction controls. In addition, such review would assist Participants in meeting their requirement to maintain the Proposed Confidentiality Policies and related procedures and usage restriction controls as required by proposed Section 6.5(g)(i), including updating and revising them as appropriate.

The Commission also proposes a new Section 6.5(g)(v) which would require that, on an annual basis, each Participant shall engage an independent accountant to perform an examination of compliance with the policies required by Section 6.5(g)(i) in accordance with attestation standards of the American Institute of Certified Public Accountants (''AICPA'') (referred to as U.S. Generally Accepted Auditing Standards or GAAS) or the Public Company Accounting Oversight Board (''PCAOB''), and with Commission independence standards based on SEC Rule 2–01 of Regulation S–X.[366] In addition, the examination results shall be submitted to the Commission upon completion, in a text-searchable format (*e.g.* a text-searchable PDF). The examination report shall be considered submitted to the Commission when electronically received by an email address provided by Commission staff. The Commission preliminarily believes that this additional oversight would help result in such data being used solely for surveillance and regulatory purposes.

The Commission preliminarily believes that requiring the annual examination to be performed by an independent accountant should result in an examination that is performed by experienced professionals who are subject to certain professional standards. The Commission believes that permitting the examination to be in accordance with either the attestation standards of the AICPA or the PCAOB should give Participants greater flexibility in choosing an independent accountant. The Commission preliminarily believes that either standard is sufficient for the annual examinations to be performed adequately in these circumstances and both are familiar to the Commission, Participants and other market participants. The Commission believes that the independence standard of SEC Rule 2–01 of Regulation S–X would require Participants to engage an independent accountant that is independent of the Participant. The Commission understands that under the proposed requirement, Participants can likely use their existing auditors to perform this task as long as the existing auditors meet the independence requirements. The Commission further believes that as proposed, Participants that are affiliated would be permitted to

public at large since that time. *See* CAT NMS Plan, *supra* note 3, at Appendix C–109.

[365] The Commission would delete existing language in current Section 6.5(g)(i) that states: ''Each Participant shall periodically review the effectiveness of the policies and procedures required by this paragraph, and take prompt action to remedy deficiencies in such policies and procedures.'' The Commission believes that this language would be replaced and enhanced in substance by proposed Section 6.5(g)(i)(J).

[366] *See* 17 CFR 210.2–01. The Commission stresses that the proposed change relates only to a required ''examination'' by independent accountants, and has no relation to ''examinations'' performed by Commission staff.

use the same auditor for each affiliated entity.

The Commission believes that it is appropriate to require that the Participants provide the examination reports to the Commission. The Commission believes that this will allow the Commission to review the results of the examination, and to assess whether or not Participants are adequately complying with the Proposed Confidentiality Policies. The Commission believes that the examination reports should be protected from disclosure subject to the provisions of applicable law.[367]

The Commission requests comment on the amendments to consolidate and enhance Participants' data confidentiality policies and procedures. Specifically, the Commission solicits comment on the following:

132. Are current requirements relating to Participant data usage and confidentiality policies and procedures in Section 6.5(f)(ii), 6.5(f)(iii), and 6.5(g) in the CAT NMS Plan sufficient to protect the confidentiality and security of CAT Data?

133. Are the requirements of the Proposed Confidentiality Policies sufficiently robust to protect the confidentiality and security of CAT Data? Would additional or fewer requirements for such policies be beneficial?

134. Should the Proposed Confidentiality Policies be required to provide any other limitations on the extraction or usage of CAT Data? Do the proposed requirements sufficiently address concerns about policies and procedures related to the extraction and usage of CAT Data, including Customer and Account Attributes?

135. Should the Proposed Confidentiality Policies include specific data security requirements to help protect the confidentiality of CAT Data (*e.g.,* data loss prevention controls that include data access controls, data encryption, specific availability restrictions, and controls on data movement for securing CAT Data within any environment where CAT Data is used)? Should the Proposed Confidentiality Policies require Participants to maintain a full technical audit log of all CAT Data movement within their own environments?

136. Should the Proposed Confidentiality Policies or the CAT NMS Plan itself be required to define what ''surveillance and regulatory purposes'' means?

137. Should the Participants be required to establish, maintain, and enforce identical written policies as proposed Section 6.5(g)(i)? Should Participants be required to create procedures and usage restriction controls in accordance with the Proposed Confidentiality Policies?

138. Should the Proposed Confidentiality Policies limit extraction of CAT Data to the minimum amount of data necessary to achieve a specific surveillance or regulatory purpose? Should other policies and/or procedures regarding the extraction of CAT Data be required?

139. Should the Proposed Confidentiality Policies do more than define the individual roles and regulatory activities of specific users, *e.g.,* require documentation relating to each instance of access of CAT Data or define both appropriate and inappropriate usages of CAT Data?

140. The proposed amendments define Regulatory Staff. Is the proposed definition of Regulatory Staff appropriate and reasonable? Is the definition too broad or too narrow? Why or why not? For example, should the Commission limit the definition of Regulatory Staff to staff that *exclusively* report to the Chief Regulatory Officer (or similarly designated head(s) of regulation) or to persons within the Chief Regulatory Officer's (or similarly designated head(s) of regulation's) reporting line?

141. Is it reasonable and appropriate to require that the Proposed Confidentiality Policies limit access to CAT Data to Regulatory Staff and technology and operations staff that require access solely to facilitate access to and usage of the CAT Data by Regulatory Staff? Should any other Participant staff be permitted access to CAT Data?

142. The proposed amendments provide that the Proposed Confidentiality Policies require, absent exigent circumstances, that all Participant staff who are provided access to CAT Data must sign a ''Safeguard of Information affidavit'' and participate in the training program developed by the Plan Processor. Is this requirement appropriate and reasonable? Should Participants be permitted to allow access to CAT Data by staff that have not met the affidavit and training requirements if there are exigent circumstances? If so, how should exigent circumstances be defined? Who should determine what are exigent circumstances?

143. The proposed amendments provide that the Proposed Confidentiality Policies shall provide for only one limited exception for access to CAT Data by non-Regulatory Staff (other than technology and operations staff as provided for in Section 6.5(g)(i)(B)), namely a ''specific regulatory need for access.'' Is this exception clearly defined and easily understood? Is this exception too broad or too narrow? Should non-Regulatory Staff be permitted access to CAT Data in any other circumstance? Should non-Regulatory Staff be required to obtain written approval from a Participant's CRO for each instance of access to CAT Data? Should there be other requirements for non-Regulatory Staff to access CAT Data? Would this proposed requirement restrict the ability of certain non-Regulatory Staff, such as Chief Executive Officers, from carrying out their oversight over regulatory matters?

144. Is it appropriate and reasonable to require the Chief Information Security Officer of the Plan Processor, in collaboration with the Chief Compliance Officer of the Plan Processor, to review the Proposed Confidentiality Policies? Is it appropriate and reasonable to require the Operating Committee to approve the Proposed Confidentiality Policies? Should other individuals, entities, or the Commission be responsible for reviewing and/or approving these policies and procedures? Should such review and/or approval be subject to objective or subjective criteria, or explicit standards? If so, what should those criteria or standards be?

145. Are the proposed requirements for policies relating to Customer and Account Attributes, and CAIS and CCID Subsystem access, specifically proposed Section 6.5(g)(i)(I), appropriate and reasonable? Should other requirements relating to access or usage of Customer and Account Attributes be required? Is it appropriate and reasonable to have policy provisions that apply only to Customer and Account Attributes data instead of CAT Data more broadly?

146. Is it appropriate and reasonable to require that the Participants engage an independent accountant to examine on an annual basis each Participant's compliance with the policies required by proposed Section 6.5(g)(i)? Are the proposed attestation and independence standards appropriate?

147. Is it appropriate and reasonable to require that the Proposed Confidentiality Policies document monitoring and testing protocols that will be used to assess Participant compliance with the policies? Should additional specificity be added regarding the monitoring and testing requirements, such as requiring that these requirements include specific data loss prevention controls? Is it

[367] *See, e.g.,* 5 U.S.C. 552 *et seq.;* 15 U.S.C. 78x (governing the public availability of information obtained by the Commission).

appropriate and reasonable to require that Participants periodically review the effectiveness of the policies and procedures and usage restriction controls required by Section 6.5(g)(i)? Should more or fewer requirements regarding review of Participant compliance with the Proposed Confidentiality Policies or related procedures and/or usage restrictions be implemented?

148. Is it appropriate and reasonable to require that the Proposed Confidentiality Policies be made public? Is it appropriate and reasonable to provide that Participants have no obligation to disclose sensitive information? Should Participants be permitted to withhold any other type of information? Should the policies be published or made public in a form different than publication on the CAT NMS Plan website?

H. Regulator & Plan Processor Access

1. Regulatory Use of CAT Data

As noted earlier, Rule 613 and the CAT NMS Plan already limits the use of CAT Data to solely surveillance and regulatory purposes.[368] The CAT NMS Plan also provides that the Plan Processor must provide Participants' regulatory staff and the Commission with access to CAT Data for regulatory purposes only.[369] Examples of functions for which Participants' regulatory staff and the SEC could use CAT Data include economic analysis, market structure analyses, market surveillance, investigations, and examinations.[370] The Commission has received letters stating that ''surveillance and regulatory purposes'' is too broad and vague a limit on the use of CAT Data and should be clarified to prohibit SROs from using CAT Data for any commercial purpose.[371] The Commission believes that it is important that CAT Data be used only for surveillance and regulatory purposes. The Commission also believes it is important to prohibit Participants from using CAT Data in situations where use of CAT Data may serve both a surveillance or regulatory purpose, and commercial purpose, and, more specifically prohibit use of CAT Data for economic analyses or market structure analyses in support of rule filings submitted to the Commission pursuant to Section 19(b) of the Exchange Act (''SRO rule filings'') in these instances.

The Commission proposes to amend Section 8.1 of Appendix D to add to the requirement that access to CAT Data would be only for surveillance and regulatory purposes that the access should be consistent with Proposed Confidentiality Policies as set forth in Section 6.5(g) of the CAT NMS Plan. The Commission also proposes to amend Section 8.1 of Appendix D to specify that Regulatory Staff and the SEC must be performing regulatory functions when using CAT Data, including for economic analyses, market structure analyses, market surveillance, investigations, and examinations, and 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. The Commission further proposes that in any case where the use of CAT Data may serve both a surveillance or regulatory purpose and a commercial purpose, such as economic analyses or market structure analyses in support of SRO rule filings with both a regulatory and commercial purpose, use of CAT Data is not permitted. This would be consistent with the existing requirement in Rule 613 the CAT NMS Plan that CAT Data must be used for *solely* regulatory and surveillance purposes.[372]

The Commission preliminarily believes that the proposed amendments to Section 8.1 of Appendix D are appropriate because adding the requirement that surveillance and regulatory purposes be consistent with the Proposed Confidentiality Policies would establish a minimum standard for what constitutes regulatory use of CAT Data that is identical across the Participants. It would additionally help protect the security of CAT Data by limiting the extraction of CAT Data to, as proposed, the minimum amount of data necessary to achieve a specific surveillance or regulatory purpose. The Commission's proposed amendments concerning the functions for which CAT Data can be used reiterate that the CAT Data may only be used for solely surveillance and regulatory purposes.

The Commission believes that prohibiting the use of CAT Data for SRO rule filings with a regulatory and commercial purpose is important because exchange groups are no longer structured as mutual organizations that are owned, for the most part, by SRO members. 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.[373] CAT Data includes data submitted by the SROs and broker-dealers.[374] 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

[368] *See, e.g.,* Rule 613(e)(4)(i)(A) and CAT NMS Plan, *supra* note 3, at Section 6.5(f)(i)(A), 6.5(g). However, a Participant may use data that *it* reports to the Central Repository for regulatory, surveillance, commercial, or other purposes as otherwise not prohibited by applicable law, rule or regulation. *See* CAT NMS Plan, *supra* note 3, at Section 6.5(h).

[369] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 8.1. Because this section currently only refers to ''regulatory purposes,'' the Commission proposes to amend this section to clarify that such access is for surveillance and regulatory purposes only, to be consistent with Rule 613 and other sections of the CAT NMS Plan. *See, supra* note 368. This change would also be consistent with proposed changes discussed below, that would clarify the requirement that CAT Data should be used only for surveillance and regulatory purposes.

[370] *Id.*

[371] *See* letter dated November 11, 2019 from Kenneth E. Bentsen, Jr., President and CEO, Securities Industry and Financial Markets Association (''SIFMA''), to the Honorable Jay Clayton, Chairman, Commission (''[t]he Commission should clarify the meaning of the term 'surveillance and regulatory purposes' . . . . In doing so, the Commission should ensure that the SROs will be clearly prohibited from using CAT Data for any commercial purpose''); letter dated December 16, 2019 from Ronald Newman, National Political Director, and Kate Ruane, Senior Legislative Counsel, American Civil Liberties Union, to the Honorable Jay Clayton, Chairman, Commission (''[t]his standard is far too broad and vague to assure that the data will only be acquired and used for specific and legitimate enforcement purposes. The SEC should provide a clearly defined standard that must be met in order to access and use information in the CAT and should specifically prohibit those with access from using the information for any commercial purpose'').

[372] *See* 17 CFR 242.613(e)(4)(i)(A); CAT NMS Plan, *supra* note 3, Sections 6.5(c) and 6.5(g). Because the CAT NMS Plan requires CAT Data to be used for solely regulatory or surveillance purposes, Participants may not use CAT Data for any economic analyses or market structure analyses that do not have a solely regulatory or surveillance purpose.

[373] *See* Securities Exchange Act Release No. 50699 (Nov. 18, 2004), 69 FR 71125, 71132 (Dec. 8, 2004) (noting that SROs had been challenged by the trend to demutualize and that the ''impact of demutualization is the creation of another SRO constituency—a dispersed group of public shareholders—with a natural tendency to promote business interests'').

[374] SROs compete for order flow with off exchange venues, including alternative trading systems (which also match buyers and sellers but are subject to a different regulatory framework and in many cases do not display pricing information to the general public) and other liquidity providers (*e.g.,* broker-dealer internalizers).

requirement that CAT Data must be used for *solely* regulatory and surveillance purposes,[375] 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.[376] However, this prohibition would not restrict an SRO's ability to use CAT Data for SRO rule filings with a solely surveillance or regulatory purpose, such as monitoring for market manipulation or compliance with sales practice rules.[377]

2. Access to CAT Data

As described above, the Commission proposes to amend Appendix D, Section 8.1 of the CAT NMS Plan to add that access to CAT Data must be consistent with the Participants' Confidentiality Policies and Procedures as set forth in proposed Section 6.5(g). The Commission also continues to believe that access of Participants' Regulatory Staff and the Commission to CAT Data must be based on an RBAC model. RBAC 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.[378] An RBAC model specifically assigns the access and privileges of individual CAT users based on the individual's job responsibilities and need for access. Users would not be directly assigned specific access and privileges but would instead receive access and privileges based on their assigned role in the system.

The CAT NMS Plan currently provides that an RBAC model ''must be used to permission user[s] with access to different areas of the CAT System.'' [379] The CAT NMS Plan further requires the CAT System to support an arbitrary number of roles with access to different types of CAT Data, down to the attribute level.[380] The administration and management of roles must be documented, and Participants, the SEC, and the Operating Committee must be provided with periodic reports detailing the current list of authorized users and the date of their most recent access.[381] The Plan Processor is required to log every instance of access to Central Repository data by users.[382] The CAT NMS Plan, as part of its data requirements surrounding Customer and Account Attributes,[383] further requires that using the RBAC model, access to Customer and Account Attributes shall be configured at the Customer and Account Attribute level, following the ''least privileged'' practice of limiting access to the greatest extent possible.

The Commission now believes that it is important to require that access of Participants' Regulatory Staff [384] to all CAT Data must be through the RBAC model, and extend the practice of requiring ''least privileged'' access to all CAT Data, and not just to Customer and Account Attributes. Specifically, the Commission proposes to amend Appendix D, Section 8.1 of the CAT NMS Plan by adding that the Plan Processor must provide Participants' Regulatory Staff and the SEC with access to all CAT Data based on an RBAC model that follows ''least privileged'' practices.

The Commission preliminarily believes that this proposed amendment would strengthen the requirement that, in addition to requiring a regulatory purpose, access to CAT Data is also restricted by an RBAC model that follows ''least privileged'' practices. The Commission preliminarily believes that this proposed amendment would provide consistency across the CAT NMS Plan by requiring that the RBAC and ''least privileged'' practices requirement that applies to the CAT System and the Customer and Account Attributes also applies to accessing CAT Data. An RBAC model and ''least privileged'' practices requirement would provide access only to those who have a legitimate purpose in accessing CAT Data, and limit the privileges of those users to the minimum necessary to perform their regulatory roles and functions.

The Commission also proposes amendments to Appendix D, Section 4.1.4 to address the general requirements relating to access to Customer Identifying Systems and transactional CAT Data by Plan Processor employees and contractors. Specifically, the Commission proposes amendments to Appendix D, Section 4.1.4 to require that ''[f]ollowing 'least privileged' practices, separation of duties, and the RBAC model for permissioning users with access to the CAT System, all Plan Processor employees and contractors that develop and test Customer Identifying Systems shall only develop and test with non-production data and shall not be entitled to access production data (*i.e.,* Industry Member Data, Participant Data, and CAT Data) in CAIS or the CCID Subsystem. All Plan Processor employees and contractors that develop and test CAT Systems containing transactional CAT Data shall use non-production data for development and testing purposes; if it is not possible to use non-production data, such Plan Processor employees and contractors shall use the oldest available production data that will support the desired development and testing, subject to the approval of the Chief Information Security Officer.'' [385]

The Commission believes that imposing the limitations on which Plan

[375] *See supra* note 368.

[376] The Commission preliminarily believes that this is consistent with the Participants' understanding of the CAT NMS Plan, and notes that the current CAT Reporter Agreement, which is between the Plan Processor and CAT Reporters, states that the signing parties acknowledge that the Consolidated Audit Trail, LLC, the Participants, and the Plan Processor ''are not authorized by the CAT NMS Plan to use the submitted CAT Data for commercial purposes[.]'' *See* ''Consolidated Audit Trail Reporter Agreement,'' *available at: https://www.catnmsplan.com/sites/default/files/2020-05/Consolidated-Audit-Trail-Reporter-Agreement-amended_0.pdf.*

[377] Although the Participants would be permitted to use CAT Data to support a rule filing with a solely surveillance or regulatory purpose, proposed Section 6.13(a)(i)(C) would permit only the extraction of the minimum amount of CAT Data necessary to achieve that specific regulatory purpose. However, the proposed amendment would not prevent a Participant from using the data that it reports to the Central Repository for regulatory, surveillance, commercial, or other purposes as otherwise not prohibited by applicable law, rule or regulation. See CAT NMS Plan, *supra* note 3, at 6.5(h).

[378] See CAT NMS Plan, *supra* note 3, at Appendix C, note 250.

[379] See CAT NMS Plan, *supra* note 3, at Appendix D, Section 4.1.4. The Commission also proposed to correct certain grammatical errors. *See* Appendix D, Sections 4.1.4, 8.2.2.

[380] The Commission proposes to amend Appendix D, Section 4.1.4 to state that the CAT System must support as many roles as required by Participants and the Commission to permit access to different types of CAT Data, down to the attribute level. The Commission believes that this change clarifies what ''arbitrary number of roles'' means in the context of the RBAC model required by the CAT NMS Plan and should result in the implementation of an RBAC model that will support the number of roles required by Participants and the Commission.

[381] The CAT NMS Plan provides that the reports of the Participants and the SEC will include only their respective list of users and that the Participants must provide a response to the report confirming that the list of users is accurate. The required frequency of this report would be defined by the Operating Committee. See CAT NMS Plan, *supra* note 3, at Appendix D, Section 4.1.4. The Commission proposes to amend the language in Appendix D, Section 4.1.4 to make clear that the reports provided to the Participants and the SEC will include only their respective list of users and that the CAT NMS Plan obligates the Participants to provide a response to the report confirming that the list of users is accurate. The Commission believes that these changes are consistent with existing expectations and could help avoid potential confusion regarding obligations relating to these reports.

[382] *Id.*

[383] See CAT NMS Plan, *supra* note 3, at Appendix D, Section 4.1.6.

[384] As noted earlier, the Commission proposes to amend Appendix D, Section 8.1 to remove references to ''regulatory staff'' and replace them with the defined term ''Regulatory Staff.'' *See supra* note 342.

[385] *See* proposed Appendix D, Section 4.1.4 (Data Access).

Processor employees and contractors can access Customer Identifying Systems is appropriate as the possibility of misuse of CAT Data exists with those individuals as with any Regulatory Staff. Therefore it is also appropriate to require that Plan Processor employees and contractors accessing Customer Identifying Systems must follow ''least privileged'' practices, separation of duties, and the RBAC model for permissioning users with access to the CAT System. The Commission also believes it is appropriate to limit the actual testing and development of Customer Identifying Systems to non-production data because such non-production data will not contain Customer and Account Attributes and other data that could be used to identify Customers and other market participants. With respect to transactional CAT Data, the Commission believes that is reasonable to require that Plan Processor employees and contractors use non-production data if possible; however, the Commission recognizes that for practical purposes, it may be difficult or impossible to generate non-production transactional CAT Data sufficient for desired development and testing. As a result, Plan Processor employees and contractors may use production data in the testing and development of CAT Systems that contains transactional CAT Data, but they must use the oldest available production data that will support the desired development and testing. Given that production data will be accessed in this specific circumstance, the Commission believes that the Chief Information Security Officer should approve such access.

The Commission requests comment on the proposed amendments concerning the access of regulators and the Plan Processor to CAT Data. Specifically, the Commission solicits comment on the following:

149. There is existing CAT NMS Plan language stating that CAT Data may be used solely for surveillance and regulatory purposes.[386] Is it necessary to further provide that the use of CAT Data is prohibited in cases where it would serve both a regulatory or surveillance purpose, and a commercial purpose?

150. The Commission proposes to prohibit the use of CAT Data in SRO rule filings that have both a regulatory and commercial purpose. Are there instances where it is necessary to use CAT Data in an SRO rule filing that may have a commercial impact but is essential for regulatory purposes? Please provide examples. If so, what should be the conditions or process by which SROs would be permitted to use CAT Data for SRO rule filings?

151. Does requiring that access to CAT Data be restricted by an RBAC model that follows ''least privileged'' practices, and adding the requirement that access must be consistent with the Proposed Confidentiality Policies enhance the security of CAT Data? Is adding the requirement that access to CAT Data must be consistent with the Proposed Confidentiality Policies necessary and appropriate? Should the proposed amendments be more prescriptive and define potential roles generally or specifically that would be used in an RBAC model or least privileged access model?

152. The proposed amendments require the Plan Processor employees and contractors that test and develop Customer Identifying Systems to follow ''least privileged'' practices, separation of duties, and the RBAC model for permissioning users with access to the CAT System. Do commenters agree that such employees and contractors should follow these principles and practices in order to access Customer Identifying Systems?

153. Should Plan Processor contractors supporting the development or operation of the CAT System be subject to certain additional access restrictions? For example, should Plan Processor contractors be required to access CAT system components through dedicated systems? Should Plan Processor contractors be subject to heightened personnel security requirements before being granted access to Customer Identifying Systems or any component of the CAT System?

154. The proposed amendment requires that all Plan Processor employees and contractors that develop and test Customer Identifying Systems shall only develop and test with non-production data and shall not be entitled to access production data (*i.e.,* Industry Member Data, Participant Data, and CAT Data) in CAIS or the CCID Subsystem. Do commenters agree that is appropriate? If data other than non-production data should be permitted to be used, what type of data should be used by Plan Processor employees and contractors to test and develop Customer Identifying Systems? Please be specific in your response.

155. The proposed amendments require that if non-production data is not available for Plan Processor employees and contractors to develop and test CAT Systems containing transactional CAT Data, then such employees and contractors shall use the oldest available production data that will support the desired development and testing. Do commenters agree that Plan Processor employees and contractors should be permitted to use the oldest available production data that will support the desired development and testing?

156. The proposed amendments require that the Chief Information Security Officer approve access to the oldest available production data that will support the desired development and testing for Plan Processor employees and contractors that are testing and developing systems that contain transactional CAT Data. Do commenters agree that the Chief Information Security Officer should approve such access?

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

I. Secure Connectivity & Data Storage

The Commission proposes to amend the CAT NMS Plan to enhance the security of connectivity to the CAT infrastructure. Currently under the CAT NMS Plan, Appendix D, Section 4.1.1, the CAT System ''must have encrypted internet connectivity'' and CAT Reporters must connect to the CAT infrastructure, ''using secure methods such as private lines or (for smaller broker-dealers) Virtual Private Network connections over public lines.'' The Participants have stated that the CAT NMS Plan does not require CAT Reporters to use private lines to connect to the CAT due to cost concerns, particularly for small broker dealers.[387] Because the CAT NMS Plan does not explicitly require private lines for any CAT Reporters and does not differentiate between Participants and Industry Members, the Commission now proposes to amend Section 4.1.1 of Appendix D to codify and enhance existing secure connectivity practices, and to differentiate between connectivity requirements for Participants and Industry Members.

First, the Commission proposes to amend Section 4.1.1 of Appendix D to require Participants to connect to CAT infrastructure using private lines. Since

[386] *See supra* note 368.

[387] *See* CAT NMS Plan Approval Order, *supra* note 3, at 84760.

the Commission approved the CAT NMS Plan and the Participants began implementing the CAT, the Participants have determined that they would connect to the CAT infrastructure using private lines only. The Commission preliminarily believes that it is appropriate for the CAT NMS Plan to reflect a current practice which provides additional security benefits over allowing Participants to connect to CAT infrastructure through public lines, even if through encrypted internet connectivity. The 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.

Next, the Commission proposes to amend Appendix D, Section 4.1.1 to clarify the methods that CAT Reporters may use to connect to the CAT infrastructure and to make the provision consistent with existing practice. The Commission proposes to state that Industry Members must connect to the CAT infrastructure using secure methods such as private lines for machine-to-machine interfaces or encrypted Virtual Private Network connections over public lines for manual web-based submissions. ''Machine-to-machine'' interfaces mean direct communications between devices or machines, with no human interface or interaction, and in the CAT context would generally be automated processes that can be used to transmit large amounts of data. In contrast, manual web-based submissions would require human interaction and input. These proposed amendments would be consistent with existing requirements imposed by FINRA CAT, LLC (''FINRA CAT'') regarding connectivity, which has required that all machine-to-machine interfaces utilize private lines and only permits the use of public lines by establishing an authenticated, encrypted connection through the CAT Secure Reporting Gateway.[388]

The Commission preliminarily believes that codifying these existing FINRA CAT secure connectivity requirements for Industry Members is appropriate. 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. The Commission preliminarily believes that private lines would be more robust and capable of handling the automated transfer of potentially large amounts of data, in comparison to public lines, because the private lines would not be shared with public users and the private lines could be designed to meet the bandwidth and stability requirements necessary for CAT reporting. In addition, as noted above, the Commission preliminarily believes that private lines are more secure than public lines, which may be shared with other users. However, the Commission believes that for manual web-based submissions, it is appropriate to codify FINRA CAT's existing secure connectivity framework, which allows broker-dealers that do not need or use machine-to-machine connectivity to submit data to CAT using the CAT Secure Reporting Gateway.[389] The Commission preliminarily believes that such an allowance is appropriate for Industry Members that can meet their reporting obligations through manual web-based submissions that do not contain an amount of data that justifies the expense and effort required to install and maintain private lines. Requiring manual web-based submissions to be submitted in an encrypted Virtual Private Network should result in submissions that remain secure, even if transmitted over public lines.

The Commission is also proposing to add specific requirements relating to connections to CAT infrastructure, specifically, to amend Appendix D, Section 4.1.1 to require ''allow listing.'' Specifically, the Commission proposes 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 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. While the CAT NMS Plan currently specifies certain connectivity requirements, it does not require the Plan Processor to limit access to the CAT infrastructure based on an authorized end user's location. The Commission preliminarily believes that it is not generally appropriate for CAT Reporters or Participants to access the CAT System in countries where regulatory use is not both necessary and expected. As proposed, CAT Reporters or Participants would need to justify to the Participants and the Plan Processor the addition of a new country to the ''allow list.'' The Commission further believes that the Plan Processor has a detailed understanding of both authorized users and their organization's IP address information and has the ability to restrict access accordingly. The Commission also preliminarily believes that the burden of maintaining an allowed list may be minimized by using the same set of allowed countries for both CAT Reporters and regulatory user access.

In cases where it is not possible to use multi-factor authentication technology to determine the location of a CAT Reporter or a regulatory user, the Commission preliminarily believes that a policies and procedures approach to compliance is appropriate. The proposed amendments would allow the Plan Processor to allow access in such circumstances under established policies and procedures that would improve the security of the CAT System. Similarly, when using bypass codes, the policies and procedures could mandate that Help Desk staff facilitating such access ask relevant questions on the location of the CAT Reporter or Regulatory Staff and remind them of CAT access geo-restrictions. Based on its experience during the implementation of CAT, the Commission believes that it is likely that the usage of bypass codes will be minimal compared to standard multi-factor authentication push technology or other technologies that allow for geo-

[388] *See* FINRA CAT Connectivity Supplement for Industry Members, Version 1.5 (dated February 27, 2020), *available at: https://www.catnmsplan.com/sites/default/files/2020-03/FINRA_CAT_Connectivity_Supplement_for_Industry_Members_1.5.pdf.* The FINRA CAT Connectivity Supplement for Industry Members describes the methods available for Industry Members and CAT Reporting Agents to connect to the CAT system. The CAT Secure Reporting Gateway enables end users with secure access to the CAT Reporter Portal via a web browser. FINRA CAT is the Plan Processor.

[389] *See id.*

restrictions, and preliminarily believes that policies and procedures applicable to such circumstances would help protect the security of CAT Data.

The Commission recognizes that it may not always be possible to accurately detect the location of a CAT Reporter or Regulatory Staff given distributed networking, and that there is a potential for malicious spoofing of location or IP addresses. As discussed above, in situations where a CAT Reporter or Regulatory Staff is unable to be located, the proposed policies and procedures could address whether or not connectivity is possible and address how such connectivity is granted. With regard to malicious spoofing by third parties, the Commission preliminarily believes that existing protections, such as the private line connectivity described above, should help result in a framework where only authorized CAT Reporters or Regulatory Staff are able to connect to CAT infrastructure. In addition, in spite of these potential issues, the Commission believes that in comparison to existing requirements, the benefits of ''allow listing,'' and in particular identifying specific known access points such as specific countries and IP addresses, would enhance the security of connectivity to the CAT while not being substantially difficult to implement in available technologies.

Currently, the CAT NMS Plan imposes requirements on data centers housing CAT Systems (whether public or private), but does not impose any geographical restrictions or guidelines.[390] The Commission now believes it is appropriate the enhance requirements applicable to data centers housing CAT Systems by imposing geographic restrictions. Specifically, the Commission proposes to amend Appendix D, Section 4.1.3 to require that data centers housing CAT Systems (whether public or private) must be physically located in the United States.

The Commission preliminarily believes that requiring CAT data centers to be physically located in the United States will help strengthen the security of CAT Data by ensuring that no data center housing CAT Systems with CAT Data is located outside of the United States. Locating data centers housing the CAT System outside of the United States could subject such data centers, and the CAT System and CAT Data within, to security risks that may arise only because of their location. The Commission also preliminarily believes that requiring CAT data centers to be physically located in the United States would result in CAT data centers that are within the jurisdiction of both the Commission and the United States legal system. The Commission also preliminarily believes that any benefit, such as any cost advantages, of locating data centers housing the CAT System outside of the United States would not justify the increased risks associated with locating the data centers outside of the United States.

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

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

160. Should the CAT NMS Plan be amended to require the Plan Processor to allow access based on countries and where possible, based on IP addresses? Is it too restrictive or should the restriction be more granular? Should the CAT NMS Plan specify which countries are or are not acceptable to be allowed access or provide specific guidance or standards on how the Plan Participant can select countries to be allowed access? Do CAT Reporters have business or regulatory staff or operations in countries outside of the United States? Should Participant access be restricted to specific countries, *e.g.,* the United States, Five Eyes? If so, which countries and why? Should Plan Processor access be restricted to specific countries, *e.g.,* the United States, Five Eyes? If so, which countries and why?

161. Is it appropriate to require the Plan Processor to establish policies and procedures governing access when the location of a CAT Reporter or Regulatory Staff cannot be determined technologically? Do commenters believe that such a provision is necessary, or would it be more appropriate for the CAT NMS Plan to prohibit access if the location of a CAT Reporter or Regulatory Staff cannot be determined technologically?

162. Should the CAT NMS Plan specifically prescribe what types of multi-factor authentication are permissible? Should the CAT NMS Plan prohibit the usage of certain methods of multi-factor authentication, such as usage of one-time passcodes?

163. Should the CAT NMS Plan require data centers housing CAT Systems (whether public or private) to be physically located within the United States? Would it be appropriate to locate data centers housing CAT Systems in any foreign countries?

164. Currently, the CAT NMS Plan states that the CAT databases must be deployed within the network infrastructure so that they are not directly accessible from external end-user networks. If public cloud infrastructures are used, virtual private networking and firewalls/access control lists or equivalent controls such as private network segments or private tenant segmentation must be used to isolate CAT Data from unauthenticated public access. Should additional isolation requirements be added to the CAT NMS Plan to increase system protection? For example, should the Commission require that the CAT System use dedicated cloud hosts that are physically isolated from a hardware perspective? Please explain the impact on the implementation of the CAT including costs and benefits.

165. Should the use of multiple dedicated hosts be required so that development is physically isolated from production? Should all development and production be done on a separate dedicated host or should only Customer Identifying Systems development and/or production be done on its own dedicated cloud host? Please explain the impact on the implementation and security of the CAT including costs and benefits.

J. Breach Management Policies and Procedures

Appendix D, Section 4.1.5 of the CAT NMS Plan requires the Plan Processor to develop policies and procedures governing its responses to systems or data breaches, including a formal cyber incident response plan and documentation of all information relevant to breaches.[391] The CAT NMS Plan further specifies that the cyber incident response plan will provide guidance and direction during security incidents, but otherwise states that the cyber incident response plan *may* include several items.[392] The Commission believes that due to the importance of the security of CAT Data and the CAT System, and the potential

[390] *See* CAT NMS Plan, *supra* note 3, Appendix D, Section 4.1.3. While the CAT NMS Plan does not impose geographical restrictions on CAT Systems, Regulation SCI, which applies to the Central Repository, *see supra* note 54, requires SCI entities to establish, maintain, and enforce written policies and procedures that, among other things, shall include business continuity and disaster recovery plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse and that are reasonably designed to achieve two-hour resumption of critical SCI systems following a wide-scale disruption. *See 17* CFR 242.1001(a)(2)(v).

[391] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 4.1.5. The cyber incident response plan is subject to review by the Operating Committee. *See id.*

[392] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 4.1.5. The CAT NMS Plan also lists a series of items that documentation of information relevant to breaches should include. *Id.*

for serious harm should a system or data breach (*e.g.,* any unauthorized entry into the CAT System or indirect SCI systems) [393] occur, that more specific requirements for the formal cyber incident response plan required by Appendix D, Section 4.1.5 of the CAT NMS Plan would be beneficial.[394] Specifically, as discussed below, the Commission believes that requiring the formal cyber incident response plan to incorporate corrective actions and breach notifications, modeled after similar provisions in Regulation SCI, is appropriate.

The Commission believes that the cyber incident response plan should require the Plan Processor to take appropriate corrective action in response to any data security or breach (*e.g.,* any unauthorized entry into the CAT System or indirect SCI systems). Specifically, the Commission proposes to modify Appendix D, Section 4.1.5 of the CAT NMS Plan to require that the formal cyber incident response plan must include ''taking appropriate corrective action that includes, at a minimum, mitigating potential harm to investors and market integrity, and devoting adequate resources to remedy the systems or data breach as soon as reasonably practicable.'' This language relating to taking corrective action and devoting adequate resources mirrors the similar requirement applicable to SCI entities for SCI events [395] in Rule 1002(a) of Regulation SCI.[396] This requirement would obligate the Plan Processor to respond to systems or data breaches with appropriate steps necessary to remedy each systems or data breach and mitigate the negative effects of the breach, if any, on market participants and the securities markets more broadly.[397] The specific steps that the Plan Processor would need to take to mitigate the harm will be dependent on the particular systems or data breach, its causes, and the estimated impact of the breach, among other factors. To the extent that a systems or data breach affects not only just the users of the CAT System, but the market 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. In requiring ''appropriate'' corrective action, this provision would not prescribe with specificity the types of corrective action that must be taken, but instead would afford flexibility to the Plan Processor in determining how to best respond to a particular systems or data breach in order to remedy the issue and mitigate the resulting harm after the issue has already occurred.[398] In addition, as with Rule 1002(a) of Regulation SCI, the proposed provision does not require ''immediate'' corrective action, but instead would require that corrective action be taken ''as soon as reasonably practicable,'' which would allow for appropriate time for the Plan Processor to perform an initial analysis and preliminary investigation into a potential systems or data breach before beginning to take corrective action.

In addition, the Commission believes that the Plan Processor should be required to provide breach notifications of systems or data breaches, and that such notifications should be incorporated into the formal cyber incident response plan. Specifically, the Commission proposes to modify Appendix D, Section 4.1.5 of the CAT NMS Plan to require the Plan Processor to provide breach notifications of systems or data breaches to CAT Reporters that it reasonably estimates may have been affected, as well as to the Participants and the Commission, promptly after any responsible Plan Processor personnel have a reasonable basis to conclude that a systems or data breach has occurred.[399] The Commission also proposes to require that the cyber incident response plan provide for breach notifications. As proposed, such breach notifications could be delayed, as described in greater detail below, if the Plan Processor determines that dissemination of such information would likely compromise the security of the CAT System or an investigation of the systems or data breach, and would not be required if the Plan Processor reasonably estimates the systems or data breach would have no or a de minimis impact on the Plan Processor's operations or on market participants.

The Commission believes that in the case of systems or data breaches, impacted parties should receive notifications, including CAT Reporters affected by the systems or data breaches, such as the SROs or Industry Members, as well as the Participants and Commission, which use the CAT System for regulatory and surveillance purposes. The Commission notes that these breach notifications could

[393] ''Indirect SCI systems'' are defined as ''any systems of, or operated by or on behalf of, an SCI entity that, if breached, would be reasonably likely to pose a security threat to SCI systems.'' 17 CFR 242.1000.

[394] The Commission adopted Regulation SCI in November 2014 to strengthen the technology infrastructure of the U.S. securities markets. *See* Securities Exchange Act Release No. 73639 (November 19, 2014), 79 FR 72251 (December 5, 2014). Regulation SCI is designed to reduce the occurrence of systems issues in the U.S. securities markets, improve resiliency when systems problems occur, and enhance the Commission's oversight of securities market technology infrastructure. Regulation SCI applies to certain core technology systems (''SCI systems'') of key market participants called ''SCI entities'' which include, among others, the Participants. The CAT System is an SCI system of the Participants. Regulation SCI imposes corrective action and breach management obligations on SCI entities, but also includes requirements for SCI entities to, among other things: Establish, maintain, and enforce written policies and procedures reasonably designed to ensure that their key automated systems have levels of capacity, integrity, resiliency, availability, and security adequate to maintain their operational capability and promote the maintenance of fair and orderly markets; operate such systems in accordance with the Exchange Act and the rules and regulations thereunder and the entities' rules and governing documents, as applicable; provide certain notifications and reports to the Commission regarding systems problems and systems changes; inform members and participants about systems issues; conduct business continuity and disaster recovery testing and penetration testing; conduct annual reviews of their automated systems; and make and keep certain books and records.

The Commission notes that the proposed changes to Appendix D, Section 4.1.5, would apply separately and independently to the Participants, but would not in any way increase, reduce or otherwise change the Plan Processor and Participants' responsibilities applicable under Regulation SCI.

[395] An ''SCI event'' is an event at an SCI entity that constitutes a system disruption, a systems compliance issue, or a systems intrusion. A ''systems disruption'' means an event in an SCI entity's SCI systems that disrupts, or significantly degrades, the normal operation of an SCI system. A ''systems compliance issue'' means ''an event at an SCI entity that has caused any SCI system of such entity to operate in a manner that does not comply with the Act and the rules and regulations thereunder or the entity's rules or governing documents, as applicable.'' A ''systems intrusion'' means any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity.'' *See* Rule 1000 of Regulation SCI, 17 CFR 242.1000.

[396] *See* Rule 1002(a) of Regulation SCI, 17 CFR 242.1002(a).

[397] The CAT NMS Plan already requires the Plan Processor to develop policies and procedures that include ''documentation of all information relevant to breaches,'' which ''should include,'' among other things, a chronological timeline of events, relevant information related to the breach, response efforts and the impact of the breach. *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 4.1.5. In addition, to the extent that a systems or data breach meets the definition of an SCI Event, *see supra* note 395, Regulation SCI would require written notification to the Commission that includes, among other things: (i) The SCI entity's assessment of the impact of the SCI event on the market; (ii) the steps the SCI entity has taken, is taking, or plans to take with respect to the SCI event; (iii) the time the SCI event was resolved; (iv) the SCI entity's rule(s) and or governing document(s), as applicable, that relate to the SCI event; and (v) any other pertinent information known by the SCI entity about the SCI event. *See* 242.1002(b)(4)(ii)(A).

[398] For example, appropriate corrective action to a CAT Data breach could include the rotation of CCIDs, to limit the potential harm of inadvertent disclosure of CCIDs. *See also* Regulation SCI Adopting Release, *supra* note 54, at 72307–08.

[399] CAT Reporter means each national securities exchange, national securities association, and Industry Member that is required to record and report information to the Central Repository pursuant to SEC Rule 613(c). *See* CAT NMS Plan *supra* note 3, Section 1.1.

potentially allow affected CAT Reporters, the Participants, and the Commission to proactively respond to the information in a way to mitigate any potential harm to themselves, customers, investors, and the public. The Commission preliminarily believes that requiring breach notifications promptly after any responsible Plan Processor personnel have a reasonable basis to conclude that a systems or data breach has occurred should result in breach notifications that are not delayed for inappropriate reasons once the conclusion that a systems or data breach has occurred is made, but the proposed requirement would not require breach notifications to be prematurely released before Plan Processor personnel have adequate time to investigate potential systems or data breaches and consider whether or not such dissemination would likely compromise the security of the CAT System or an investigation of the systems or data breach.

Pursuant to proposed Appendix D, Section 4.1.5 of the CAT NMS Plan, these breach notifications would be required to include a summary description of the systems or data breach, including a description of the corrective action taken and when the systems or data breach was or is expected to be resolved. This requirement mirrors the information dissemination requirement in Rule 1002(c)(2) of Regulation SCI for systems intrusions. Notably, in contrast to other types of ''SCI events'' for which more detailed information is required to be disseminated, only summary descriptions are required for systems intrusions under Regulation SCI. The Commission recognizes that information relating to systems or data breaches in many cases may be sensitive and could raise security concerns, and thus preliminarily believes that it is appropriate that the required breach notifications be provided in a summary form. Even so, the proposal would still require a summary description of the systems or data breach, which would be required to describe the impacted data, and which must also include a description of the corrective action taken and when the systems or data breach has been or is expected to be resolved.

In addition, as proposed, the Plan Processor would be allowed to delay breach notifications ''if the Plan Processor determines that dissemination of such information would likely compromise the security of the CAT System or an investigation of the systems or data breach, and documents the reasons for such determination,'' which mirrors the similar provision in Rule 1002(c)(2) of Regulation SCI. The Commission preliminarily believes this proposed provision is appropriate so that breach notifications do not expose the CAT System to greater security risks or compromise an investigation into the breach. The proposal would require the affirmative documentation of the reasons for the Plan Processor's determination to delay a breach notification, which would help prevent the Plan Processor from improperly invoking this exception. In addition, the breach notification may only be temporarily, rather than indefinitely, delayed; once the reasons for the delay no longer apply, the Plan Processor must provide the appropriate breach notification to affected CAT Reporters, the Participants, and the Commission.

Finally, proposed Appendix D, Section 4.1.5 of the CAT NMS Plan would provide an exception to the requirement for breach notifications for systems or data breaches ''that the Plan Processor reasonably estimates would have no or a de minimis impact on the Plan Processor's operations or on market participants'' (''de minimis breach''), which also mirrors the Commission's approach relating to information dissemination for de minimis SCI events under Rule 1002(c) of Regulation SCI. Importantly, the Plan Processor would be required to document all information relevant to a breach the Plan Processor believes to be de minimis. The Plan Processor should have all the information necessary should its initial determination that a breach is de minimis prove to be incorrect, so that it could promptly provide breach notifications as required. In addition, maintaining documentation for all breaches, including de minimis breaches, would be helpful in identifying patterns among systems or data breaches.[400]

The Commission requests comment on the proposed amendments to the breach management policies and procedures. Specifically, the Commission solicits comment on the following:

166. Are the proposed modifications to the breach notification provision of the CAT NMS Plan necessary and appropriate? Should specific methods of notifying affected CAT Reporters, the Participants, and the Commission be required? Should specific corrective action measures be required, such as the provision of credit monitoring services to impacted parties or rotation of CCIDs in the event of a breach of CAT Data? If so, under what circumstances should such corrective actions be required?

167. Should the Plan Processor be required to provide breach notifications of systems or data breaches to CAT Reporters that it reasonably estimates may have been affected, as well as to the Participants and the Commission? Is it necessary and appropriate to require such breach notifications promptly after any responsible Plan Processor personnel have a reasonable basis to conclude that a systems or data breach has occurred? Should any disclosure to the public be required? For example, should breach notifications of systems or data breaches be reported by the Plan Processor on a publicly accessible website (such as the CAT NMS Plan website)? Should other requirements or direction regarding the breach notifications be adopted? Should there be an exception for de minimis breaches?

168. Is it reasonable to require that breach notifications be part of the formal cyber incident response plan? Should any currently optional items of the cyber incident response plan be required to be in the cyber incident response plan?

169. The proposed modifications to the breach notification provision of the CAT NMS Plan are modeled, in part, after Regulation SCI. Should other industry standards or objective criteria (*e.g.,* NIST) be used to determine when and how breach notifications will be required?

K. Firm Designated ID and Allocation Reports

Prior to approval of the CAT NMS Plan, the Commission granted exemptive relief to the SROs, for, among other things, relief related to allocations of orders.[401] Specifically, the Commission, pursuant to Section 36(a)(1) of the Act,[402] exempted the SROs from Rule 613(c)(7)(vi)(A),[403] which requires the Participants to require each CAT Reporter to record and report the account number for any subaccounts to which an execution is allocated. As a condition to this exemption, the SROs must require that

[400] Importantly, the proposed exception to breach notifications for de minimis breaches would apply specifically to the proposed breach notification requirement under the CAT NMS Plan. It would not apply to any obligations of the Plan Processor with respect to Regulation SCI, and thus, for example, would not obviate the need for the Plan Processor to immediately share information for all SCI events, including systems or data breaches that are systems intrusions, with those SCI SROs for which the CAT System is an SCI system and which themselves are independently subject to Regulation SCI.

[401] *See* Securities and Exchange Act Release No. 77265 (March 1, 2016), 81 FR 11856 (March 7, 2016) (''2016 Exemptive Order'').

[402] 15 U.S.C. 78mm(A)(1).

[403] 17 CFR 242.613(c)(7)(vi)(A).

(i) CAT Reporters submit an ''Allocation Report'' to the Central Repository, which would at minimum contain several elements, including the unique firm-designated identifier assigned by the broker-dealer of the relevant subaccount (*i.e.,* the Firm Designated ID), and (ii) the Central Repository be able to link the subaccount holder to those with authority to trade on behalf of the account.[404] This approach was incorporated in the CAT NMS Plan that was approved by the Commission.[405]

Under the Allocation Report approach there is no direct link in the Central Repository between the subaccounts to which an execution is allocated and the execution itself. Instead, CAT Reporters are required to report the Firm Designated ID of the relevant subaccount on an Allocation Report, which could be used by the Central Repository to link the subaccount holder to those with authority to trade on behalf of the account. However, the Commission believes that because the CAT NMS Plan does not currently explicitly require Customer and Account Attributes be reported for Firm Designated IDs that are submitted in Allocation Reports, as it does for Firm Designated IDs associated with the original receipt or origination of an order, there is a potential for confusion with regard to reporting requirements for Firm Designated IDs.

The Commission proposes to amend Section 6.4(d)(ii)(C) of the CAT NMS Plan to require that Customer and Account Attributes be reported for Firm Designated IDs submitted in connection with Allocation Reports, and not just for Firm Designated IDs submitted in connection with the original receipt or origination of an order. Specifically, the Commission proposes to amend Section 6.4(d)(ii)(C) of the CAT NMS Plan to state that each Participant shall, through its Compliance Rule, require its Industry Members to record and report, for original receipt or origination of an order and Allocation Reports, the Firm Designated ID for the relevant Customer, and in accordance with Section 6.4(d)(iv), Customer and Account Attributes for the relevant Customer.

The Commission believes that if Industry Members do not provide Customer and Account Attributes for the relevant Firm Designated ID submitted in an Allocation Report, then there would be no ability for the Central Repository to link the subaccount holder to those with authority to trade on behalf of the account. The Commission preliminarily believes that amending the language in Section 6.4(d)(ii)(C) to implement the previously approved exemptive relief is appropriate.

In addition, the Commission believes that these proposed amendments do not substantively change the obligations of Industry Members, who, through Participant Compliance Rules, are already required to submit customer information for all Active Accounts pursuant to the CAT NMS Plan.[406] Specifically, Section 6.5(d)(iv) states that Participant Compliance Rules must require Industry Members to, among other things, submit an initial set of Customer information required in Section 6.4(d)(ii)(C) for Active Accounts to the Central Repository upon the Industry Member's commencement of reporting, and submit updates, additions or other changes on a daily basis for all Active Accounts. Active Accounts are defined as ''an account that has activity in Eligible Securities within the last six months,'' and the Commission believes that ''activity'' would include the allocation of shares to an account, reflected in Allocation Reports.[407] Thus, Section 6.5(d)(iv) already requires the information required by proposed Section 6.4(d)(ii)(C), but the Commission preliminarily believes that amending the language in Section 6.4(d)(ii)(C) would help avoid confusion regarding when Customer and Account Attributes are required to be submitted for Firm Designated IDs.

170. Is it reasonable and appropriate to clarify that Industry Members, for Allocation Reports, are required to report the Firm Designated ID for the relevant Customer, and in accordance with Section 6.4(d)(iv) of the CAT NMS Plan, Customer Account Information and Customer Identifying Information for the relevant Customer?

L. Appendix C of the CAT NMS Plan

Rule 613(a)[408] required the Participants to discuss various considerations related to how the Participants propose to implement the requirements of the CAT NMS Plan, cost estimates for the proposed solution, and the costs and benefits of alternate solutions considered but not proposed.[409] Appendix C of the CAT NMS Plan generally contains a discussion of the considerations enumerated in Rule 613,[410] which were required to be addressed when the CAT NMS Plan was filed with the Commission, prior to becoming effective.[411] The Rule 613 Adopting Release stated that the additional information and analysis generated by discussing these considerations was intended to ensure that the Commission and the Participants had sufficiently detailed information to carefully consider all aspects of the NMS plan that would ultimately be submitted by the Participants.[412] Therefore the Commission believes that the discussion of these considerations was not intended to be continually updated once the CAT NMS Plan was approved.[413] However, in addition to the discussion of considerations, Appendix C of the CAT NMS Plan also contains provisions such as those that set forth objective milestones with required completion dates to assess the Participants' progress toward the implementation of the CAT.[414] Therefore, the Commission proposes to amend Appendix C of the CAT NMS Plan to insert introductory language to clarify that Appendix C has not been updated to reflect subsequent amendments to the CAT NMS Plan and Appendix D.[415]

M. Proposed Implementation

As discussed below, the Commission proposes to allow additional time beyond the effective date for the Participants to comply with certain requirements in the proposed amendments.

1. Proposed 90-Day Implementation Period

The Commission proposes that requirements related to developing and implementing certain policies and procedures, design specifications, and changes to logging in the proposed amendments must be met no later than

[404] *See* 2016 Exemptive Order, *supra* note 401, at 11868.

[405] *See, e.g.,* CAT NMS Plan, *supra* note 3, at Section 1.1 (defining ''Allocation Report'') and Section 6.4(d)(ii)(A)(i) (requiring an Allocation Report if an order is executed in whole in or in part).

[406] *See* CAT NMS Plan, *supra* note 3, at Section 6.4(d)(ii)(C).

[407] Section 6.5(d)(iv) of the CAT NMS Plan was amended in the CAT NMS Plan Approval Order ''to clarify that each Industry Member must submit an initial set of customer information for Active Accounts at the commencement of reporting to the Central Repository, as well as any updates, additions, or other changes in customer information, including any such customer information for any new Active Accounts.'' *See* CAT NMS Plan Approval Order, *supra* note 3, at 84868–69.

[408] 17 CFR 242.613(a).

[409] *See* Rule 613 Adopting Release, *supra* note 2, at 45789.

[410] 17 CFR 242.613(a)(1).

[411] *See* Rule 613 Adopting Release, *supra* note 2, at 45789–90.

[412] *See id.*

[413] *See id.* The CAT NMS Plan was approved on November 15, 2016. *See supra* note 3.

[414] *See* Appendix C of the CAT NMS Plan, at Section C.10.

[415] *See* proposed Appendix C.

90 days from the effective date of the amendment. Specifically, the Commission believes that this timeframe would provide sufficient time for the Participants to collectively develop and approve the Proposed Confidentiality Policies [416] pursuant to proposed Section 6.5(g)(i), 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 [417] pursuant to proposed Sections 6.12 and 6.13(a), and to develop detailed design specifications for the SAWs [418] pursuant to proposed Section 6.13(b), 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. 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.

2. Proposed 120-Day Implementation Period

The Commission proposes that requirements related to the Plan Processor providing the SAWs to Participants [419] contained in proposed Section 6.1(d)(v) must be met no later than 120 days from the effective date of the amendment. The Commission believes that this timeframe would provide sufficient time for the Plan Processor to establish the Participants' SAWs because the Plan Processor has already been authorized to build similar environments for some of the Participants since November 2019.[420] In addition, 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, the Plan Processor will already have achieved interim elements of SAW implementation.

3. Proposed 180-Day Implementation Period

The Commission proposes that requirements related to the Participants complying with SAW access and usage [421] pursuant to proposed Section 6.13(a), or having received an exception,[422] pursuant to proposed Section 6.13(d), must be met no later than 180 days from the effective date of the amendment. The Commission believes that this timeframe would provide sufficient time 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. The Commission also believes that this timeframe would provide sufficient time for Participants seeking an exception from the requirement to use the SAW to access CAT Data through the user-defined direct query and bulk extract tools to go through the required process. Specifically, these Participants would have 30 days after the SAW design specifications have been provided to prepare their application materials for submission to the Plan Processor's CISO, CCO, and the Security Working Group. Then, the CISO and CCO would be required to issue a determination to the requesting Participant within 60 days of receiving the application materials, with the result that the requesting Participant should have a response by the compliance date 180 days from the effective date of the amendment.

The Commission requests comment on the proposed implementation timeframes. Specifically, the Commission solicits comment on the following:

171. Does the proposed 90-day implementation period with respect to the requirement for the Participants to develop and approve the Proposed Confidentiality Policies strike an appropriate balance between timely implementation and the time needed for the Participants to develop these policies and related procedures?

172. Does the proposed 90-day implementation period with respect to the requirement for the Plan Processor to implement SAW-specific policies and procedures for the CISP and to develop detailed design specifications for the SAWs strike an appropriate balance between timely implementation and the time needed for the Plan Processor to complete these tasks? Does the proposed 90-day implementation period with respect to the requirement for the Plan Processor to make programming changes to implement the new logging requirements strike an appropriate balance between timely implementation and the time needed for the Plan Processor to complete the necessary coding to its systems?

173. Does the proposed 120-day implementation period with respect to the requirement for the Plan Processor to provide the SAWs to Participants strike an appropriate balance between timely implementation and the time needed for the Plan Processor to achieve implementation of the SAWs?

174. Does the proposed 180-day implementation period with respect to the requirements for the Participants to either comply with SAW access and usage, or receive an exception, strike an appropriate balance between timely implementation and the time needed for the Participants to either complete their components of the SAW, or seek and receive an exception from the CISO and CCO?

N. Application of the Proposed Amendments to Commission Staff

The Commission takes very seriously concerns about maintaining the security and confidentiality of CAT Data and believes that it is imperative that all CAT users, including the Commission, implement and maintain a robust security framework with appropriate safeguards to ensure that CAT Data is kept confidential and used only for surveillance and regulatory purposes. However, the Commission is not a party to the CAT NMS Plan.[423] By statute, the Commission is the regulator of the Participants, and the Commission oversees and enforces their compliance with the CAT NMS Plan.[424] To 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.[425] 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. Accordingly, the Commission is not including its staff within the definition of Regulatory Staff in the proposed amendments. Rather, the obligations of the Commission and

[416] *See* Part II.G.1–2 *supra.*

[417] *See* Part II.C.2–3 *supra.*

[418] *See* Part II.C.4 *supra.*

[419] *See* Part II.C.2 *supra.*

[420] *See supra* note 52 and accompanying text.

[421] *See* Parts II.C.2 and II.C.4 *supra.*

[422] *See* Part II.C.5 *supra.*

[423] *See* 17 CFR 242.608(a)(1) (stating that NMS plans are filed by two or more SROs).

[424] *See* 17 CFR 242.608(b)(2), (c), (d); 17 CFR 242.613(b).

[425] *See* CAT NMS Plan Approval Order, *supra* note 3, at 84764–65.

its personnel with respect to the security and confidentiality of CAT Data should be reflected through different mechanisms from those of the Participants. The Commission reiterates that in each instance the purpose of excluding Commission personnel from these provisions is not to subject the Commission or its personnel to more lenient data security or confidentiality standards. Despite these differences in the origins of their respective obligations, the rules and policies applicable to the Commission and its personnel will be comparable to those applicable to the Participants and their personnel.[426]

Consistent with the CAT Approval Order,[427] a cross-divisional steering committee of senior Commission Staff was formed that has designed and continue to maintain comparable policies and procedures regarding Commission and Commission Staff access to, use of, and protection of CAT Data. These policies and procedures also must comply with the Federal Information Security Modernization Act of 2014 and the NIST standards required thereunder,[428] and are subject to audits by the SEC Office of Inspector General and the Government Accountability Office. The Commission will review and update, as necessary, its existing confidentiality and data use policies and procedures to account for access to the CAT, and, like the Participants, will periodically review the effectiveness of these policies and procedures and take prompt action to remedy deficiencies in such policies and procedures.

For example, with respect to restrictions on the use of Manual and Programmatic CCID Subsystem and CAIS Access, the Commission intends to have comparable policies and restrictions as the Participants but as adopted and enforced by the Commission. In addition, under the restrictions set forth in the proposed amendments, Commission personnel would also be permitted to extract only the minimum amount of CAT Data necessary to achieve a specific surveillance or regulatory purpose—which could include supporting discussions with a regulated entity regarding activity that raises concerns, filing a complaint against a regulated entity, or supporting an investigation or examination of a regulated entity. Consistent with what the Commission stated when the CAT NMS Plan was approved, the Commission will ensure that its policies and procedures impose protections upon itself and its personnel that are comparable to those required under the proposed 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.[429]

III. Paperwork Reduction Act

As discussed above, the Commission is proposing to make various changes to the CAT NMS Plan, and certain provisions of the proposed amendment contain ''collection of information requirements'' within the meaning of the Paperwork Reduction Act of 1995 (''PRA'').[430] The Commission is requesting public comment on the new collection of information requirements in this proposed amendment to the CAT NMS Plan. The Commission is submitting these collections of information to the Office of Management and Budget (''OMB'') for review in accordance with 44 U.S.C. 3507(d) and 5 CFR 1320.11.[431] An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the agency displays a currently valid control number.[432] The title of the new collection of information is ''CAT NMS Plan Data Security Amendments.''

A. Summary of Collections of Information

The proposed amendments to the CAT NMS Plan include several obligations that would require a collection of information within the meaning of the PRA.

1. Evaluation of the CISP

The CAT NMS Plan currently requires the CCO to oversee the regular written assessment of the Plan Processor's performance, which must be provided to the Commission at least annually and which must include an evaluation of the existing information security program ''to ensure that the program is consistent with the highest industry standards for the protection of data.'' [433] The proposed amendments would require the CCO to evaluate the newly-defined CISP. This change would newly require the CCO to evaluate elements of the CISP that relate to the SAWs provided by the Plan Processor.[434] The proposed amendments would also require the CCO, in collaboration with the CISO, to include in this evaluation a review 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 to identify any appropriate corrective measures.[435] The Participants, under the existing provisions of the CAT NMS Plan, would be entitled to review and comment on these new elements of the written assessment of the Plan Processor's performance.[436]

2. Security Working Group

The proposed amendments would require the Security Working Group 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 security 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.[437] The proposed amendments would also require the CISO to apprise the Security Working Group of relevant developments and to provide it with all

[426] *See id.* at 84765. In addition, Commission and SEC staff are subject to federal and Commission rules and policies that address security and confidentiality obligations. For example, disclosure or misuse of CAT Data would potentially subject Commission personnel to criminal penalties (including fines and imprisonment), disciplinary action (including termination of employment), civil injunction, and censure by professional associations for attorneys and accountants. *Id.*

[427] *See id.* at 84765.

[428] *See id. See also* Public Law 113–283 (Dec. 18, 2014); NIST, Security and Privacy Controls for Federal Information Systems and Organizations, Special Publication 800–53, revision 4 (Gaithersburg, Md.: April 2013); NIST, Contingency Planning Guide for Federal Information Systems, Special Publication 800–34, revision 1 (Gaithersburg, Md.: May 2010).

[429] *See id.* at 84765–66.

[430] 44 U.S.C. 3501 *et seq.*

[431] 44 U.S.C. 3507; 5 CFR 1320.11.

[432] 5 CFR 1320.11(l).

[433] *See* Section 6.6(b)(i)(A)–(B); Section 6.6(b)(ii)(B)(3).

[434] *See id.; see also* proposed Section 1.1, definition of ''Comprehensive Information Security Program'' and ''Secure Analytical Workspace.'' The Commission preliminarily believes that all other elements of the CISP are currently required by the CAT NMS Plan.

[435] *See* proposed Section 6.6(b)(ii)(B)(3). These requirements are also enshrined in proposed Section 6.2. *See also* proposed Section 6.2(a)(v)(T) (requiring the CCO to determine, pursuant to Section 6.6(b)(ii)(B)(3), to review CAT Data that has been extracted from the CAT System to assess the security risk of allowing such CAT Data to be extracted); proposed Section 6.2(b)(x) (requiring the CISO to determine, pursuant to Section 6.6(b)(ii)(B)(3), to review CAT Data that has been extracted from the CAT System to assess the security risk of allowing such CAT Data to be extracted).

[436] *See* CAT NMS Plan, *supra* note 3, at Section 6.6(b)(i)(B).

[437] *See* proposed Section 4.12(c).

information and materials necessary to fulfill its purpose.[438]

3. SAWs

There are a number of information collections related to the proposed SAW requirements, including collections related to the following categories: (a) Policies, Procedures, and Detailed Design Specifications; (b) Implementation and Operation Requirements; and (c) Non-SAW Environment Requirements. These collections are explained in more detail below.

a. Policies, Procedures, and Detailed Design Specifications

The proposed definition for the CISP would define the scope of the existing information security program. However, the proposed amendments would add one new element to this information security program or CISP—the SAWs provided by the Plan Processor.[439] The proposed amendments would therefore require the Plan Processor to develop and maintain a CISP that would include SAWs[440] and, more specifically, that would include data access and extraction policies and procedures and security controls, policies, and procedures for SAWs.[441]

In addition, the proposed amendments would require the Plan Processor to develop, maintain, and make available to the Participants detailed design specifications for the technical implementation of the access, monitoring, and other controls required for SAWs by the CISP.

b. Implementation and Operation Requirements

The proposed amendments would require the Plan Processor to notify the Operating Committee that each Participant's SAW has achieved compliance with the detailed design specifications required by proposed Section 6.13(b)(i) before that SAW may connect to the Central Repository.[442]

The proposed amendments would also require the Plan Processor to monitor each Participant's SAW in accordance with the detailed design specifications developed pursuant to proposed Section 6.13(b)(i), for compliance with the CISP and the detailed design specifications only, and to notify the Participant of any identified non-compliance with the CISP or the detailed design specifications.[443]

c. Non-SAW Environments

There are a number of information collections related to the proposed requirements for non-SAW environments, including collections related to the following categories: (i) Application Materials; (ii) Exception Determinations; and (iii) Non-SAW Implementation and Operation Requirements. These collections are explained in more detail below.

i. Application Materials

The proposed amendments would require the Participant requesting an exception from the proposed SAW usage requirements to provide the CISO, the CCO, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group with various application materials. First, the Participant would be required to provide a security assessment of the non-SAW environment, conducted within the prior twelve 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 pursuant to Section 6.13(a)(ii), (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 the user-defined direct query or bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2 of the CAT NMS Plan, and (c) includes a Plan of Action and Milestones document detailing the status and schedule of any corrective actions recommended by the assessment.[444] Second, the Participant would be required to provide 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 proposed Section 6.13(b)(i), and (b) that the design specifications will enable the operational requirements set forth for non-SAW environments in proposed Section 6.13(d)(iii), which include, among other things, Plan Processor monitoring.[445]

Under the proposed amendments, Participants who are denied an exception or who want to apply for a continuance must submit a new security assessment that complies with the requirements of proposed Section 6.13(d)(i)(A)(1) and up-to-date versions of the materials required by proposed Section 6.13(d)(i)(A)(2).[446]

ii. Exception and Revocation Determinations

The proposed amendments would require the CISO and the CCO to review initial application materials submitted by requesting Participants, in accordance with policies and procedures developed by the Plan Processor, and to simultaneously notify the Operating Committee and the requesting Participant of their determination.[447] If the exception is granted, the proposed amendments would require the CISO and the CCO to provide the requesting Participant with a detailed written explanation setting forth the reasons for that determination.[448] For applications that are denied, the proposed amendments would require the CISO and the CCO to specifically identify the deficiencies that must be remedied before an exception could be granted.[449] The proposed amendments would also require the CISO and the CCO to follow the same procedures when reviewing applications for a continued exception and issuing determinations regarding those applications.[450]

For Participants that are denied a continuance, or for Participants that fail to submit the proper application materials, the CISO and the CCO would also be required to revoke the exception and require such Participants to cease using their non-SAW environments to access CAT Data through the user-defined direct query and bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2 of the CAT NMS Plan, in accordance with the remediation timeframes developed by the Plan Processor.[451]

iii. Non-SAW Implementation and Operation Requirements

The proposed amendments would prevent an approved Participant from employing a non-SAW environment to access CAT Data through the user-

[438] *See id.*

[439] *See* proposed Section 1.1, definition of ''Comprehensive Information Security Program'' and ''Secure Analytical Workspace.''

[440] *See* proposed Section 6.12. The Commission preliminarily believes that all other elements of the CISP are currently required by the CAT NMS Plan.

[441] *See* proposed Section 6.13(a).

[442] *See* proposed Section 6.13(b)(ii).

[443] *See* proposed Section 6.13(c)(i).

[444] *See* proposed Section 6.13(d)(i)(A)(1).

[445] *See* proposed Section 6.13(d)(i)(A)(2).

[446] *See* proposed Section 6.13(d)(i)(C), (d)(ii)(C).

[447] *See* proposed Section 6.13(d)(i)(B).

[448] *See* proposed Section 6.13(d)(i)(B)(1).

[449] *See* proposed Section 6.13(d)(i)(B)(2).

[450] *See* proposed Section 6.13(d)(ii)(B).

[451] *See* proposed Section 6.13(d)(ii)(A), (C).

defined direct query or bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2 until the Plan Processor notifies the Operating Committee that the non-SAW environment has achieved compliance with the detailed design specifications submitted by that Participant as part of its application for an exception (or continuance).[452]

The proposed amendments would also require the Plan Processor to monitor the non-SAW environment in accordance with the detailed design specifications submitted with the exception (or continuance) application, for compliance with those detailed design specifications only, and to notify the Participant of any identified non-compliance with such detailed design specifications.[453] Furthermore, the proposed amendments would require the Participant to simultaneously notify the Plan Processor, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group of any material changes to its security controls for the non-SAW environment.[454]

4. Online Targeted Query Tool and Logging of Access and Extraction

The CAT NMS Plan currently requires the targeted online query tool to log submitted queries, query parameters, the user ID of the submitter, the date and time of the submission, and the delivery of results.[455] The CAT NMS Plan further requires that the Plan Processor provides monthly reports based on this information to each Participant and the SEC of its respective metrics on query performance and data usage, and that the Operating Committee receive the monthly reports to review items, including user usage and system processing performance. The Commission proposes to modify these requirements by defining the term ''delivery of results'' as ''the number of records in the result(s) and the time it took for the query to be performed'' and requiring that access and extraction of CAT Data be logged.[456] This change would also require the same logging of access and extraction of CAT Data from the user-defined direct queries and bulk extraction tools.

5. CAT Customer and Account Attributes

The CAT NMS Plan currently requires that Industry Members report a Customer's SSN or ITIN as part of the information necessary for the Plan Processor to create a Customer-ID.[457] The Commission is proposing to amend the Plan to modify the information that Industry Members must report to CAT to be consistent with the CCID Alternative for creating Customer-IDs outlined in the PII Exemption Request and the PII Exemption Order. First, in lieu of reporting a Customer's SSN or ITIN to CAT, the Commission is proposing that Industry Members would use the CCID Transformation Logic[458] in conjunction with an API provided by the Plan Processor to transform their Customer's SSN/ITIN using the CCID Transformation Logic to create a Transformed Value and then report that Transformed Value to the CCID Subsystem.[459] Once the Transformed Value is reported to the CCID Subsystem, the CCID Subsystem would perform another transformation of the Transformed Value to create a globally unique Customer-ID for each Customer.

The CAT NMS Plan currently requires the CCO to oversee the Regular Written Assessment of the Plan Processor's performance, which must be provided to the Commission at least annually and which must include an evaluation of the performance of the CAT.[460] As proposed, the overall performance and design of the CCID Subsystem and the process for creating Customer-ID(s) must be included in the annual Regular Written Assessment of the Plan Processor, as required by Article VI, Section 6.6(b)(ii)(A).

6. Customer Identifying Systems Workflow

The CAT NMS Plan currently requires Industry Members to report PII[461] to the CAT, and states that such ''PII can be gathered using the 'PII workflow' described in Appendix D, Data Security, PII Data Requirements.''[462] However, the ''PII workflow'' was neither defined nor established in the CAT NMS Plan.[463] The Commission is therefore proposing to amend the CAT NMS Plan to define the PII workflow for accessing Customer and Account Attributes, and to apply the existing provisions of the CAT NMS Plan to Customer and Account Attributes going forward.[464]

The current CAT NMS Plan requires that a full audit trail of PII access (who accessed what data, and when) be maintained, and that the CCO and the CISO have access to daily PII reports that list all users who are entitled to PII access, as well as the audit trail of all PII access that has occurred for the day.[465] The Commission is proposing to amend the Plan to require that the Plan Processor maintain a full audit trail of access to Customer Identifying Systems by each Participant and the Commission (who accessed what data within each Participant, and when), and to require that the Plan Processor provide to each Participant and the Commission the audit trail for their respective users on a monthly basis. The CCO and the CISO will continue to have access to daily reports that list all users who are entitled to Customer Identifying Systems access, as is the case today; however, the Commission is proposing that such reports also be provided to the Operating Committee on a monthly basis.[466]

The proposed Customer Identifying Systems Workflow would permit regulators to use Programmatic CAIS Access or Programmatic CCID Subsystem Access to query those databases. The Commission is proposing to require that each Participant submit an application that has been approved by the Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation) to the Commission for authorization to use Programmatic CAIS Access or Programmatic CCID Subsystem Access if a Participant requires programmatic access. The application must explain:

- Which programmatic access is being requested: Programmatic CAIS Access and/or Programmatic CCID Subsystem Access;
- Why Programmatic CAIS Access or Programmatic CCID Subsystem is required, and why Manual CAIS Access or Manual CCID Subsystem Access cannot achieve the regulatory purpose of an inquiry or set of inquiries;
- The Participant's rules that require Programmatic Access for surveillance and regulatory purposes;
- The regulatory purpose of the inquiry or set of inquires requiring programmatic access;

[452] *See* proposed Section 6.13(d)(iii)(A).

[453] *See* proposed Section 6.13(d)(iii)(B).

[454] *See* proposed Section 6.13(d)(iii)(C).

[455] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 8.1.1.

[456] *See* proposed Appendix D, Section 8.1.1.

[457] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 9.1

[458] The Commission is proposing that the CCID Transformation Logic will be embedded in the CAT Reporter Portal or used by the Industry Member in machine-to machine-processing. *See* proposed Appendix D, Section 9.1.

[459] *See* proposed Section 6.4(D)(ii)(d), Appendix D, Section 9.1 and 9.2. *See also* notes 168–173, *supra* and accompanying text.

[460] *See* CAT NMS Plan, *supra* note 3, Section 6.6(b)(ii)(A).

[461] *See supra* note 10.

[462] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 4.1.6.

[463] *Id.*

[464] *See* Part II.F., *supra* and accompanying text for a complete description of the Customer Identifying Systems Workflow.

[465] *See* CAT NMS Plan, *supra* note 3, Appendix D, Section 4.1.6 (PII Data Requirements).

[466] *See* proposed Appendix D, Section 4.1.6.

• A detailed description of the functionality of the Participant's SAW system(s) that will use data from CAIS or the CCID Subsystem;
• A system diagram and description indicating architecture and access controls to the Participant's SAW system(s) that will use data from CAIS or the CCID Subsystem; and
• The expected number of users of the Participant's system(s) that will use data from CAIS or the CCID Subsystem.

7. Proposed Confidentiality Policies, Procedures and Usage Restrictions

The Commission is proposing to amend Section 6.5(g)(i) of the CAT NMS Plan to require the Participants to create and maintain identical confidentiality and related policies (''Proposed Confidentiality Policies''). Proposed Section 6.5(g)(i) would require each Participant to establish, maintain and enforce procedures and usage restriction controls in accordance with the Proposed Confidentiality Policies. As proposed, the Proposed Confidentiality Policies must: (i) Be reasonably designed to (1) ensure the confidentiality of the CAT Data; and (2) limit the use of CAT Data to solely surveillance and regulatory purposes; (ii) limit extraction of CAT Data to the minimum amount of data necessary to achieve a specific surveillance or regulatory purpose; (iii) limit access to CAT Data to persons designated by Participants, who must be (1) Regulatory Staff or (2) technology and operations staff that require access solely to facilitate access to and usage of the CAT Data by Regulatory Staff;[467] (iv) implement effective information barriers between such Participants' Regulatory Staff and non-Regulatory Staff with regard to access and use of CAT Data; (v) limit access to CAT Data by non-Regulatory Staff, by allowing such access only where there is a specific regulatory need for such access and requiring that a Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation), or his or her designee, document his or her written approval of each instance of access by non-Regulatory Staff; (vi) require that, in the absence of exigent circumstances, all Participant staff who are provided access to CAT Data, or have been provided access to CAT Data, must (1) sign a ''Safeguard of Information'' affidavit as approved by the Operating Committee pursuant to Section 6.5(f)(i)(B); and (2) participate in the training program developed by the Plan Processor that addresses the security and confidentiality of information accessible in the CAT pursuant to Section 6.1(m); (vii) define the individual roles and regulatory activities of specific users; (viii) impose penalties for staff non-compliance with Participants' or the Plan Processor's policies or procedures with respect to information security, including, the policies required by Section 6.5(g)(i); (ix) be reasonably designed to implement and satisfy the Customer and Account Attributes data requirements of Section 4.1.6 of Appendix D such that Participants must be able to demonstrate that a Participant's ongoing use of Programmatic CAIS and/or CCID Subsystem access is in accordance with the Customer Identifying Systems Workflow; and (x) document monitoring and testing protocols that will be used to assess Participant compliance with the policies.

Proposed Section 6.5(g)(ii) would require the Participant to periodically review the effectiveness of the policies and procedures and usage restriction controls required by Section 6.5(g)(i), including by using the monitoring and testing protocols documented within the policies pursuant to Section 6.5(g)(i)(J), and take prompt action to remedy deficiencies in such policies, procedures and usage restriction controls. In addition, proposed Section 6.5(g)(iii) would require that each Participant, as reasonably practicable, and in any event within 24 hours of becoming aware, report to the Chief Compliance Officer, in accordance with the guidance provided by the Operating Committee: (A) any instance of noncompliance with the policies, procedures, and usage restriction controls adopted by such Participant pursuant to Section 6.5(g)(i); or (B) a breach of the security of the CAT.

Proposed Section 6.5(g)(iv) would require that that the Proposed Confidentiality Policies be made publicly available on each of the Participants' websites, or collectively on the CAT NMS Plan website, redacted of sensitive proprietary information.[468]

Proposed Section 6.5(g)(v) would require that, on an annual basis, each Participant engage an independent accountant to perform an examination of compliance with the policies required by Section 6.5(g)(i) in accordance with attestation standards of the American Institute of Certified Public Accountants (''AICPA'') (referred to as U.S. Generally Accepted Auditing Standards or GAAS) or the Public Company Accounting Oversight Board (''PCAOB''), and with Commission independence standards based on SEC Rule 2–01 of Regulation S–X.[469] In addition, the examination results shall be submitted to the Commission upon completion, in a text-searchable format (*e.g.* a text-searchable PDF). The examination report shall be considered submitted to the Commission when electronically received by Commission staff at the Commission's principal office in Washington DC.[470]

The Commission proposes Sections 6.2(a)(v)(R) and 6.2(b)(viii) in the CAT NMS Plan to require that both the CISO and CCO of the Plan Processor be required to review the Proposed Confidentiality Policies. In addition, the Commission proposes to require that the CCO of the Plan obtain assistance and input from the Compliance Subcommittee,[471] and require that the policies required by proposed Section 6.5(g)(i) of the CAT NMS Plan be subject to review and approval by the Operating Committee, after review by the CISO and CCO.[472]

8. Secure Connectivity—''Allow Listing''

The Commission is proposing to amend Appendix D, Section 4.1.1 of the CAT NMS Plan to require ''allow listing.'' Specifically, the Commission proposes 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.

9. Breach Management Policies and Procedures

Appendix D, Section 4.1.5 of the CAT NMS Plan requires the Plan Processor to

[467] The Commission proposes to define Regulatory Staff as the Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation) and staff within the Chief Regulatory Officer's (or similarly designated head(s) of regulation's) reporting line. *See* proposed Section 1.1.

[468] *See* proposed Section 6.5(g)(iv).

[469] *See* 17 CFR 210.2–01.

[470] *See* proposed Section 6.5(g)(v).

[471] *See* proposed Section 6.2(a)(v)(R). The CAT NMS Plan requires the Operating Committee to maintain a compliance Subcommittee (the ''Compliance Subcommittee'') whose purpose shall be to aid the Chief Compliance Officer as necessary. *See* CAT NMS Plan, *supra* note 3, at Section 4.12(b).

[472] *See* proposed Section 6.5(g)(vi).

develop policies and procedures governing its responses to systems or data breaches, including a formal cyber incident response plan, and documentation of all information relevant to breaches.[473] The CAT NMS Plan further specifies that the cyber incident response plan will provide guidance and direction during security incidents, but otherwise states that the cyber incident response plan *may* include several items.[474] The Commission proposes to require that the formal cyber incident response plan incorporate corrective actions and breach notifications.[475]

Specifically, the Commission is proposing to modify Appendix D, Section 4.1.5 of the CAT NMS Plan to require that the formal cyber incident response plan must include ''taking appropriate corrective action that includes, at a minimum, mitigating potential harm to investors and market integrity, and devoting adequate resources to remedy the systems or data breach as soon as reasonably practicable.'' In addition, the Commission is proposing to modify Appendix D, Section 4.1.5 of the CAT NMS Plan to require the Plan Processor to provide breach notifications of systems or data breaches to CAT Reporters that it reasonably estimates may have been affected, as well as to the Participants and the Commission, promptly after any responsible Plan Processor personnel have a reasonable basis to conclude that a systems or data breach has occurred. The Commission also proposes to state that the cyber incident response plan must provide for breach notifications. As proposed, these breach notifications would be required to include a summary description of the systems or data breach, including a description of the corrective action taken and when the systems or data breach has been or is expected to be resolved.

As proposed, the Plan Processor would be allowed to delay breach notifications ''if the Plan Processor determines that dissemination of such information would likely compromise the security of the CAT System or an investigation of the systems or data breach, and documents the reasons for such determination.'' The proposal would further require affirmative documentation of the reasons for the Plan Processor's determination to delay a breach notification. In addition, breach notifications would not be required for systems or data breaches ''that the Plan Processor reasonably estimates would have no or a de minimis impact on the Plan Processor's operations or on market participants.'' [476] For a breach that the Plan Processor believes to be a de minimis breach, the Plan Processor would be required to document all information relevant to such breach.

10. Customer Information for Allocation Report Firm Designated IDs

Proposed Section 6.4(d)(ii)(C) would explicitly require that Customer and Account Attributes be reported for Firm Designated IDs submitted in connection with Allocation Reports, and not just for Firm Designated IDs submitted in connection with the original receipt or origination of an order. Specifically, proposed Section 6.4(d)(ii)(C), as amended, of the CAT NMS Plan would state that each Participant shall, through its Compliance Rule, require its Industry Members to record and report, for original receipt or origination of an order and Allocation Reports, the Firm Designated ID for the relevant Customer, and in accordance with Section 6.4(d)(iv), Customer and Account Attributes for the relevant Customer.

B. Proposed Use of Information

1. Evaluation of the CISP

The Commission preliminarily believes that the proposed review of CAT Data extracted from the CAT System will facilitate Commission oversight of the security risks posed by the extraction of CAT Data. The proposed review would be part of the evaluation of the CISP attached by the Participants to the written assessment of the Plan Processor's performance and provided to the Commission at least annually.[477] The Commission preliminarily believes the proposed review should enable the Commission to better assess whether the current security measures should be enhanced or lightened and whether any planned corrective measures are appropriate. The proposed amendments require the CCO to evaluate the CISP, which includes SAWs, and the evaluation would be included in the regular written assessment.

2. Security Working Group

The proposed amendments require the CISO to keep the Security Working Group apprised of relevant developments, and to provide it with all information and materials necessary to fulfill its purpose, which will help to keep the Security Working Group adequately informed about issues that fall within its purview. The Commission further preliminarily believes that the Security Working Group will be able to provide the CISO and the Operating Committee with valuable feedback regarding the security of the CAT.

3. SAWs

a. Policies, Procedures, and Detailed Design Specifications

By requiring the Plan Processor to develop and maintain a CISP that would include SAWs and, more specifically, that will include specified data access and extraction policies and procedures and security controls, policies, and procedures for SAWs, the Commission preliminarily believes that the proposed amendments would better protect CAT Data by keeping it within the CAT System and therefore subject to the security controls, policies, and procedures of the CISP when accessed and analyzed by the Participants. In addition, the Commission preliminarily believes that requiring the Plan Processor to develop, maintain, and make available to the Participants detailed design specifications for the technical implementation of the access, monitoring, and other controls required for SAWs may increase the likelihood that the CISP is implemented consistently across the SAWs and at a high standard.

b. Implementation and Operation Requirements

Requiring the Plan Processor to notify the Operating Committee that each Participant's SAW has achieved compliance with the detailed design specifications developed pursuant to proposed Section 6.13(b)(i) before that SAW may connect to the Central Repository will protect the CAT, because this process will confirm that the CISP has been implemented properly before any Participant is permitted to use its SAW to access CAT Data.

Requiring the Plan Processor to monitor each Participant's SAW in accordance with the detailed design specifications developed pursuant to proposed Section 6.13(b)(i) should enable the Plan Processor to conduct such monitoring, including automated monitoring, consistently and efficiently across SAWs. It should also help the Plan Processor to identify and to escalate any non-compliance events,

[473] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 4.1.5. The cyber incident response plan is subject to review by the Operating Committee. *See id.*

[474] *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 4.1.5. The CAT NMS Plan also lists a series of items that documentation of information relevant to breaches should include. *Id.*

[475] *See supra* Part II.J.

[476] *See* proposed Appendix D, Section 4.1.5.

[477] *See* Section 6.6(b)(ii)(B)(3).

threats, and/or vulnerabilities as soon as possible, thus reducing the potentially harmful effects of these matters. Likewise, requiring the Plan Processor to notify the Participant of any identified non-compliance will likely speed remediation of such non-compliance by the Participant.

c. Non-SAW Environments

i. Application Materials

The Commission preliminarily believes that requiring the Participants to submit new and/or up-to-date versions of the specified application materials in connection with an initial application, a re-application, or a continuance will help the CISO and the CCO to determine whether it is appropriate to grant an exception (or continuance) to the proposed SAW usage requirements. For example, the proposed requirement that the Participant produce a security assessment conducted within the last twelve months by an independent and named third party security assessor should give these decision-makers access to up-to-date, accurate, and unbiased information about the security and privacy controls put in place for the relevant non-SAW environment, including reliable information about risk mitigation measures and recommended corrective actions.[478] The Commission preliminarily believes that this information will help the CISO and the CCO to determine whether the non-SAW environment is sufficiently secure to be granted an exception (or continuance) from the SAW usage requirements set forth in proposed Section 6.13(a)(i)(B). Similarly, the Commission preliminarily believes that requiring the requesting Participant to provide detailed design specifications for its non-SAW environment that demonstrate the extent of adherence to the SAW design specifications developed by the Plan Processor pursuant to Section 6.13(b)(i) and that the detailed design specifications will support required non-SAW environment operations will help the CISO and the CCO to assess the security-related infrastructure of the non-SAW environment and to determine whether the non-SAW environment will support the required functionality.

ii. Exception and Revocation Determinations

For both initial applications and applications for a continued exception, the proposed amendments would require the CISO and the CCO to notify the Operating Committee and the requesting Participant and to provide the Participant with a detailed written explanation setting forth the reasons for their determination and, for denied Participants, specifically identifying the deficiencies that must be remedied before an exception could be granted. The Commission preliminarily believes that this kind of feedback could be quite valuable—not only because it should prevent the CISO and the CCO from denying applications without basis, but also because it should provide denied Participants with the information needed to effectively bring their non-SAW environments into compliance with the proposed standards. The Commission also preliminarily believes it is valuable to require that the Operating Committee be notified of determinations related to non-SAW environments, because this should enhance the ability of the Operating Committee to oversee the security of CAT Data.

iii. Non-SAW Implementation and Operation Requirements

By requiring the Plan Processor to notify the Operating Committee that a non-SAW environment has achieved compliance with the detailed design specifications submitted by a Participant in connection with its application for an exception (or continuance), the Commission preliminarily believes that the proposed amendments will protect the security of the CAT.[479] The Commission preliminarily believes that it is important for approved Participants to adhere to and implement the detailed design specifications that formed a part of their application packages, because such detailed design specifications will have been reviewed and vetted by the CISO, the CCO, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group.[480] Therefore, the Commission preliminarily believes that non-SAW environments that implement their submitted design specifications should be sufficiently secure, and, for an additional layer of protection and oversight, the proposed amendments require the Plan Processor to determine and notify the Operating Committee that the non-SAW environment has achieved compliance with such detailed design specifications before CAT Data can be accessed via the user-defined direct query or bulk extraction tools.

Similarly, the Commission preliminarily believes that the proposed monitoring and notification requirements will improve the security of the non-SAW environments that are granted an exception by the CISO and the CCO and, therefore, the overall security of the CAT. Requiring the Plan Processor to monitor each non-SAW environment that has been granted an exception will help the Plan Processor to identify any non-compliance events, threats, and/or vulnerabilities, thus reducing the potentially harmful effects these matters could have if left unchecked and uncorrected. The Commission also preliminarily believes that it is appropriate to require approved Participants to simultaneously notify the Plan Processor, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group of any material changes to the security controls for the non-SAW environment. If the security controls reviewed and vetted by the CISO, the CCO, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group change in any material way, the Commission preliminarily believes it is appropriate to require the simultaneous escalation of this information to the Plan Processor, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group.

4. Online Targeted Query Tool and Logging of Access and Extraction

The Commission preliminarily believes the proposed definition of ''delivery of results'' would result in logs that provide more useful information to the Plan Processor and Participants and will assist in the identification of potential issues relating to the security or access to CAT Data. The Commission also preliminarily believes that the requirement to log access and extraction of CAT Data is appropriate because the monthly reports of information relating to the query tools will permit the Operating Committee and Participants to review information concerning access and extraction of CAT Data regularly and to identify issues related to the security of CAT Data.

5. CAT Customer and Account Attributes

The Commission preliminarily believes that it is appropriate to amend the CAT NMS Plan to eliminate the

[478] *See* proposed Section 6.13(d)(i)(A)(1).

[479] The proposed amendments do not specify a particular format for this notification; the Commission preliminarily believes that such notification could be made with a phone call or through email.

[480] *See* proposed Section 6.13(d)(i)(A), (d)(ii)(A).

requirement that Industry Members report SSNs/ITINs and instead require that they report a Transformed Value. As proposed, the Transformed Value will be reported to the CCID Subsystem, which will perform another transformation to create the Customer-ID.[481] The Plan Processor will then link the Customer-ID to the Customer and Account Attributes for use by Regulatory Staff for regulatory and surveillance purposes. Replacing the reporting of ITIN(s)/SSN(s) of a natural person Customer with the reporting of Transformed Values obviates the need for the CAT to collect certain sensitive pieces of identifying information associated with a natural person Customer.[482]

The Commission preliminarily believes that the proposed language in Appendix D, Section 9.1 requires that the Participants must assess the overall performance and design of the CCID Subsystem and the process for creating Customer-ID(s) as part of each annual Regular Written Assessment of the Plan Processor, as required by Article VI, Section 6.6(b)(ii)(A). The Commission preliminarily believes the assessment should enable the Commission to better assess the overall performance and design of the CCID Subsystem, including the ingestion of the Transformed Value and the subsequent creation of an accurate Customer-ID, to confirm the CCID Subsystem is operating as intended, or whether any additional measures should be taken to address the creation and protection of Customer-IDs.

6. Customer Identifying Systems Workflow

The Commission preliminarily believes it is appropriate to require the Plan Processor to maintain a full audit trail of access to Customer Identifying Systems by each Participant and the Commission (who accessed what data and when), and to require the Plan Processor to provide to each Participant and the Commission the audit trail for their respective users on a monthly basis. The information contained in the audit trail and the reports could help the Participants, the Commission, and the Operating Committee develop and implement internal policies, procedures and control systems that allow only Regulatory Staff who are entitled to access to Customer Identifying Systems to have such access.

The Commission preliminarily believes that requiring each Participant to submit an application that has been approved by the Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation) to use Programmatic CAIS Access or Programmatic CCID Subsystem Access will help the Commission to determine whether it is appropriate for a particular Participant to have authorization to use programmatic access. The Commission preliminarily believes that some Participants may not require programmatic access to either CAIS or the CCID Subsystem in order to carry out their regulatory and oversight responsibilities. However, the Commission recognizes that in some circumstances, *e.g.,* determining the scope and nature of hacking and associated trading misconduct may require programmatic access. The specific information required in the application will assist the Commission in evaluating on a case-by-case basis whether programmatic access is needed for a Participant.

7. Proposed Confidentiality Policies, Procedures and Usage Restrictions

The Commission believes that the proposed amendments to Section 6.5(g)(i), which would require the Participants to create and maintain identical confidentiality and related policies, and individualized procedures and usage restrictions, would help protect the security and confidentiality of CAT Data and help ensure that CAT Data is used only for appropriate regulatory and surveillance purposes.

The Commission preliminarily believes that requiring the Participants to periodically review the effectiveness of the policies and procedures and usage restriction controls required by Section 6.5(g)(i), including by using the monitoring and testing protocols documented within the policies pursuant to Section 6.5(g)(i)(J), and take prompt action to remedy deficiencies in such policies, procedures and usage restriction controls, should help ensure that the Proposed Confidentiality Policies, as well as the Participant-specific procedures and usage restriction controls developed pursuant to the Proposed Confidentiality Policies, are effective and being complied with by each Participant.

The Commission preliminarily believes that requiring each Participant, as reasonably practicable, and in any event within 24 hours of becoming aware, report to the Chief Compliance Officer, in accordance with the guidance provided by the Operating Committee: (A) Any instance of noncompliance with the policies, procedures, and usage restriction controls adopted by such Participant pursuant to Section 6.5(g)(i); or (B) a breach of the security of the CAT should help ensure that Participants comply with the Proposed Confidentiality Policies and related procedures, and help ensure the security of CAT Data.

The Commission preliminarily believes that requiring that the Proposed Confidentiality Policies be made publicly available on each of the Participants' websites, or collectively on the CAT NMS Plan website, redacted of sensitive proprietary information, could help ensure that the Proposed Confidentiality Policies are robust and thoroughly considered by Participants. The Commission also believes that such a requirement will allow other Participants, broker-dealers, investors and the public to better understand and analyze the Proposed Confidentiality Policies that govern Participant usage of and the confidentiality of CAT Data. The Commission preliminarily believes that broker-dealers and investors that generates the order and trade activity that is reported to CAT should have some insight on the policies governing usage of CAT Data, particularly due to the sensitivity and importance of CAT Data, which may contain personally identifiable information, trading strategies and other valuable or sensitive information.

The Commission preliminarily believes that requiring each Participant to engage an independent accountant to perform an examination of compliance with the policies required by Section 6.5(g)(i) would provide additional oversight which should enhance confidence that Participants are complying with policies designed to ensure the confidentiality of CAT Data and would help ensure that such data is used solely for surveillance and regulatory purposes. The Commission preliminarily believes that requiring the Participants to submit the examination reports to the Commission would allow the Commission to review the results of the examination that was performed, and to assess whether or not Participants are adequately complying with the Proposed Confidentiality Policies.

The Commission preliminarily believes that requiring the policies required by proposed Section 6.5(g)(i) be subject to review and approval by the Operating Committee, after review by the CISO and CCO, will further help ensure that the Proposed Confidentiality Policies are consistent with the requirements of the CAT NMS Plan and proposed changes herein, while

[481] *See* proposed Section 6.1(v) and proposed Appendix D, Section 9.1 of the CAT NMS Plan.

[482] *See* PII Exemption Order, *supra* note 5, at 16156.

providing for multiple opportunities for feedback and input while the Proposed Confidentiality Policies are being developed. It would allow the Plan Processor to have input in the creation of the Proposed Confidentiality Policies and help ensure consistency with policies and procedures created by the Plan Processor itself. The Commission preliminarily believes that it is appropriate to require the CCO to receive the assistance of the Compliance Subcommittee because the Compliance Subcommittee's purpose is to aid the CCO and because it would further allow for more input into the process of developing the Proposed Confidentiality Policies.[483]

8. Secure Connectivity—''Allow Listing''

The Commission preliminarily believes that requiring ''allow listing,'' which would require the Plan Processor to allow access only to those countries or more granular access points where CAT reporting or regulatory use is both necessary and expected would enhance the security of CAT infrastructure and connections to the CAT infrastructure by requiring the Plan Processor to limit access to the CAT infrastructure based on an authorized end user's geolocation of the IP addresses of CAT Reporters. Similarly, the Commission preliminarily believes that requiring the Plan Processor to establish policies and procedures to allow access if the source location for a particular instance of access cannot be determined technologically would improve the security of the CAT System, by addressing whether or not connectivity is possible and how such connectivity could be granted.

9. Breach Management Policies and Procedures

The Commission preliminarily believes that requiring the Plan Processor's cyber incident response plan to include ''taking appropriate corrective action that includes, at a minimum, mitigating potential harm to investors and market integrity, and devoting adequate resources to remedy the systems or data breach as soon as reasonably practicable,'' would obligate the Plan Processor to respond to systems or data breaches with appropriate steps necessary to remedy each systems or data breach and mitigate the negative effects of the breach, if any, on market participants and the securities markets more broadly.

The Commission preliminarily believes that requiring the Plan Processor's cyber incident response plan to incorporate breach notifications, and requiring the Plan Processor to provide breach notifications, would inform affected CAT Reporters, and the Participants and the Commission, in the case of systems or data breaches. The Commission preliminarily believes that it is appropriate for these breach notifications to include a summary description of the systems or data breach, including a description of the corrective action taken and when the systems or data breach has been or is expected to be resolved. These breach notifications could potentially allow affected CAT Reporters, Participants and/or the Commission to proactively respond to the information in a way to mitigate any potential harm to themselves, customers, investors and the public. Furthermore, requiring the Plan Processor to document all information relevant to de minimis breaches should ensure that the Plan Processor has all the information necessary should its initial determination that a breach is de minimis prove to be incorrect, so that it could promptly provide breach notifications as required, and would be helpful in identifying patterns among systems or data breaches.

10. Customer Information for Allocation Report Firm Designated IDs

The Commission preliminarily believes proposed Section 6.4(d)(ii)(c) would explicitly require that Customer and Account Attributes be reported for Firm Designated IDs submitted in connection with Allocation Reports, and will require Industry Members to report such information. The Commission preliminarily believes that this proposed amendment is consistent with previously granted exemptive relief, which requires the Central Repository to have the ability to use elements of Allocation Reports to link the subaccount holder to those with authority to trade on behalf of the account.[484] The Commission preliminarily believes that if Industry Members do not provide Customer and Account Attributes for the relevant Firm Designated ID submitted in an Allocation Report, then there would be no ability for the Central Repository to link the subaccount holder to those with authority to trade on behalf of the account. The Commission preliminarily believes that amending the language in Section 6.4(d)(ii)(C) to implement the previously approved exemptive relief is appropriate. However, the Commission does not believe that the proposed amendment substantively changes the obligations of Industry Members, who, through Participant Compliance Rules, are already required to submit customer information for all Active Accounts pursuant to the CAT NMS Plan.[485]

C. Respondents

1. National Securities Exchanges and National Securities Associations

The respondents to certain proposed collections of information would be the 25 Participants (the 24 national securities exchanges and one national securities association (FINRA)) currently registered with the Commission.[486]

2. Members of National Securities Exchanges and National Securities Association

The respondents for certain information collection are the Participants' broker-dealer members, that is, Industry Members. The Commission understands that there are currently 3,734 broker-dealers; however, not all broker-dealers are expected to have CAT reporting obligations. The Commission estimates that approximately 1,500 broker-dealers currently quote or execute transactions in NMS Securities, Listed Options or OTC Equity Securities and would likely have CAT reporting obligations.[487]

D. Total Initial and Annual Reporting and Recordkeeping Burdens

The Commission's total burden estimates in this Paperwork Reduction Act section reflect the total burden on

[483] Members of the Advisory Committee, composed of members that are not employed by or affiliated with any Participant or any of its affiliates or facilities, are currently on the Compliance Subcommittee. *See* CAT NMS Plan, *supra* note 3, at Section 4.13.

[484] *See* Securities and Exchange Act Release No. 77265 (March 1, 2016), 81 FR 11856, 11868 (March 7, 2016); *see also* CAT NMS Plan, *supra* note 3, at Section 1.1 (defining ''Allocation Report'') and Section 6.4(d)(ii)(A)(i) (requiring an Allocation Report if an order is executed in whole in or in part).

[485] *See supra,* note 407.

[486] The Participants are: BOX Options Exchange LLC, Cboe BZX Exchange, Inc., Cboe BYX Exchange, Inc., Cboe C2 Exchange, Inc., Cboe EDGA Exchange, Inc., Cboe EDGX, Inc., Cboe Exchange, Inc., Financial Industry Regulatory Authority, Inc., Investors Exchange Inc., Long-Term Stock Exchange, Inc., MEMX, LLC, Miami International Securities Exchange LLC, MIAX PEARL, LLC, MIAX Emerald, LLC, NASDAQ BX, Inc., NASDAQ GEMX, LLC, NASDAQ ISE, LLC, NASDAQ MRX, LLC, NASDAQ PHLX LLC, The NASDAQ Stock Market LLC, New York Stock Exchange LLC, NYSE MKT LLC, and NYSE Arca, Inc., NYSE Chicago Stock Exchange, Inc., NYSE National, Inc.

[487] The Commission understands that the remaining 2,234 registered broker-dealers either trade in asset classes not currently included in the definition of Eligible Security or do not trade at all (*e.g.,* broker-dealers for the purposes of underwriting, advising, private placements).

all Participants and Industry Members. The burden estimates per Participant or Industry Member are intended to reflect the average paperwork burden for each Participant or Industry Member, but some Participants or Industry Members may experience more burden than the Commission's estimates, while others may experience less. The burden figures set forth in this section are the based on a variety of sources, including Commission staff's experience with the development of the CAT and estimated burdens for other rulemakings.

Many aspects of the proposed amendment to the CAT NMS Plan would require the Plan Processor to do certain activities. However, because the CAT NMS Plan applies to and obligates the Participants and not the Plan Processor, the Commission preliminarily believes it is appropriate to estimate the Participants' external cost burden based on the estimated Plan Processor staff hours required to comply with the proposed obligations. The Commission derives these estimated costs associated with Plan Processor staff time based on per hour figures from SIFMA's *Management & Professional Earnings in the Securities Industry 2013,* modified by Commission staff to account for an 1800-hour work-year, and multiplied by 5.35 to account for bonuses, firm size, employee benefits and overhead, and adjusted for inflation based on Bureau of Labor Statistics data on CPI–U between January 2013 and January 2020 (a factor of 1.12).[488]

1. Evaluation of the CISP

The CAT NMS Plan already requires the Participants to submit to the Commission, at least annually, a written assessment of the Plan Processor's performance that is prepared by the CCO. As part of this assessment, the Participants are required to include an evaluation of the information security program ''to ensure that the program is consistent with the highest industry standards for the protection of data,'' which the Participants may review and comment on before providing the assessment to the Commission.

The proposed amendments would newly require the CCO to evaluate elements of the CISP that relate to SAWs and, in collaboration with the CISO, to include a review of CAT Data extracted from the CAT System to assess the security risk of permitting such CAT Data to be extracted. In connection with these new requirements, the Commission preliminarily estimates that the Participants would incur an ongoing aggregate expense of $129,900 per year, or that each Participant would incur an annual expense of $5,196, in connection with these proposed amendments, based on a preliminary estimate that Plan Processor staff would need approximately 250 hours per year to comply with these new requirements.[489]

Under the CAT NMS Plan, the Participants would also have the right to review and comment on these new elements of the written assessment. The Commission preliminarily estimates that each Participant would spend approximately 25 hours reviewing and commenting on these new elements [490] and that all Participants would incur an aggregate burden of approximately 625 hours.[491] In addition, the Commission preliminarily estimates that each Participant would spend approximately $1,000 on external legal consulting costs [492] or that all Participants would spend approximately $25,000 on external legal consulting costs.[493]

2. Security Working Group

The Commission preliminarily believes that each Participant would incur an ongoing annual burden of 364 hours to comply with the proposed requirement that the Security Working Group aid the CISO and the Operating Committee or that the Participants will incur an aggregated annual burden of 9,100 hours.[494]

The Commission preliminarily believes that requiring the CISO to keep the Security Working Group apprised of relevant developments, to provide it with all information and materials necessary to fulfill its purpose, and to prepare for and attend meetings of the Security Working Group will take the CISO approximately 570 hours per year. Accordingly, the Commission preliminarily estimates that the Participants would incur an ongoing aggregate expense of approximately $309,510 per year, or that each Participant would incur an ongoing annual expense of $12,380, in connection with these proposed amendments.[495]

3. SAWs

a. Policies, Procedures, and Detailed Design Specifications

The burdens associated with the development and maintenance of the CISP are already largely accounted for in the CAT NMS Plan Approval Order.[496] For the Plan Processor to develop a CISP that incorporates the SAW-specific additions that would be

[488] For example, the 2020 inflation-adjusted effective hourly wage rate for attorneys is estimated at $426 ($380 × 1.12). For purposes of this Paperwork Reduction Act analysis, the Commission has preliminarily estimated the per hour cost of a Chief Information Security Officer to be identical to the per hour cost of a Chief Compliance Officer ($543 per hour).

[489] The estimated 250 hours of Plan Processor staff time include 100 hours by the CCO, 100 hours by the CISO, and 50 hours for an attorney. Accordingly, the Commission preliminarily estimates that the Participants would together incur an ongoing annual expense of $129,900. (100 hours for CCO = $54,300) + (100 hours for CISO = $54,300) + (50 hours for Attorney = $21,300). Each Participant would therefore incur an ongoing annual expense of $5,196. $129,900/25 Participants = $5,196 per Participant.

[490] The Commission is basing these estimates on the CAT NMS Plan Approval Order, which estimated that each Participant would incur a burden of 171.43 hours to review and comment on the entire written assessment required by Section 6.6(b)(ii). *See* CAT NMS Plan Approval Order, *supra* note 3, at 84925 note 3409. The written assessment is made up of many components, and the Commission preliminarily believes the proposed amendments would only require a portion of the time that was originally estimated for the entire assessment. The Commission therefore preliminarily believes that each Participant would incur a burden of 25 hours to review and comment on the new elements of the written assessment. 15 hours for attorney + 10 hours for chief compliance officer = 25 hours.

[491] 25 hours per Participant * 25 Participants = 625 hours.

[492] The Commission is basing these estimates on the CAT NMS Plan Approval Order, which estimated that each Participant would spend $1,000 on external legal consulting costs in order to review and comment on the entire written assessment required by Section 6.6(b)(ii). *See* CAT NMS Plan Approval Order, *supra* note 3, at 84925–26. The Commission preliminarily believes this is an appropriate estimate for the amount the Participants might spend on the proposed elements of the written assessment.

[493] $1,000 per Participant * 25 Participants = $25,000.

[494] The Commission preliminarily believes, based on the activity of the current group established by the Operating Committee to discuss the security of the CAT, that the Security Working Group will meet weekly. The Commission preliminarily estimates that the chief or deputy chief information security officer of each Participant will likely spend approximately 5 hours per week, on average, to prepare for this meeting and 2 hours to attend this meeting. 7 hours * 52 weeks = 364 hours per Participant. 364 hours per Participant * 25 Participants = 9,100 hours.

[495] The Commission preliminarily estimates that the Security Working Group will meet weekly and that the CISO will spend 8 hours preparing for each meeting of the Security Working Group and 2 hours to attend each meeting. 10 hours * 52 weeks = 520 hours. In addition, the Commission preliminarily estimates that the CISO will spend approximately 50 hours per year to keep the Security Working Group apprised of relevant developments and to provide it with all information and materials necessary to fulfill its purpose. 520 hours + 50 hours = 570 hours for CISO. 570 hours for CISO = $309,510. $309,510/25 Participants = $12,380.40 per Participant. The Commission does not believe that any initial or one-time burdens would be incurred in association with these proposed amendments.

[496] *See* CAT NMS Plan Approval Order, *supra* note 3, at 84219–20. In addition, to the extent that the CISO consults with the Security Working Group regarding the development and maintenance of the CISP, those costs have already been detailed elsewhere. *See* Part III.D.2. *supra.*

required under the proposed amendments,[497] the Commission preliminarily estimates that the Participants would incur an initial, one-time expense of approximately $89,020, or that each Participant would incur an initial, one-time annual expense of approximately $3,561, based on a preliminary estimate that Plan Processor staff would need approximately 270 hours to comply with these new requirements.[498] The Commission also preliminarily estimates that the Participants would incur an initial, one-time burden of approximately $27,000 in external legal and consulting costs [499] or that each Participant would incur an initial, one-time burden of $1,080.[500] Furthermore, to maintain a CISP that incorporated the SAW-specific additions that would be required under the proposed amendments, the Commission preliminarily estimates that the Participants would incur an ongoing expense of approximately $56,648 per year, or that each Participant would incur an ongoing, annual expense of approximately $2,266, based on a preliminary estimate that Plan Processor staff would need approximately 175 hours per year to maintain those elements of the CISP that relate to SAWs.[501]

For the Plan Processor to develop detailed design specifications for the technical implementation of the access, monitoring, and other controls required for SAWs,[502] the Commission preliminarily estimates that the Participants would incur an initial, one-time expense of approximately $56,180, or that each Participant would incur an initial, one-time annual expense of approximately $2,247, based on a preliminary estimate that Plan Processor staff would need approximately 160 hours to comply with these new requirements.[503] The Commission also preliminarily estimates that the Participants would incur an initial, one-time burden of approximately $47,000 in external legal and consulting costs [504] or that each Participant would incur an initial, one-time burden of $1,880.[505] In addition, the Commission believes that the Participants would incur an initial, one-time expense of approximately $2,965 to make the required detailed design specifications available to the Participants [506] or that each Participant would incur an initial, one-time expense of approximately $119.[507] Furthermore, to maintain the required detailed design specifications, the Commission preliminarily estimates that the Participants would incur an ongoing expense of approximately $48,250 per year, or that each Participant would incur an ongoing, annual expense of approximately $1,930, based on a preliminary estimate that Plan Processor staff would need approximately 145 hours per year to maintain the required detailed design specifications.[508]

b. Implementation and Operation Requirements

For the Plan Processor to evaluate each Participant's SAW to confirm that the SAW has achieved compliance with the detailed design specifications required by proposed Section 6.13(b)(i), the Commission preliminarily estimates that the Participants would incur an initial, one-time expense of approximately $463,750, or that each Participant would incur an initial, one-time expense of $18,550, based on a preliminary estimate that Plan Processor staff would need approximately 45 hours per SAW to perform the required evaluation and notification of the Operating Committee.[509]

[497] *See* proposed Section 1.1, ''Comprehensive Information Security Program'' and ''Secure Analytical Workspace.'' *See also* proposed Section 6.12; proposed Section 6.13(a).

[498] The estimated 270 hours of Plan Processor staff time include 200 hours by a senior systems analyst, 40 hours by a compliance attorney, 20 hours by the chief compliance officer, and 10 hours by a director of compliance. Accordingly, the Commission preliminarily estimates that the Participants would together incur an ongoing annual expense of $89,020. (200 hours for senior systems analyst = $58,200) + (40 hours for compliance attorney = $14,960) + (20 hours for chief compliance officer = $10,860) + (10 hours for director of compliance = $5,000) = $89,020. Each Participant would therefore incur an ongoing annual expense of $3,560.80. $89,020/25 Participants = $3,560.80 per Participant. This estimate is based on burdens estimated in the adopting release for Regulation SCI for the development of systems compliance policies and procedures. *See* Securities Exchange Act Release No. (November 19, 2014), 79 FR 72252, at 72378 (December 5, 2014) (''Regulation SCI Adopting Release'').

[499] This estimate is based on burdens estimated in the adopting release for Regulation SCI for the development of systems compliance policies and procedures. *See* Regulation SCI Adopting Release, *supra* note 498, at 72378.

[500] $27,000/25 Participants = $1,080 per Participant.

[501] The estimated 175 hours of Plan Processor staff time include 134 hours by a senior systems analyst, 26 hours by a compliance attorney, 10 hours by the chief compliance officer, and 5 hours by a director of compliance. Accordingly, the Commission preliminarily estimates that the Participants would together incur an ongoing annual expense of $56,648. (134 hours for senior systems analyst = $38,994) + (26 hours for compliance attorney = $9,724) + (10 hours for chief compliance officer = $5,430) + (5 hours for director of compliance = $2,500) = $56,648. Each Participant would therefore incur an ongoing annual expense of $2,265.92. $56,648/25 Participants = $2,265.92 per Participant. This estimate is based on burdens estimated in the adopting release for Regulation SCI for the development of systems compliance policies and procedures. *See* Regulation SCI Adopting Release, *supra* note 498, at 72378.

[502] *See* proposed Section 6.13(b)(i).

[503] The estimated 160 hours of Plan Processor staff time include 100 hours by a senior systems analyst, 30 hours by a compliance attorney, 20 hours by the chief compliance officer, and 10 hours by a director of compliance. Accordingly, the Commission preliminarily estimates that the Participants would together incur an ongoing annual expense of $56,180. (100 hours for senior systems analyst = $29,100) + (30 hours for compliance attorney = $11,220) + (20 hours for chief compliance officer = $10,860) + (10 hours for director of compliance = $5,000) = $56,180. Each Participant would therefore incur an ongoing annual expense of $2,247.20. $56,180/25 Participants = $2,247.20 per Participant. This estimate is based on burdens estimated in the adopting release for Regulation SCI for the development of policies and procedures related to the design, development, testing, maintenance, operation, and surveillance of systems. *See* Regulation SCI Adopting Release, *supra* note 498, at 72377. To the extent that the CISO consults with the Security Working Group regarding the development and maintenance of the required detailed design specifications, those costs have already been accounted elsewhere. *See* Part III.D.2. *supra.*

[504] This estimate is based on burdens estimated in the adopting release for Regulation SCI for the development of policies and procedures related to the design, development, testing, maintenance, operation, and surveillance of systems. *See* Regulation SCI Adopting Release, *supra* note 498, at 72377.

[505] $47,000/25 Participants = $1,880 per Participant.

[506] The Commission's estimate includes 5 hours by a senior systems analyst, 2 hours by a compliance attorney, and 3 hours by a webmaster. (5 hours for senior systems analyst = $1,455) + (2 hours for compliance attorney = $748) + (3 hours for webmaster = $762) = $2,965.

[507] $2,965/25 Participants = $118.60 per Participant.

[508] The estimated 145 hours of Plan Processor staff time include 100 hours by a senior systems analyst, 30 hours by a compliance attorney, 10 hours by the chief compliance officer, and 5 hours by a director of compliance. Accordingly, the Commission preliminarily estimates that the Participants would together incur an ongoing annual expense of $48,250. (100 hours for senior systems analyst = $29,100) + (30 hours for compliance attorney = $11,220) + (10 hours for chief compliance officer = $5,430) + (5 hours for director of compliance = $2,500) = $48,250. Each Participant would therefore incur an ongoing annual expense of $1,930. $48,250/25 Participants = $1,930 per Participant. This estimate is based on burdens estimated in the adopting release for Regulation SCI for the development of policies and procedures related to the design, development, testing, maintenance, operation, and surveillance of systems. *See* Regulation SCI Adopting Release, *supra* note 498, at 72377. To the extent that the CISO consults with the Security Working Group regarding the development and maintenance of the required detailed design specifications, those costs have already been accounted for elsewhere. *See* Part III.D.2. *supra.*

[509] The estimated 45 hours of Plan Processor staff time include 20 hours by a senior systems analyst, 20 hours by the chief information security officer, and 5 hours by a compliance attorney. Assuming each Participant will only have one SAW, the Commission therefore preliminarily estimates that the Participants would together incur an initial, one-time expense of $18,550 per SAW, or an initial, one-time expense of $463,750. (20 hours for senior systems analyst = $5,820) + (20 hours for chief information security officer = $10,860) + (5 hours

Continued

For the Plan Processor to build automated systems that will enable monitoring of the SAWs, the Commission preliminarily estimates that the Participants would incur an initial, one-time expense of $52,350, or that each Participant would incur an initial, one-time expense of $2,094, based on a preliminary estimate that Plan Processor staff would need approximately 170 hours to build the required systems.[510] For the Plan Processor to maintain such systems and to monitor each Participant's SAW in accordance with the detailed design specifications developed pursuant to proposed Section 6.13(b)(i), the Commission preliminarily estimates that the Participants would incur an ongoing annual expense of approximately $629,220, or that each Participant would incur an ongoing annual expense of approximately $25,169, based on a preliminary estimate that Plan Processor staff would need approximately 2,150 hours to maintain the required systems and to conduct such monitoring.[511] For the Plan Processor to simultaneously notify the Participant of any identified non-compliance with the CISP or the detailed design specifications, the Commission preliminarily estimates that the Participants would incur an ongoing annual expense of approximately $58,969, or that each Participant would incur an ongoing annual expense of approximately $2,359, based on a preliminary estimate that Plan Processor staff would need approximately 1.5 hours for each notification of non-compliance.[512]

c. Non-SAW Environments

i. Application Materials

The Commission preliminarily estimates that 6 Participants will apply for an exception to the SAW usage requirements, based on the assumption that one exchange family will seek an exception.[513] In connection with the initial application for an exception, the Commission further estimates that each of these Participants would spend an initial, one-time amount of approximately $250,000 on external consulting costs to obtain the required security assessment from a named and independent third party security assessor and approximately 270 hours to provide the required detailed design specifications.[514] The Commission further estimates that the each Participant would spend 5 hours submitting these materials to the CCO, the CISO, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group.[515] Accordingly, with respect to initial application materials, the Commission preliminarily estimates that the Participants would incur an initial, one-time expense of approximately $1,500,000[516] and an initial, one-time burden of approximately 1,650 hours.[517]

Under the proposed amendments, Participants that are denied an exception or that want to apply for a continuance must submit a new security assessment that complies with the requirement of proposed Section 6.13(d)(i)(A)(1) and up-to-date versions of the design specifications required by proposed Section 6.13(d)(i)(A)(2). The Commission preliminarily believes that the cost to obtain a new security assessment would still be $250,000 in these scenarios, because the Participants would have to obtain the security assessment from a named and independent third party security assessor that might not be able to leverage previous work. However, the Commission preliminarily believes that each Participant would only incur about half of the hourly burdens associated with preparation of initial application materials to prepare the updated detailed design specifications needed to support a re-application or an application for a continuance, because

for compliance attorney = $1,870) = $18,550 per SAW. $18,550 * 25 Participants = $463,750. Each Participant would therefore incur an initial, one-time expense of $18,550. $463,750/25 Participants = $18,550 per Participant. To the extent that the CISO consults with the Security Working Group regarding the evaluation or validation of the SAWs, those costs have already been accounted for elsewhere. *See* Part III.D.2. *supra.*

[510] Because the SAWs should all be implementing the CISP according to the detailed design specifications developed by the Plan Processor, the Commission preliminarily believes that much of the monitoring required by the proposed amendments could be automated. To build a system that would enable such monitoring, the Commission preliminarily believes that Plan Processor would require 170 hours, including 40 hours by a senior programmer, 40 hours by 3 programmers, and 10 hours by the CISO. Accordingly, the Commission preliminarily estimates that the Participants would together incur an initial, one-time expense of $52,350. (40 hours for senior programmer = $13,560) + (40 hours for programmer = $11,120) + (40 hours for programmer = $11,120) + (40 hours for programmer = $11,120) + (10 hours for CISO = $5,430) = $52,350. Each Participant would therefore incur an initial, one-time expense of $2,094. $52,350/25 Participants = $2,094. To the extent that the CISO consults with the Security Working Group regarding the build of such monitoring systems, those costs have already been accounted for elsewhere. *See* Part III.D.2. *supra.*

[511] The Commission preliminarily believes that one senior systems analyst working 40 hours per week could conduct the required monitoring for all SAWs. Accordingly, the Commission preliminarily estimates that the Participants would together incur an ongoing annual expense of $605,280. 40 hours * 52 weeks = 2,080 hours. 2,080 hours for senior systems analyst = $605,280. Each Participant would therefore incur an ongoing annual expense of $24,211.20. $605,280/25 Participants = $24,211.20. In addition, to maintain the automated monitoring systems, the Commission preliminarily estimates that Plan Processor staff would need 70 hours, including 30 hours for a senior programmer, 30 hours for a programmer, and 10 hours for the CISO. Accordingly, the Commission preliminarily estimates that the Participants would together incur an ongoing annual expense of $23,940. (30 hours for senior programmer = $10,170) + (30 hours for programmer = $8,340) + (10 hours for CISO = $5,430) = $23,940. Each Participant would therefore incur an ongoing annual expense of $957.60. $23,940/25 Participants = $957.60 per Participant. Altogether, the ongoing annual expenses to the Participants as a whole would be $629,220, or $25,168.80 for each individual Participant. $605,280 + $23,940 = $629,220. $629,220/25 Participants = $25,168.80 per Participant. To the extent that the CISO consults with the Security Working Group regarding SAW monitoring or the results of such monitoring, those costs have already been accounted for elsewhere. *See* Part III.D.2. *supra.*

[512] The Commission preliminarily estimates that the Plan Processor would identify 5 non-compliance events per year for each SAW or, assuming that each Participant only has one SAW, 125 non-compliance events across all SAWs. 5 events per SAW * 25 SAWs = 125 events. For each non-compliance event, the Commission preliminarily estimates that the Plan Processor will spend 1.5 hours notifying the Participant of the identified non-compliance, including 0.5 hours by a senior systems analyst, 0.25 hours by a compliance manager, 0.25 hours by an attorney, and 0.5 hours by a senior business analyst. (0.5 hours for senior systems analyst = $145.50) + (0.25 for compliance manager = $79.25) + (0.25 for attorney = $106.50) + (0.5 hours for senior business analyst = $140.50) = $471.75 per event. This estimate is based on estimates set forth in the Regulation SCI Adopting Release for oral notifications of SCI events, as the Commission preliminarily expects that such notifications would typically be provided orally on a phone call or in a short email. *See* Regulation SCI Adopting Release, *supra* note 498, at 72384. Accordingly, the Commission preliminarily estimates that the Participants would together incur an ongoing annual expense of $58,968.75. 125 events * $471.75 = $58,968.75. Each Participant would therefore incur an ongoing annual expense of $2,358.75. $58,968.75/25 Participants = $2,358.75. To the extent that the CISO consults with the Security Working Group regarding any non-compliance events, those costs have already been accounted for elsewhere. *See* Part III.D.2. *supra.*

[513] For example, there are six Participants in the Cboe Global Markets, Inc. exchange group, six Participants in the Nasdaq, Inc. exchange group, and five Participants in the Intercontinental Exchange, Inc. exchange group. All estimates in this section represent an average; the Commission believes that some Participants may incur greater costs and some lesser costs due to variances in economies of scale for Participants who share a common corporate parent.

[514] The estimated 270 hours include 200 hours by a senior systems analyst, 40 hours by a compliance attorney, 20 hours by the chief compliance officer, and 10 hours by a director of compliance. These estimates mirror the estimated hours for the Plan Processor to perform the similar task of developing the detailed design specifications for the SAWs.

[515] The estimated 5 hours include 5 hours by a compliance attorney.

[516] $250,000 per non-SAW environment * 6 non-SAW environments = $1,500,000.

[517] 270 hours + 5 hours = 275 hours per non-SAW environment. 275 hours per non-SAW environment * 6 non-SAW environments = 1,650 hours.

the Commission believes that each Participant would be able to significantly leverage its previous work. Accordingly, the Commission preliminarily estimates that each of these Participants would spend an ongoing annual [518] amount of approximately $250,000 on external consulting costs to obtain the required security assessment from a named and independent third party and approximately 135 hours to provide the required detailed design specifications.[519] The Commission further estimates that each Participant would spend 5 hours submitting these materials to the CCO, the CISO, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group.[520] Accordingly, with respect to updated application materials submitted in connection with a re-application or an application for a continuance, the Commission preliminarily estimates that the Participants would incur an ongoing annual expense of approximately $1,500,000 [521] and an ongoing annual burden of approximately 840 hours.[522]

ii. Exception and Revocation Determinations

In connection with the requirement that the Plan Processor develop policies and procedures governing the review of applications for exceptions to the proposed SAW usage requirements, the Commission preliminarily estimates that the Participants would incur an initial, one-time expense of $63,400, or that each Participant would incur an initial, one-time expense of $2,536, based on a preliminary estimate that Plan Processor staff would need approximately 130 hours to develop such policies and procedures.[523] The Commission also preliminarily estimates that the Participants would incur an ongoing annual expense of $31,700, or that each Participant would incur an ongoing annual expense of approximately $1,268, based on a preliminary estimate that Plan Processor staff would need approximately 65 hours to maintain and update such policies and procedures as needed.[524]

As noted above, the Commission preliminarily estimates that 6 Participants will apply for an exception to the SAW usage requirements. In connection with initial applications for an exception, the Commission also preliminarily estimates that the Participants would incur an initial, one-time expense of approximately $550,560, or that each Participant would incur an initial, one-time expense of $22,022, based on a preliminary estimate that Plan Processor staff would need approximately 200 hours per initial application to review the application and issue the required determination and supporting written statement.[525] The Commission preliminarily believes that the ongoing annual expenses associated with each application for a continued exception would be the same, as the process for continued exceptions is the same as the process for initial applications. Therefore, in connection with applications for a continued exception, the Commission preliminarily estimates that the Participants would incur an ongoing annual expense of approximately $550,560, or that each Participant would incur an ongoing annual expense of $22,022, based on a preliminary estimate that Plan Processor staff would need approximately 200 hours per application to review the application and issue the required determination and supporting written statement.[526]

The Commission is unable to estimate in advance whether Participants would submit their application materials for a continued exception on time or whether Participants would be denied a continued exception by the CISO and the CCO. For each such instance, however, the Commission preliminarily believes that the Participants would incur an ongoing annual expense of approximately $17,510, or that each Participant would incur an ongoing annual expense of approximately $700, based on a preliminary estimate that Plan Processor staff would need approximately 40 hours to revoke an exception and to determine on which remediation timeframe the Participant should be required to cease using its non-SAW environment to access CAT Data through the user-defined direct query and bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2 of the CAT NMS Plan.[527]

[518] Participants that are denied an exception and re-apply may incur these ongoing costs more quickly than Participants that are initially granted an exception and subsequently seek a continuance. For example, a denied Participant might incur these ongoing costs approximately 90 days after submitting its initial application materials, whereas a Participant that is initially granted an exception may not incur these costs for 11 months. Nevertheless, the Commission preliminarily believes these costs and burdens will most likely be incurred annually in both scenarios, in part because Participants that re-apply are unlikely to be denied an exception twice. The proposed amendments require the CISO and the CCO to detail the deficiencies in a denied Participant's application, thus making it easier for the Participant to correct such deficiencies. *See* proposed Section 6.13(d)(i)(B)(2); proposed Section 6.13(d)(ii)(B)(2).

[519] The estimated 135 hours include 100 hours by a senior systems analyst, 20 hours by a compliance attorney, 10 hours by the chief compliance officer, and 5 hours by a director of compliance.

[520] The estimated 5 hours include 5 hours by a compliance attorney.

[521] $250,000 per non-SAW environment * 6 non-SAW environments = $1,500,000.

[522] 135 hours + 5 hours = 140 hours per non-SAW environment. 140 hours per non-SAW environment * 6 non-SAW environments = 840 hours.

[523] The estimated 130 hours of Plan Processor staff time include 40 hours by the CISO, 40 hours by the CCO, 40 hours by a compliance attorney, and 10 hours by a director of compliance. Accordingly, the Commission preliminarily estimates that the Participants would together incur an ongoing annual expense of $63,400. (40 hours for CISO = $21,720) + (40 hours for CCO = $21,720) + (40 hours for compliance attorney = $14,960) + (10 hours for director of compliance = $5,000) = $63,400. Each Participant would therefore incur an ongoing annual expense of $2,536. $63,400/25 Participants = $2,536 per Participant.

[524] The estimated 65 hours of Plan Processor staff time include 20 hours by the CISO, 20 hours by the CCO, 20 hours by a compliance attorney, and 5 hours by a director of compliance. Accordingly, the Commission preliminarily estimates that the Participants would together incur an ongoing annual expense of $31,700. (20 hours by the CISO = $10,860) + (20 hours by the CCO = $10,860) + (20 hours for compliance attorney = $7,480) + (5 hours for director of compliance = $2,500) = $31,700. Each Participant would therefor incur an ongoing annual expense of $1,268. $31,700/25 Participants = $1,268 per Participant.

[525] The estimated 200 hours of Plan Processor staff time include 60 hours by the CCO, 60 hours by the CISO, 40 hours by a senior systems analyst, and 40 hours by a compliance attorney. Assuming only 6 Participants will apply for an exception to use a non-SAW environment, the Commission preliminarily estimates that the Participants would together incur an initial, one-time expense of $550,560. (60 hours by the CCO = $32,580) + (60 hours by the CISO = $32,580) + (40 hours for senior systems analyst = $11,640) + (40 hours for compliance attorney = $14,960) = $91,760 per initial application. $91,760 * 6 Participants = $550,560. Each Participant would therefore incur an initial, one-time expense of $22,022.40. $550,560/25 Participants = $22,022.40 per Participant. To the extent that the CISO consults with the Security Working Group regarding these applications, those costs have already been accounted for elsewhere. *See* Part III.D.2. *supra.*

[526] The estimated 200 hours of Plan Processor staff time include 60 hours by the CCO, 60 hours by the CISO, 40 hours by a senior systems analyst, and 40 hours by a compliance attorney. Assuming that 6 Participants will apply for a continued exception to use a non-SAW environment, and that 6 Participants will submit their application materials on time, the Commission preliminarily estimates that the Participants would together incur an ongoing annual expense of $550,560. (60 hours by the CCO = $32,580) + (60 hours by the CISO = $32,580) + (40 hours for senior systems analyst = $11,640) + (40 hours for compliance attorney = $14,960) = $91,760 per application. $91,760 * 6 Participants = $550,560. Each Participant would therefore incur an ongoing annual expense of $22,022.40. $550,560/25 Participants = $22,022.40 per Participant. To the extent that the CISO consults with the Security Working Group regarding these applications, those costs have already been accounted for elsewhere. *See* Part III.D.2. *supra.* To the extent that Participants fail to submit their continuance application materials on time, the costs associated with continuance determinations would be lower.

[527] The estimated 40 hours of Plan Processor staff time include 10 hours by the CCO, 10 hours by the

Continued

iii. Non-SAW Environment Implementation and Operation Requirements

The requirement that the Plan Processor notify the Operating Committee that a non-SAW environment has achieved compliance with the detailed design specifications submitted by a Participant as part of its application for an exception (or continuance) largely mirrors the proposed requirements set forth for SAWs.[528] However, as noted above, the Commission preliminarily believes that only 6 Participants will apply for an exception to use a non-SAW environment, such that the Plan Processor will only need to evaluate 6 non-SAW environments.[529] As the above estimates set forth for SAWs assume that the Plan Processor will need to perform this task for 25 SAWs,[530] instead of for 6 environments, the Commission has correspondingly reduced the preliminary estimates described above for the Plan Processor to evaluate each Participant's SAW and notify the Operating Committee. Accordingly, the Commission preliminarily estimates that the Participants would incur an initial, one-time expense of approximately $111,300, or that each Participant would incur an initial, one-time expense of $4,452, based on a preliminary estimate that Plan Processor staff would need approximately 45 hours per non-SAW environment to perform the required evaluation and notification.[531]

The requirement that the Plan Processor monitor the non-SAW environment in accordance with the detailed design specifications submitted with the exception (or continuance) application and notify the Participant of any identified non-compliance with such detailed design specifications largely mirrors the proposed requirements set forth for SAWs.[532] However, as explained above, the Commission preliminarily believes that only 6 Participants will apply for an exception to use a non-SAW environment and has correspondingly reduced the preliminary estimates described above for the Plan Processor to monitor each SAW and notify Participants of any identified non-compliance.[533] Accordingly, for the Plan Processor to monitor non-SAW environments for compliance with the detailed design specifications submitted with the exception (or continuance) application, the Commission preliminarily estimates that the Participants would incur an ongoing annual expense of approximately $302,640, or that each Participant would incur an ongoing annual expense of approximately $12,106, based on a preliminary estimate that Plan Processor staff would need approximately 1,040 hours to conduct such monitoring.[534] For the Plan Processor to notify the Participant of any identified non-compliance with the detailed design specifications, the Commission preliminarily estimates that the Participants would incur an ongoing annual expense of approximately $14,153, or that each Participant would incur an ongoing annual expense of approximately $566, based on a preliminary estimate that Plan Processor staff would need approximately 1.5 hours for each notification of non-compliance.[535]

Finally, with respect to the requirement that each Participant using a non-SAW environment simultaneously notify the Plan Processor, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group of any material changes to its security controls for the non-SAW environment, the Commission preliminarily believes that 6 Participants would apply for an exception to use a non-SAW environment and that each of these Participants would need to simultaneously notify the Plan Processor, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group of a material change to its security controls approximately 4 times a year. The Commission also preliminarily believes that each such notification would require 15 burden hours.[536]

CISO, 10 hours by a senior systems analyst, and 10 hours by a compliance attorney. The Commission preliminarily estimates that the Participants would together incur an ongoing annual expense of $17,510. (10 hours by the CCO = $5,430) + (10 hours by the CISO = $5,430) + (10 hours for senior systems analyst = $2,910) + (10 hours for compliance attorney = $3,740) = $17,510 per application. Each Participant would therefore incur an ongoing annual expense of $700.40. $17,510/25 Participants = $700.40 per Participant. To the extent that the CISO consults with the Security Working Group regarding such a decision, those costs have already been accounted for elsewhere. *See* Part III.D.2. *supra.* To the extent that Participants that are denied a continuance, or that fail to submit their continuance application materials on time, do not re-apply for an exception, the ongoing annual costs detailed above for preparation of application materials and for exception determinations would be lower.

[528] *See, e.g.,* proposed Section 6.13(b); *see also* Part III.D.3.b. *supra.*

[529] *See* note 513 and associated text *supra.*

[530] *See* note 509 and associated text *supra.*

[531] The estimated 45 hours of Plan Processor staff time include 20 hours by a senior systems analyst, 20 hours by the chief information security officer, and 5 hours by a compliance attorney. Assuming only 6 Participants will apply for an exception to use a non-SAW environment, the Commission preliminarily estimates that the Participants would together incur an initial, one-time expense of $111,300. (20 hours for senior systems analyst = $5,820) + (20 hours for chief information security officer = $10,860) + (5 hours for compliance attorney = $1,870) = $18,550 per non-SAW environment. $18,550 * 6 Participants = $111,300. Each Participant would therefore incur an initial, one-time expense of $4,452. $111,300/25 Participants = $4,452 per Participant. To the extent that the CISO consults with the Security Working Group regarding the evaluation of the non-SAW environments, those costs have already been accounted for elsewhere. *See* Part III.D.2. *supra.*

[532] *See* proposed Section 6.13(c)(i); *see also* Part III.D.3.b. *supra.*

[533] For the purposes of this section, the Commission preliminarily estimates that all Participants will choose to utilize a SAW in some capacity, but that only 6 Participants will choose to apply for an exception to use a non-SAW environment to access CAT Data through the user-defined direct query and bulk extraction tools. *See* note 513 and associated text *supra.*

[534] Because Participants seeking an exception are required to demonstrate the extent to which non-SAW environments are consistent with the detailed design specifications developed by the Plan Processor for SAWs, the Commission preliminarily believes that much of the monitoring required by the proposed amendments could be automated. Therefore, the Commission preliminarily believes that a senior systems analyst working 20 hours per week could perform the required monitoring for all non-SAW environments. Accordingly, the Commission preliminarily estimates that the Participants would together incur an ongoing annual expense of $302,640. 20 hours * 52 weeks = 1,040 hours. 1,040 hours for senior systems analyst = $302,640. Each Participant would therefore incur an ongoing annual expense of $12,105.60. $302,640/25 Participants = $12,105.60.

[535] The Commission preliminarily estimates that the Plan Processor would identify 5 non-compliance events per year for each non-SAW environment, or, assuming that only 6 Participants have non-SAW environments, 30 non-compliance events across all non-SAW environments. 5 events per non-SAW environment * 6 non-SAW environments = 30 events. For each non-compliance event, the Commission preliminarily estimates that the Plan Processor will spend 1.5 hours notifying the Participant of the identified non-compliance, including 0.5 hours by a senior systems analyst, 0.25 hours by a compliance manager, 0.25 hours by an attorney, and 0.5 hours by a senior business analyst. (0.5 hours for senior systems analyst = $145.50) + (0.25 for compliance manager = $79.25) + (0.25 for attorney = $106.50) + (0.5 hours for senior business analyst = $140.50) = $471.75 per event. This estimate is based on estimates set forth in the Regulation SCI Adopting Release for oral notifications of SCI events, as the Commission preliminarily believes that such notifications would typically be provided orally on a conference call or in a short email to all relevant parties. *See* Regulation SCI Adopting Release, *supra* note 498, at 72384. Accordingly, the Commission preliminarily estimates that the Participants would together incur an ongoing annual expense of $14,152.50. 30 events * $471.75 = $14,152.50. Each Participant would therefore incur an ongoing annual expense of $566.10. $14,152.50/25 Participants = $566.10. To the extent that the CISO consults with the Security Working Group regarding any non-compliance events, those costs have already been accounted for elsewhere. *See* Part III.D.2. *supra.*

[536] This estimate includes 10 hours by a senior systems analyst, 3 hours by a compliance attorney, and 2 hours by the chief information security office.

Accordingly, the Commission preliminarily estimates that the Participants would incur an ongoing annual burden of approximately 360 hours, or that each Participant would incur an ongoing annual burden of approximately 60 hours.[537]

4. Online Targeted Query Tool and Logging of Access and Extraction

The CAT NMS Plan currently states that the logs required by Appendix D, Section 8.1.1 of the CAT NMS Plan are to be submitted to the Operating Committee on a monthly basis. The Commission preliminarily estimates that the ongoing burden of Participants to review the newly required information in these logs, through the Operating Committee, would be an estimated 10 aggregate internal burden hours each month. The Commission preliminarily believes it is reasonable to estimate aggregate internal burden hours because the obligation to receive and review the logs required by Appendix D, Section 8.1.1 is with the Operating Committee itself and is not an obligation of individual Participants. This results in an estimated annual ongoing total burden of 120 burden hours for Participants,[538] or an annual burden of 4.8 burden hours for each Participant.[539]

The Commission preliminarily estimates that the Participants would incur an initial, one-time external expense of $87,960, or a per Participant expense of $3,518.40[540] for Plan Processor staff time required to make the initial necessary programming and systems changes to log delivery of results and the access and extraction of CAT Data, based on a preliminarily estimate that it would take 260 hours of Plan Processor staff time to implement these changes.[541] The Commission preliminarily estimates that the Participants would incur an annual ongoing external expense of $5,100, or $204 per Participant,[542] for Plan Processor staff time required to generate and provide the additional information required by proposed Section Appendix D, Section 8.1.1, which the Commission preliminarily estimates to be 2 hours for each monthly report or 24 hours annually.[543]

5. CAT Customer and Account Attributes

The Commission preliminarily estimates that the one-time burden to Industry Members to modify systems to report a Transformed Value to the CAT instead of SSNs or ITINs per the proposed amendment to Section 6.4(d)(ii)(D), will be minimal. However, the Commission preliminarily believes there will be a cost to install and test the transformation logic. As proposed, Industry Members would use the CCID Transformation Logic in conjunction with an API provided by the Plan Processor and the only cost to Industry Members will be installation and testing of the transformation logic. The Commission estimates that the one-time burden to each Industry Member to install and test this technology will be 80 staff burden hours per Industry Member or 120,000 hours in the aggregate.[544] The Commission believes that the on-going annual burden to report the Transformed Value will be the same as the burden to report a SSN or ITIN once the CCID Transformation Logic is installed.

The Commission estimates that the modifications necessary to the CAT System to develop the CCID Subsystem to generate Customer-IDs using Transformed Values, as opposed to SSNs or ITINs, would result in an initial, one-time aggregate external cost of $650,052 for the Participants,[545] or $26,002 for each Participant.[546] This estimated one-time aggregate external cost represents ten percent of Commission's estimate in the CAT NMS Approval Order to develop the Central Repository, of which the CCID Subsystem is a part.[547]

The CAT NMS Plan, Article VI, Section 6.6(b)(ii)(A), currently requires the CCO to oversee the Regular Written Assessment of the Plan Processor's performance, which must be provided to the Commission at least annually and which must include an evaluation of the performance of the CAT.[548] As proposed, Appendix D, Section 9.1 requires an evaluation of the overall performance and design of the CCID Subsystem and the process for creating Customer-ID(s) to be included in each such annual Regular Written Assessment of the Plan Processor's Performance.

In the CAT NMS Plan Adopting Release, the Commission estimated that the annual on-going cost of preparing the Regular Written Assessment would be 171.43 ongoing burden hours per Participant, plus $1,000 of external costs for outsourced legal counsel per Participant per year, for an estimated aggregate annual ongoing burden of approximately 3,600.03 hours and an estimated aggregate ongoing external cost of $21,000.[549] The amendments propose a new method for creating a Customer-ID that involve a new CCID

To the extent that the CISO consults with the Security Working Group regarding notifications of material changes to security controls, those costs have already been accounted for elsewhere. *See* Part III.D.2. *supra*.

[537] 15 hours per notification * 4 notifications per year = 60 hours per year. 60 hours per year * 6 non-SAW environments = 360 hours.

[538] 12 months × 10 hours = 120 burden hours.

[539] 120 burden hours/25 Participants = 4.8 burden hours per Participant.

[540] $87,960/25 Participants = $3,518.40 per Participant.

[541] The estimated 260 hours of Plan Processor staff time include 160 hours by a Senior Programmer, 40 hours by a Senior Database Administrator, 40 hours for a Senior Business Analyst and 20 hours for an Attorney. The Commission is basing this figure on the estimated internal burden for a broker-dealer that handles orders subject to customer specific disclosures required by Rule 606(b)(3) to both update its data capture systems in-house and format the report required by Rule 606. *See* Securities Exchange Act Release No. 84528 (November 2, 2018), 83 FR 58338, 58383 (November 19, 2018) (''Rule 606 Adopting Release''). The Commission preliminarily estimates that the initial, one-time external expense for Participants will be $87,960 = (Senior Programmer for 160 hours at $339 an hour = $54,240) + (Senior Database Administrator for 40 hours at $349 an hour = $13,960) + (Senior Business Analyst for 40 hours at $281 an hour = $11,240) + (Attorney for 20 hours at $426 an hour = $8,520).

[542] $5,100/25 Participants = $204 per Participant.

[543] The estimated 2 hours of Plan Processor staff time include 1 hour by a Programmer Analyst and 1 hour by a Junior Business Analyst. This estimate would apply monthly, meaning the annual ongoing estimate would be 24 hours of Plan Processor staff time, which would include 12 hours by a Programmer Analyst and 12 hours by a Junior Business Analyst. The Commission is basing this figure on the estimated internal burden for broker-dealer that handle relevant orders and respond in-house to a customer request under Rule 606(b)(3). *See* Rule 606 Adopting Release, *supra* note 541, at 58385. The Commission preliminarily estimates the annual ongoing external cost to generate and provide the proposed information on logs would be $5,100 = (Programmer Analyst for 12 hours at $246 per hour = $2,952) + (Junior Business Analyst for 12 hours at $179 an hour = $2,148).

[544] 80 burden hours × 1,500 Industry Members = 120,000.

[545] The Commission preliminarily estimates the one-time aggregate external cost to update the CAT System to ingest and use the Transformed Value reported by Industry Members would be $650,052. The Commission preliminarily believes that this modification will take an estimated 2,101 hours of Plan Processor staff time including 130 hours by the CCO, 130 hours by the CISO, 602 hours by a Senior Programmer and 1239 hours by a Program Analyst. Accordingly, the Commission preliminarily estimates that the Participants would together incur a one-time aggregated external cost $650,052. (Chief Compliance Officer for 130 hours at $543 per hour = $70,590) + (Chief Information Security Officer for 130 hours at $543 per hour = $70,590) + (Senior Programmer for 602 hours at $339 = $204,078) + (Program Analyst for 1239 hours at $246 = $304,794) = $650,052. $650,052/25 Participants = $26,002/Participant.

[546] $650,052/25 Participants = $26,002 per Participant.

[547] *See* CAT NMS Approval Order, *supra* note 3, at 84918. (''[T]he Commission estimates that the initial one-time cost to develop the Central Repository would be an aggregate initial external cost to the Participants of $65 million, or $3,095,238.09 per Participant.'')

[548] *See* CAT NMS Plan, *supra* note 3, Section 6.6(b)(ii)(A).

[549] *See* CAT NMS Plan Approval Order, *supra* note 3, at 84925–6

Subsystem, which performs a two-phase transformation of a Customer's ITIN/SSN in order to create a Customer-ID; thus, the Commission preliminarily believes there is added complexity to the process for creating a Customer-ID. Due to this increase in complexity, the Commission preliminarily estimates that assessment the CCID subsystem require an additional 50 ongoing burden hours of internal legal, compliance, business operations, and information technology, per Participant, for an aggregate ongoing burden of approximately 1,250 hours.[550]

6. Customer Identifying Systems Workflow

The Commission preliminarily believes that the requirement that the Plan Processor maintain a full audit trail of access to Customer Identifying Systems by each Participant and the Commission (who accessed what data within each Participant, and when) and provide such audit trail of each Participant's and the Commission's access to each the Participant and the Commission for their respective users on a monthly basis, and the requirement to provide the Operating Committee with the daily reports that list all users who are entitled to Customer Identifying Systems access on a monthly basis [551] will require 4 hours of Plan Processor Staff time per report and will result in an aggregate ongoing annual external cost to the Participants of $373,464 per year or $14,939 per Participant.[552] This cost represents approximately $700 per monthly report—one monthly report to the Operating Committee, and the daily reports of all users to the Operating Committee on a monthly basis. This estimate recognizes that Plan Processor currently is required to collect the audit trail information and create the daily reports of all users entitled to access Customer and Account Attributes. The Commission does not believe that the compilation of new reports will require the Plan Processor to gather any new information, but would however require the re-packaging of information to provide to the Participants and the Operating Committee according to the amended requirements of Appendix D, Section 9.1.[553]

The Commission cannot precisely estimate the number of Participants that will apply for authorization to use Programmatic CAIS Access and/or Programmatic CCID Subsystem Access.[554] As noted above, the Commission does not believe that all the Participants require programmatic access to conduct effect surveillance. The Commission preliminarily believes that number of Participants that may apply for such access will range from 1 to 25 Participants. The Commission is taking a conservative approach and preliminarily estimating that 25 Participants will submit an application.

In connection with the application for authorization, the Commission preliminarily estimates that each of these Participants would incur a one-time burden of 50 burden hours to prepare each application for authorization to use Programmatic CAIS Access or Programmatic CCID Subsystem Access and have that application approved by the Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation).[555] Accordingly, with respect to preparation and review of the application that seeks Programmatic CAIS and/or Programmatic CCID Subsystem Access, the Commission preliminarily estimates that the Participants would incur a one-time burden of approximately 1,250 hours per application.[556]

7. Proposed Confidentiality Policies, Procedures and Usage Restrictions

The Commission preliminarily believes that proposed Section 6.5(g) creates three different types of paperwork burdens: (i) A third-party disclosure burden relating to preparation, review and public disclosure of the Proposed Confidentiality Policies; (ii) a recordkeeping burden associated with the related documentation, procedures, and usage restriction controls required by the Proposed Confidentiality Policies; and (iii) a reporting burden associated with the annual requirement to provide the Commission an examination report in Section 6.5(g)(v).

Data Confidentiality Policies—Identical Policies

The Commission preliminarily estimates that the hourly burden of preparing, reviewing and approving the Proposed Confidentiality Policies would be an aggregate 500 hours for the Participants, or 20 hours for each individual Participant.[557] This estimation includes burden hours associated with: (i) Preparing and reviewing the identical policies required by Section 6.5(g)(i); (2) making the policies publicly available on each of the Participant websites, or collectively on the CAT NMS Plan website, redacted of sensitive proprietary information as required by Section 6.5(g)(iv); and (3) Operating Committee review and approval as required by Section 6.5(g)(vi).[558] The Commission believes that Participants already have individual policies and procedures relating to the confidentiality of CAT Data, as required by existing provisions of the CAT NMS Plan, and Participants can use these existing policies and procedures in order to help prepare, review and approve the policies and procedures required by proposed Section 6.5(g)(i).

The Commission preliminarily estimates that it would require 10 hours by the CCO and 10 hours by the CISO, both employees of the Plan Processor and not the Participants, to review the Proposed Confidentiality Policies, as required by proposed Sections 6.2(a)(v)(R) and 6.2(b)(viii). The Commission preliminarily estimates that this would result in a one-time external cost of $10,860 for Participants,[559] or $434.40 for each Participant.[560] The Commission also

[550] 50 burden hours × 25 Participants = 1,250 hours.

[551] *See* proposed Appendix D, Section 4.1.6.

[552] The Commission estimates that each monthly report will require 2 hours by an Operations Specialist, 1 hour by an Attorney, and 1 hour by the Chief Compliance Officer. The ongoing aggregate cost for Participants is preliminarily estimated to be $373,464. (2 hours for Operational Specialist × $140 = $280) + (1 hours for compliance attorney × $374 = $374) + (1 hour for chief compliance officer × $543 = $543) = $1,197. $1,197 × 12 months = $14,364. $14,364 × 25 Participants + the Commission = $373,464. Each Participant would therefore incur an ongoing annual expense of $14,939 ($373,464/25 Participants).

[553] The Commission preliminarily believes that creation of the monthly reports documentation necessary for ''allow listing'' could require legal advice, discussions with staff familiar with CAT security and higher level discussions and analysis. The estimated 30 hours of Plan Processor staff time include 5 hours by an Attorney, 5 hours by an Operations Specialist, 10 hours by the Chief Compliance Officer and 10 hours by the Chief Information Security Officer. The initial, one-time aggregate external cost for Participants is preliminarily estimated to be $13,690 = (Attorney for 5 hours at $426 per hour = $2,130) + (Operations Specialist for 5 hours at $140 per hour = $700) + (Chief Compliance Officer for 10 hours at $543 per hour = $5,430) + (Chief Information Security Officer for 10 hours at $543 per hour = $5,430).

[554] *See* proposed Appendix D, Section 4.1.6 (Customer Identifying Systems Workflow).

[555] This estimate of 50 burden hours include 15 hours by an Attorney, 10 hours by a Compliance Manager, 10 hours by an Operations Specialist, 15 hours by a Chief Compliance Officer.

[556] 50 hours per application × 25 Participants = 1,250 hours.

[557] 500 hours/25 Participants = 20 hours per Participant.

[558] To the extent that the CISO consults with the Security Working Group regarding the development and approval of the Proposed Confidentiality Policies, those burdens and costs have already been accounted for elsewhere. *See* Part III.D.2. *supra.*

[559] $10,860 = (Chief Compliance Officer for 10 hours at $543 per hour = $5,430) + (Chief Information Security Officer for 10 hours at $543 per hour = $5,430).

[560] $10,860/25 Participants = $434.40 per Participant.

preliminarily believes that the Participants will consult with outside legal counsel in the drafting of the Proposed Confidentiality Policies, and estimates this external cost to be $50,000, or $2,000 [561] for each Participant.[562] The Commission believes that the total initial one-time external cost burden for each Participant will be $2,434.40, or $60,860 for all Participants.[563]

The Commission preliminarily estimates that Participants will require 100 burden hours annually to comply with proposed Section 6.5(g)(ii), which requires the Participants to periodically review the effectiveness of the policies required by Section 6.5(g)(i), including by using the monitoring and testing protocols documented within the policies pursuant to Section 6.5(g)(i)(J), and take prompt action to remedy deficiencies in such policies. The Commission preliminarily believes it is appropriate to estimate that review of and updates to the Proposed Confidentiality Policies should be one-fifth the burden hours necessary for initially creating and approving the Proposed Confidentiality Policies because the Commission preliminarily believes it should take substantially less time and effort to review and update the Proposed Confidentiality Policies than in initially creating and approving them. This estimated burden includes any updates to the Proposed Confidentiality Policies initiated by the Participants, based on their review pursuant to proposed Section 6.5(g)(ii) or based on changed regulatory needs.

For purposes of this Paperwork Reduction Act analysis only, the Commission preliminarily estimates that the Participants would revise the Proposed Confidentiality Policies once a year, which would require review by the CCO and CISO of the Plan Processor, as required by proposed Sections 6.2(a)(v)(R) and 6.2(b)(viii). The Commission preliminarily believes that the CCO and CISO would require less time to review subsequent updates to the Proposed Confidentiality Policies, so the Commission preliminarily estimates that it would require 5 hours of review by the CCO and 5 hours of review by the CISO, which would result in an external cost of $5,430 for the Participants,[564] and $217.20 for each Participant annually.[565] In addition, the Commission preliminarily estimates that Participants will consult with outside legal counsel in updating the Proposed Confidentiality Policies, and preliminarily estimates this external cost to be $5,000.[566] In total, the Commission preliminarily estimates an aggregate external cost of $10,430 for all Participants related to reviewing and updating the Proposed Confidentiality Policies, or $417.20 per Participant.[567]

Data Confidentiality Policies—Procedures and Usage Restriction Controls

The Commission preliminarily estimates that each Participant would require an average of 282 burden hours to initially develop and draft the procedures and usage restriction controls required by proposed Section 6.5(g)(i).[568] The Commission preliminarily believes that this estimation should include all initial reporting burdens associated with the procedures and usage restriction controls required by Section 6.5(g)(i), such as the requirement to implement effective information barriers between such Participants' Regulatory Staff and non-Regulatory Staff with regard to access and use of CAT Data, the requirement to document each instance of access by non-Regulatory Staff as proposed in Section 6.5(g)(i)(E) and the requirement that Participants must be able to demonstrate that a Participant's ongoing use of Programmatic CAIS and/or CCID Subsystem access is in accordance with the Customer Identifying Systems Workflow as proposed in Section 6.5(g)(i)(I).

The Commission preliminarily estimates that the ongoing annual burden of maintaining and reviewing the procedures and usage restriction controls required by Section 6.5(g)(i), including by using monitoring and testing protocols documented within the policies pursuant to Section 6.5(g)(i)(J), and taking prompt action to remedy deficiencies in such policies, procedures and usage restriction controls as required by proposed Section 6.5(g)(ii), would be 87 burden hours for each Participant,[569] or 2,175 burden hours for all Participants.[570] The Commission preliminarily believes that this estimation includes all ongoing reporting burdens associated with the procedures and usage restriction controls required by Section 6.5(g)(i), such as the requirement to document each instance of access by non-Regulatory Staff as proposed in Section 6.5(g)(i)(E) or the requirement that Participants must be able to demonstrate that a Participant's ongoing use of Programmatic CAIS and/or CCID Subsystem access is in accordance with the Customer Identifying Systems Workflow as proposed in Section 6.5(g)(i)(I). This estimation also includes the hourly burden associated with proposed Section 6.5(g)(iii), which requires each Participant, as reasonably practicable, and in any event within 24 hours of becoming aware, report to the Chief Compliance Officer, in accordance with the guidance provided by the Operating Committee, any instance of noncompliance with the policies, procedures, and usage restriction controls adopted by such Participant pursuant to Section 6.5(g)(i).[571]

---

[561] $50,000/25 Participants = $2,000 per Participant.

[562] $50,000 = (100 hours at $500 an hour). For purposes of this Paperwork Reduction Act analysis, the Commission is estimating the cost of outside legal counsel to be $500 an hour.

[563] $2,434.40 × 25 Participants = $60,860.

[564] $5,430 = (Chief Compliance Officer for 5 hours at $543 per hour = 2,715) + (Chief Information Security Officer for 5 hours at $543 per hour = $2,715).

[565] $5,430/25 Participants = $217.20 per Participant.

[566] $5,000 = (outside legal counsel for 10 hours at $500 an hour).

[567] $10,430/25 Participants = $417.20 per Participant.

[568] This estimate of 282 burden hours include 96 hours by an Attorney, 96 hours by a Compliance Manager, 30 hours by a Senior Systems Analyst, 30 hours by an Operations Specialist, 20 hours by a Chief Compliance Officer and 10 hours by a Director of Compliance. The Commission is basing this estimate on the estimated burden for SCI entities, that participated in the ''ARP Inspection Program,'' to initially develop and draft the policies and procedures required by Rule 1001(a) (except for the policies and procedures for standards that result in systems being designed, developed, tested, maintained, operated, and surveilled in a matter that facilitates the successful collection, processing, and dissemination of market data). *See* Regulation SCI Adopting Release, *supra* note 54 at 72377. The Commission believes this comparison is appropriate because Participants should already have some internal policies and procedures that could be enhanced to comply with the new proposed requirements of Section 6.5(g)(i).

[569] This estimate of 87 hours includes 28 hours by an Attorney, 28 hours by a Compliance Manager, 8 hours by a Senior Systems analyst, 8 hours by an Operations Specialist, 10 hours by a Chief Compliance Officer and 5 hours by a Director of Compliance. This estimate of 87 hours annually is based on the estimated burden for SCI entities, that participated in the ''ARP Inspection Program,'' to review and update policies and procedures required by Rule 1001(a) (except for the policies and procedures for standards that result in systems being designed, developed, tested, maintained, operated, and surveilled in a matter that facilitates the successful collection, processing, and dissemination of market data). *See* Regulation SCI Adopting Release, *supra* note 54, at 72377.

[570] 87 burden hours × 25 Participants = 2,175 burden hours.

[571] Proposed Section 6.5(g)(iii) also requires reporting of any instance a Participant becomes aware of a breach of the security of the CAT, but this obligation is a pre-existing obligation and not a new information collection requirement. *See* CAT NMS Plan, *supra* note 3, at Section 6.5(f)(iii).

Data Confidentiality Policies—Examination Report

The Commission preliminarily believes that Participants will incur annual hour burdens to comply with proposed Section 6.5(g)(v), which the Commission preliminarily estimates to be 15 hours for each Participant, or 375 hours for all Participants.[572] The Commission believes that this burden hour estimation includes the staff time necessary to engage an independent accountant, staff time required to allow the independent auditor to review compliance and prepare the examination report and the staff time required to submit the examination report to the Commission. The Commission believes that proposed Section 6.5(g)(v) does not require Participants to review and respond to the examination report, and only requires a Participant to submit the prepared examination report to the Commission. However, the Commission notes that such examination report may require Participants to take action pursuant to proposed Section 6.5(g)(ii) or Section 6.5(g)(iii), including updating policies, procedures and usage restrictions, but such burdens are accounted for in other areas of this Paperwork Reduction Act analysis.[573]

The Commission preliminarily estimates that the external cost of compliance with Section 6.5(g)(v), which requires each Participant to engage an independent accountant to perform an examination of compliance with the policies required by Section 6.5(g)(i) and submit the examination report to the Commission, would be $57,460 for each Participant,[574] or $1,436,500 for all Participants.[575] The Commission preliminarily believes that this would be the average cost of engaging an independent accountant to perform the necessary examination on an annual basis.

8. Secure Connectivity—''Allow Listing''

The Commission estimates that the proposed amendment to Appendix D, Section 4.1.1 of the CAT NMS Plan, requiring the Plan Processor to implement capabilities to allow access (*i.e.,* ''allow list'') only to those countries or more granular access points where CAT reporting or regulatory use is both necessary and expected would result in an initial, one-time aggregate external cost of $13,690 for the Participants, or $547.60 for each Participant.[576] This cost represents expenses associated with Plan Processor staff time required to develop the list of discrete access points that are approved for use, which the Commission estimates would be 30 hours of staff time.[577] In addition, the Commission estimates that Participants will incur an aggregate ongoing external cost burden of $1,226, or $49.04 for each Participant,[578] for Plan Processor staff time required to maintain and update the list of discrete access points, which the Commission estimates would be 3 hours of staff time.[579]

The Commission estimates that the proposed requirement that the Plan Processor develop policies and procedures to allow access if the source location for a particular instance of access cannot be determined technologically, as required by proposed Appendix D, Section 4.1.1 of the CAT NMS Plan, would require an aggregate one-time initial external cost of $19,430 for the Participants, or $777.20 for each individual Participant.[580] This cost represents expenses associated with Plan Processor staff time required to create these policies and procedures, which the Commission estimates would be 50 hours of staff time.[581] Further, the Commission estimates that the Participants will incur an aggregate ongoing external cost of $1,943, or $77.72 for each individual Participant,[582] for Plan Processor staff time required to maintain, update and enforce these policies and procedures, which the Commission estimates would be 5 hours of staff time.[583]

9. Breach Management Policies and Procedures

The Commission preliminarily believes that the proposed changes to Section 4.1.5 of the CAT NMS Plan creates new information collections associated with revising, maintaining and enforcing the policies and procedures and the cyber incident response plan in a manner consistent with the proposed requirements of Section 4.1.5 and the breach notification requirement.

The Plan Processor is already required to establish policies and procedures and a cyber incident response plan pursuant to Section 4.1.5 of the CAT NMS Plan, so the Commission believes it is appropriate to estimate a burden of revising breach management policies and procedures and the cyber incident response plan relate to the new

[572] 15 hours × 25 Participants = 375 hours.

[573] *See supra* Part III.D.5.

[574] The Commission is basing this estimate based on the number of estimated hours of work by a Manager Internal Audit would be required to comply with Rule 1003(b)(1) of Regulation SCI, which requires each SCI entity to conduct an SCI review of its compliance with Regulation SCI not less than once each calendar year, with certain exceptions. *See* Regulation SCI Adopting Release, *supra* note 54, at 72391. Specifically, the Commission preliminarily estimates it would require 170 hours by a Manager Internal Audit to perform the examination. The preliminary estimated cost of engaging an independent accountant to perform the examination of compliance and submit an examination report is $57,460 (Manager Internal Audit at $338 an hour for 170 hours).

[575] $57,460 × 25 Participants = $1,436,500.

[576] $13,690/25 Participants = $547.60 per Participant.

[577] The Commission preliminarily believes that creation of the documentation necessary for ''allow listing'' could require legal advice, discussions with staff familiar with CAT security and higher level discussions and analysis. The estimated 30 hours of Plan Processor staff time include 5 hours by an Attorney, 5 hours by an Operations Specialist, 10 hours by the Chief Compliance Officer and 10 hours by the Chief Information Security Officer. The initial, one-time aggregate cost for Participants is preliminarily estimated to be $ = $13,690 (Attorney for 5 hours at $426 per hour = $2,130) + (Operations Specialist for 5 hours at $140 per hour = $700) + (Chief Compliance Officer for 10 hours at $543 per hour = $5,430) + (Chief Information Security Officer for 10 hours at $543 per hour = $5,430).

[578] $1,226/25 Participants = $49.04 per Participant.

[579] The Commission believes it is appropriate to estimate that the Plan Processor staff time required to maintain and update the list as approximately one-tenth the staff time required to initially create the list. Specifically, the estimated aggregate ongoing external cost is based on an estimate of 3 hours of Plan Processor staff time include 1 hour by an Operations Specialist, 1 hour by the Chief Compliance Officer and 1 hour by the Chief Information Security Officer. The estimated aggregate ongoing external cost is preliminarily estimated to be $1,226 = (Operations Specialist for 1 hour at $140) + (Chief Compliance Officer for 1 hour at $543) + (Chief Information Security Officer for 1 hour at $543).

[580] $19,430/25 Participants = $777.20 per Participant.

[581] The estimate 50 hours of Plan Processor staff time include 10 hours by an Attorney, 10 hours by a Senior Systems Analyst, 10 hours by an Operations Specialist, 10 hours by the Chief Compliance Officer and 10 hours by the Chief Information Security Officer. The initial, one-time aggregate cost for Participants is preliminarily estimated to be $19,430 = (Attorney for 10 hours at $426 per hour = $4,260) + (Senior Systems Analyst for 10 hours at $291 per hour = $2,910) + (Operations Specialist for 10 hours at $140 per hour = $1,400) + (Chief Compliance Officer for 10 hours at $543 per hour = $5,430) + (Chief Information Security Officer for 10 hours at $543 per hour = $5,430).

[582] $1,943/25 Participants = $77.72 per Participant.

[583] The Commission believes it is appropriate to estimate that the Plan Processor staff time required to maintain, update and enforce these policies and procedures should be approximately one-tenth the staff time required to initially create these policies and procedures. Specifically, the Commission estimates 5 hours of Plan Processor staff time that includes 1 hour by an Attorney, 1 hour by a Senior Systems Analyst, 1 hour by an Operations Specialist, 1 hour by the Chief Compliance Officer and 1 hour by the Chief Information Security Officer. The ongoing external cost is preliminarily estimated to be $1,943 = (Attorney for 1 hour at $426) + (Senior Systems Analyst for 1 hour at $291) + (Operations Specialist for 1 hour at $140) + (Chief Compliance Officer for 1 hour at $543) + (Chief Information Security Officer for 1 hour at $543).

elements required by proposed Section 4.1.5 of the CAT NMS Plan. The Commission preliminarily believes that these requirements would result in a one-time external cost of $49,805 for Participants, or $1,992.20 per Participant,[584] based on the Commission's estimation that it would require approximately 124 Plan Processor staff hours to incorporate the new elements required by proposed Section 4.1.5 of the CAT NMS Plan.[585] The Commission believes that there would be an initial internal burden of 25 hours for the Participants, or 1 hour per Participant [586] for review and approval of the updated cyber incident response plan by the Operating Committee.

Further, the Commission estimates that the Participants will incur an aggregate ongoing external cost of $42,205, or $1,688.20 for each individual Participant,[587] for Plan Processor staff time required to maintain, update and enforce these policies and procedures and the cyber incident response plan, which the Commission estimates would be 103 hours of Plan Processor staff time annually.[588] This external cost estimate includes enforcement of the requirements of the cyber incident response plan relating to the proposed breach notification requirement,[589] as well as staff time for documenting breaches that the Plan processor reasonably estimates would have no impact or a de minimis impact on the Plan Processor's operations or on market participants.[590]

Cumulatively, the Commission preliminarily estimates that to implement the changes proposed in Section 4.1.5 of the CAT NMS Plan, each Participant will incur an initial hourly burden of 1 hour, or 25 hours for all Participants, an initial one-time external cost burden of $1,992.20, or $49,805 for all Participants, and an ongoing annual external cost burden of $42,205 for all Participants, or $1,688.20 for each individual Participant.[591]

10. Customer Information for Allocation Report Firm Designated IDs

The Commission preliminarily believes that this requirement is already accounted for in the existing information collections burdens associated with Rule 613 and the CAT NMS Plan Approval Order submitted under OMB number 3235–0671.[592] Specifically, the CAT NMS Plan Approval Order takes into account requirements on broker-dealer members to record and report CAT Data to the Central Repository in accordance with specified timelines, including customer information.

E. Collection of Information Is Mandatory

Each collection of information discussed above would be a mandatory collection of information.

F. Confidentiality of Responses to Collection of Information

The Commission preliminarily believes that all information required to be submitted to the Commission under the proposed amendments, including the evaluation of the Plan Processor's performance under proposed Section 6.6(b)(ii)(B)(3), the examination reports required by proposed Section 6.5(g)(v), the application materials for non-SAW environments as required under proposed Section 6.13(d), the annual Regular Written Assessment of the Plan Processor under proposed Section 6.6(b)(ii)(A) and the application for Programmatic CAIS Access and Programmatic CCID Subsystem Access under proposed Appendix D, Section 4.1.6 should be protected from disclosure subject to the provisions of applicable law.[593]

Public disclosure of other collections of information could raise concerns about the security of the CAT and therefore the Commission preliminarily believes that the Plan Processor and the Participants, as applicable, would keep these materials confidential.[594] Such

[584] $49,805/25 Participants = $1,992.20 per Participant.

[585] The estimate of 124 hours of Plan Processor staff time include 32 hours by an Attorney, 32 hours by a Compliance Manager, 10 hours by a Senior Systems Analyst, 10 hours by an Operations Specialist, 20 hours by the Chief Compliance Officer and 20 hours by the Chief Information Security Officer. The Commission is basing this estimation on the estimated initial burden to implement corrective action processes required by Rule 1002(a) of Regulation SCI. *See* Regulation SCI Adopting Release, *supra* note 54, at 72393. The total estimated one-time external cost for Participants is $49,805 = (Attorney for 32 hours at $426 per hour = $13,631) + (Compliance Manager for 32 hours at $317 per hour = $10,144) + (Senior Systems Analyst for 10 hours at $291 per hour = $2,910) + (Operations Specialist for 10 hours at $140 per hour = $1,400) + (Chief Compliance Officer for 20 hours at $543 per hour = $10,860) + (Chief Information Security Officer at $543 per hour = $10,860).

[586] 25 hours/25 Participants = 1 hour per Participant.

[587] $42,205/25 Participants = $1,688.20 per Participant.

[588] The estimated aggregate ongoing external cost is based on an estimate of 103 hours of Plan Processor staff time that includes 23 hours by an Attorney, 23 hours by a Compliance Manager, 16 hours by a Senior Systems Analyst, 3 hours by an Operations Specialist, 9 hours by an Assistant General Counsel, 17 hours by the Chief Compliance Officer and 12 hours by the Chief Information Security Officer. The Commission is basing this estimate on the ongoing burden to implement corrective action processes required by Rule 1002(a) of Regulation SCI and estimated burden for providing written notifications of Regulation SCI events under Rule 1002(b)(2). *See* Regulation SCI Adopting Release, *supra* note 54 at 72384 and 72393–94. The estimated aggregate ongoing external cost is preliminarily estimated to be $42,205 = (Attorney for 23 hours at $426 per hour = $9,798) + (Compliance Manager for 23 hours at $317 per hour = $7,291) + (Senior Systems Analyst for 16 hours at $291 per hour = $4,656) + (Operations Specialist for 3 hours at $140 per hour = $420) + (Assistant General Counsel for 9 hours at $477 per hour = $4,293) + (Chief Compliance Officer for 17 hours at $543 per hour = $9,231) + (Chief Security Officer for 12 hours at $543 per hour = $6,516).

[589] The Commission preliminarily estimates that this requirement will require 34 hours of staff time annually from the Plan Processor, resulting in an ongoing annual external cost burden of $13,756 for the Participants, or $550.24 for each Participant ($13,756/25 Participants). The 34 hours include 8 hours by an Attorney (Attorney for 8 hours at $426 an hour = $3,408), 8 hours by a Compliance Manager (Compliance Manager for $317 an hour = $2,536), 7 hours by a Senior Systems Analyst (Senior Systems Analyst for 7 hours at $291 an hour = $2,037), 3 hours by an Assistant General Counsel (Assistant General Counsel for 3 hours at $477 per hour = $1,431), 4 hours by a Chief Compliance Officer (Chief Compliance Officer for 4 hours at $543 per hour = $2,172) and 4 hours by the Chief Information Security Officer (Chief Information Security Officer for 4 hours at $543 per hour = $2,172) = $13,756. This estimate relates only to the proposed requirement that the Plan Processor provide breach notifications and does not include other costs related to breaches, such as determination of whether a breach has occurred or assessing the scope of any breach, which is already required by the CAT NMS Plan.

[590] The Commission preliminarily estimates that this requirement will require 30 hours of staff time annually from the Plan Processor, resulting in an ongoing annual external cost of $12,324 to the Participants, or $492.96 per Participant ($12,324/25 Participants). The 30 hours include 6 hours by an Attorney, 6 hours by a Compliance Manager, 6 hours by a Senior Systems Analyst, 6 hours by an Assistant General Counsel, 3 hours by the Chief Compliance Officer and 3 hours by the Chief Information Security Officer. The ongoing external cost of this obligation is preliminarily estimated to be $12,324 = (Attorney for 6 hours at $426 per hour = $2,556) + (Compliance Manager for 6 hours at $317 per hour = $1,902) + (Senior Systems Analyst for 6 hours at $291 per hour = $1,746) + (Assistant General Counsel for 6 hours at $477 per hour = $2,862) + (Chief Compliance Officer for 3 hours at $543 per hour = $1,629) + (Chief Information Security Officer for 3 hours at $543 per hour = $1,629).

[591] $42,205/25 Participants = $1,688.20 per Participant.

[592] *See,* CAT NMS Plan Approval Order, *supra* note 3, at 84911–43.

[593] *See, e.g.,* 5 U.S.C. 552 *et seq.;* 15 U.S.C. 78x (governing the public availability of information obtained by the Commission).

[594] The Participants must comply with the security plan developed by the Plan Processor pursuant to Appendix D, Section 4.1 of the CAT NMS Plan and any security-related policies and procedures developed pursuant to Regulation SCI. *See* CAT NMS Plan, *supra* note 3, at Appendix D, Section 4.1 (requiring the Plan Processor to provide to the Operating Committee a comprehensive security plan, including a process for responding to security incidents and reporting of such incidents); 17 CFR 242.1001 (requiring each SCI entity to establish, maintain, and enforce written policies and procedures reasonably designed to ensure that

Continued

collections of information include the development of SAW-specific provisions for the CISP and related policies, procedures, and security controls required pursuant to proposed Section 6.13(a); the development of the detailed design specifications required pursuant to proposed Section 6.13(b)(i); the evaluation of each Participant's SAW and related notification to the Operating Committee under proposed Section 6.13(b)(ii), the monitoring of SAWs and non-SAW environments and notification of non-compliance events required by proposed Section 6.13(c)(i) and proposed Section 6.13(d)(iii); the collection of application materials for an exception to the proposed SAW usage requirements pursuant to proposed Section 6.13(d); the development of policies and procedures for review of such applications and the issuance of exceptions to the SAW usage requirements by the CISO and the CCO pursuant to proposed Section 6.13(d); and the audit trail of access to Customer Identifying Systems and the daily reports of users entitled to access Customer Identifying Systems as required by the proposed amendments to Section 4.1.6 of Appendix D.

Finally, the policies required by proposed Section 6.5(g)(i) would not be confidential. Rather, the proposed rule would require Participants to make the policies required by Section 6.5(g)(i) publicly available on each of the Participant websites, or collectively on the CAT NMS Plan website, redacted of sensitive proprietary information.

G. Retention Period for Recordkeeping Requirements

National securities exchanges and national securities associations would be required to retain records and information pursuant to Rule 17a–1 under the Exchange Act.[595] The Plan Processor would be required to retain the information reported to Rule 613(c)(7) and (e)(6) for a period of not less than five years.[596]

H. Request for Comments

Pursuant to 44 U.S.C. 3506(c)(2)(B), the Commission solicits comments to:

175. Evaluate whether the proposed collections of information are necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility;

176. Evaluate the accuracy of our estimates of the burden of the proposed collection of information;

177. Determine whether there are ways to enhance the quality, utility, and clarity of the information to be collected; and

178. Evaluate whether there are ways to minimize the burden of collection of information on those who are to respond, including through the use of automated collection techniques or other forms of information technology.

Persons submitting comments on the collection of information requirements should direct them to the Office of Management and Budget, Attention: Desk Officer for the Securities and Exchange Commission, Office of Information and Regulatory Affairs, Washington, DC 20503, and should also send a copy of their comments to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549–1090, with reference to File Number 4–698. Requests for materials submitted to OMB by the Commission with regard to this collection of information should be in writing, with reference to File Number 4–698 and be submitted to the Securities and Exchange Commission, Office of FOIA/PA Services, 100 F Street NE, Washington, DC 20549–2736. As OMB is required to make a decision concerning the collection of information between 30 and 60 days after publication, a comment to OMB is best assured of having its full effect if OMB receives it within 30 days of publication.

IV. Economic Analysis

Section 3(f) of the Exchange Act requires the Commission, whenever it engages in rulemaking and is required to consider or determine whether an action is necessary or appropriate in the public interest, to consider, in addition to the protection of investors, whether the action would promote efficiency, competition, and capital formation.[597] In addition, Section 23(a)(2) of the Exchange Act requires the Commission, when making rules under the Exchange Act, to consider the impact such rules would have on competition.[598] Exchange Act Section 23(a)(2) prohibits the Commission from adopting any rule that would impose a burden on competition not necessary or appropriate in furtherance of the purposes of the Exchange Act. The discussion below addresses the likely economic effects of the proposed rule, including the likely effect of the proposed rule on efficiency, competition, and capital formation.

The Commission is proposing amendments to the CAT NMS Plan that would (1) define the scope of the current information security program; (2) require the Operating Committee to establish and maintain a security-focused working group; (3) require the Plan Processor to create SAWs, 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 that will enable Participants to use the user-defined direct query and bulk extract tools in other environments; (4) limit the amount of CAT Data that can be extracted from the Central Repository outside of a secure analytical workspace through the online targeted query tool described in Section 6.10(c)(i)(A) of the CAT NMS Plan and require the Plan Processor to implement more stringent monitoring controls on such data; (5) impose requirements related to the reporting of certain PII; (6) define the workflow process that should be applied to govern access to customer and account attributes that will still be reported to the Central Repository; (7) modify and supplement existing requirements relating to Participant policies and procedures regarding the confidentiality of CAT Data; (8) refine the existing requirement that CAT Data be used only for regulatory or surveillance purposes; (9) codify existing practices and enhance the security of connectivity to the CAT infrastructure; (10) require the formal cyber incident response plan to incorporate corrective actions and breach notifications; (11) amend reporting requirements relating to Firm Designated IDs and Allocation Reports; and (12) clarify that Appendix C of the CAT NMS Plan has not been updated to reflect subsequent amendments to the CAT NMS Plan.

its SCI systems have levels of security adequate to maintain operational capabilities and promote the maintenance of fair and orderly markets). In some cases, non-member invitees of the Security Working Group may be given access to otherwise confidential information, but the Commission believes that the CISO and the Operating Committee should consider requiring any non-member invitees sign a non-disclosure agreement or adhere to some other protocol designed to prevent the release of confidential information regarding the security of the CAT System. Members of the Security Working Group (and their designees) would be subject to the confidentiality obligations set forth in Section 9.6 of the CAT NMS Plan.

[595] *See* 17 CFR 242.17a–1.

[596] *See* 17 CFR 242.613.

[597] 15 U.S.C. 78c(f).

[598] 15 U.S.C. 78w(a)(2).

A. Analysis of Baseline, Costs and Benefits

The Commission preliminarily believes the proposed amendments would improve the security of CAT Data through a number of mechanisms. The amendments are likely to reduce the attack surface of CAT by further limiting the extraction of CAT Data beyond the security perimeter of the CAT System. In addition, the proposed amendments may increase the uniformity of security monitoring across environments from which CAT Data is accessed and analyzed by facilitating centralized monitoring by the Plan Processor. In addition, the Commission preliminarily believes that provisions allowing for exceptions to the SAW usage requirement may allow Participants to achieve or maintain the security standards required by the CAT NMS Plan more efficiently. Additional effects upon efficiency and competition are discussed in Part IV.B.

The Commission preliminarily believes that provisions of the proposed amendments outside of the SAW use requirement will result in one-time costs of approximately $2.0MM.[599] In addition, these provisions of the proposed amendments would result in ongoing annual costs of approximately $5.9MM.[600] The Commission also preliminarily estimates that depending on the number of Participants that choose to work within SAWs, the SAW or exception requirement will entail $4.9MM to $61.6MM in initial costs and $4.7MM to $32.8MM in ongoing annual costs. These costs are summarized in Table 1 and Table 2 [601] below, and discussed further in the sections that follow.

TABLE 1—SUMMARY OF COSTS OTHER THAN SAW COSTS ($)

Activity	Participants		Plan Processor	
	Labor	External	Labor	External
Initial				
OTQT logging			88,000	
CAIS programmatic access			620,200	
Policies and procedures	1,155,900	50,000	10,900	
Regulator and Plan Processor access			10,300	
Secure connectivity			33,100	
Breach management policies and procedures	9,500		49,800	
Total One-Time Costs	1,165,400		812,300	
Annual				
CISP	106,400	9,000	129,900	
Security Working Group	2,056,600		310,000	
OTQT logging	970,200		5,100	
Customer Identifying Systems Workflow			373,500	
Policies and procedures	480,600	1,442,500	5,400	
Secure connectivity			3,100	
Breach management policies and procedures			42,200	
Total ongoing annual costs	3,613,800	1,451,500	869,200	

1. CISP

In Section 6.12, the Plan requires the Plan Processor to develop and maintain an information security program for the Central Repository. Section 4 of Appendix D sets out information security requirements that cover ''all components of the CAT System'' and is not limited to the Central Repository.[602]

To more explicitly define the scope of the information security program referenced in Section 6.12, the proposed amendments would define the term ''Comprehensive Information Security Program'' [603] (CISP) to encompass the Plan Processor and the CAT System, including any systems provided or managed by external contractors, organizations or other sources. Additionally, the scope of the CISP would include the SAWs.[604]

The Commission preliminarily believes that the benefit of this provision of the proposed amendments is a potential improvement to the efficiency of CAT implementation by specifically defining the scope of the information security program required by the CAT NMS Plan to the extent that the Participants did not understand that these requirements applied to the Plan Processor, the entire CAT System, and external parties. Section 6.12 of the CAT NMS Plan requires the Plan Processor to develop and maintain an information security program for the Central Repository that, at a minimum, meets the security requirements set forth in Section 4 of Appendix D to the CAT NMS Plan.[605] If Participants do not apply the Plan Processor's information security program to the Plan Processor and the entire CAT System, including any components of the CAT System managed by external providers, the proposed amendments may increase the efficiency by which the CAT is implemented by preventing Participants from investing in initial implementations that do not meet CAT NMS Plan requirements.

The proposed amendments would newly require the CCO to evaluate elements of the CISP that relate to SAWs as part of the regular written assessment and, in collaboration with the CISO, to include a review of the quantity and type of CAT Data extracted from the CAT System to assess the security risk

[599] ($1,165,400 + $812,300) = $1,977,700.

[600] ($3,613,800 + $1,451,500 + $869,200) = $5,934,500.

[601] *See infra* Part IV.A.3.

[602] *See supra* Part II.A.

[603] ''Comprehensive Information Security Program'' includes the organization-wide and system-specific controls and related policies and procedures required by NIST SP 800–53 that address information security for the information and information systems that support the operations of the Plan Processor and the CAT System, including those provided or managed by an external organization, contractor, or source, inclusive of Secure Analytical Workspaces. *See supra* Part II.A.

[604] *Id.*

[605] *See supra* Part II.A.

of permitting such CAT Data to be extracted.[606] The Commission preliminarily believes that the Plan Processor[607] will incur expenses of $129,900[608] annually to execute this requirement.

The Plan provides for the Participants to review and comment on the regular written assessment provided by the Plan Processor.[609] The proposed amendments newly require the CCO to evaluate the CISP, which includes SAWs, as part of the regular written assessment which the Participants must review each year.[610] The Commission preliminarily believes that Participants that are part of a larger exchange group will perform this task at the group (''Participant Group'') level of organization because doing so will reduce duplication of effort.[611] The Commission preliminarily believes that Participants would spend $106,400[612] in labor costs to perform this review, as well as incurring $9,000 in external legal costs in performing this review and providing comments upon it.

2. Security Working Group

Although the Plan does not require formation of a Security Working Group, the Operating Committee has established such a group, which currently includes the CISO, and chief information security officers and/or other security experts from each Participant.[613] The extant Security Working Group makes recommendations to the Operating Committee regarding technical issues related to the security of the CAT, but has no formal charter or mandate outlining its responsibilities or ensuring its continued existence.

To provide support and additional resources to the CISO, the proposed amendments would require the Operating Committee to establish and maintain a security working group composed of the CISO and the chief information security officer or deputy chief information security officer of each Participant.[614] Currently, the Plan does not include a requirement for the Security Working Group. The Plan also does not require that the membership of this group will have a sufficient level of security expertise. Further, without language in the Plan describing the group's role, there is no requirement that the group will participate in decisions that will affect CAT Data security, such as in evaluating exception requests. Consequently, the Commission preliminarily believes that the degree to which this group will improve decisions affecting CAT Data at present and in the future is uncertain. The Commission preliminarily believes that the provisions of the proposed amendments that codify the existence of the Security Working Group and describe its role will improve the security of CAT Data in several ways.

First, although a security working group has been established by the Participants already, its existence is not codified in the Plan. Including these provisions in the Plan will assure the group's continued activity.

Second, the Commission preliminarily believes that these proposed amendments may improve CAT Data security because they provide the Security Working Group with a broad mandate to advise the CISO and the Operating Committee on critical security-related issues. Further, defining the membership of the Security Working Group may improve the quality of recommendations emanating from the Security Working Group, as the group already established by the Operating Committee does not currently require the participation of the chief information security officer or deputy chief information security officer of each Participant. The proposed amendments also permit the CISO to invite non-Security Working Group members to attend. Including subject matter experts outside of the Participants and Plan Processor that are knowledgeable about security may broaden or deepen the level of expertise brought to bear.

Because the Security Working Group is not required by the Plan, the Plan has no defined role as it would under the proposed amendments. For example, the proposed amendments require that the Security Working Group advise the CISO and the Operating Committee with information technology matters that pertain to the development of the CAT System. Such issues are likely to be complex and technical. To the extent that the proposed amendments result in the involvement of a range of individuals with expertise in assessing organizational-level security issues for complex information systems, the proposed amendments may result in additional security issues being considered and considered more thoroughly by the CISO and Operating Committee.

The Commission preliminarily believes however, that there are potential conflicts of interest in involving the Security Working Group in the review of certain issues. For example, the proposed amendments call for the members of the Security Working Group (and their designees) to receive application materials for exceptions to the requirement that Participants use Plan Processor provided SAWs to access and analyze CAT Data using the user defined direct query tool and bulk extract tools. To the extent that the Participant members of the Security Working Group (and their designees) also plan to obtain or maintain exceptions to the SAW requirement, they may be less critical of other Participants' application materials. Alternatively, to the extent that Participant members of the Security Working Group (and their designees) plan to use the Plan Processor's SAWs, they may be more critical of other Participants' exception application materials. Competitive relationships between Participants may also affect how Security Working Group members (and their designees) evaluate such applications. The Commission preliminarily believes that this concern is largely mitigated by its preliminary belief that Participants will adopt a variety of approaches to complying with the SAW usage requirement,[615] so reviews of these application materials are likely to reflect a variety of viewpoints. To the extent that Participants' decisions do not reflect a variety of approaches, the Commission recognizes that the potential conflicts of interest may be more pronounced. Furthermore, the exception application procedure does not require a vote of the Security Working Group, so the

[606] *See supra* Part III.D.1.

[607] Costs attributed to the Plan Processor will be passed on to Participants and Industry Members according to a fee schedule that has not yet been approved by the Commission. *See* CAT NMS Plan, *supra* note 3, at Section 11.3.

[608] *See supra* note 489.

[609] *Id.*

[610] *See supra* Part II.A.

[611] *See infra* Part IV.B.1 for a discussion of organization of exchanges into groups. There are nine Participant Groups. Four of these groups operate a single exchange while four control multiple exchanges. FINRA, the sole national securities association, comprises the final Participant Group.

[612] Throughout this Economic Analysis, the Commission derives estimated costs associated with staff time based on per hour figures from SIFMA's Management & Professional Earnings in the Securities Industry 2013, modified by Commission staff to account for an 1800-hour work-year, and multiplied by 5.35 to account for bonuses, firm size, employee benefits and overhead, and adjusted for inflation based on Bureau of Labor Statistics data on CPI–U between January 2013 and January 2020 (a factor of 1.12). Labor costs include 15 hours of attorney labor and 10 hours of chief compliance officer labor per Participant Group. (15 hours × $426/hour + 10 hours × $543/hour) = $11,820. ($11,820 per group × 9 groups) = $106,380. ($1,000 per group × 9 groups) = $9,000.

[613] *See https://www.catnmsplan.com/sites/default/files/2020-01/FINRA-CAT-Security-Approach-Overview_20190828.pdf.*

[614] *See supra* Part II.B.

[615] *See infra* Part IV.A.3.a.

Commission preliminarily believes that in the Security Working Group's advisory role to the CISO and Operating Committee, a conflict of interest in providing feedback on a competitor's SAW exception application is less likely to be a significant factor in a Participant's ability to secure an exception. Finally, the Commission believes that the Participants are incentivized to avoid security problems in all environments from which CAT Data is accessed and analyzed. Consequently, the Commission preliminarily believes that even if exceptions are widely sought by Participants, their Security Working Group members are likely to bring forward any problems they identify in their review of exception application materials because a data breach concerning CAT Data irrespective of its source is likely to be costly to all Participants both in remediation costs and reputation.

The Commission preliminarily estimates Participants will incur costs of approximately $2,056,600 [616] annually to comply with provisions of the proposed amendments related to participation in the Security Working Group. In addition, requiring the Plan Processor CISO to keep the Security Working Group apprised of relevant developments, to provide it with all information and materials necessary to fulfill its purpose, and to prepare for and attend meetings of the Security Working Group will cause the Plan Processor to incur approximately $310,000 [617] per year in labor costs.

3. Secure Analytical Workspaces

The Commission understands that the Participants have recently authorized the Plan Processor to build analytic environments for the Participants.[618] Use of such environments is currently optional; the Participants are not required to use the analytic environments built by the Plan Processor when accessing and analyzing Customer and Account Attributes and, without the proposed amendments, could continue to access large amounts of CAT Data outside of these controlled environments.[619] The Commission also understands that the security controls for these analytic environments would not be implemented by one centralized party. Rather, each Participant would be responsible for the selection and implementation of security controls for its own analytic environment(s).[620]

The central repository is hosted in an Amazon Web Services (''AWS'') cloud environment.[621] The Commission is aware of two Participant Groups that have presences in this environment.[622]

The CAT NMS Plan requires that the Plan Processor CISO ''review the information security policies and procedures of the Participants that are related to the CAT to ensure that such policies and procedures are comparable to the information security policies and procedures applicable to the Central Repository.'' [623] If the CISO finds that a Participant is not meeting this standard and if the deficiency is not promptly addressed, the CISO, in consultation with the CCO, is required by the CAT NMS Plan to notify the Operating Committee. Consequently, security within the Participants' analytic environments that access CAT Data is expected to be comparable to that of the Central Repository.

The Commission preliminarily believes that provisions of the proposed amendments that require Participants to work within SAW or non-SAW environments that have been granted an exception for the proposed SAW usage requirements set forth in proposed Section 6.13(a)(i)(B) (''Excepted Environments'') would provide a number of benefits. First, to the extent that the Plan Processor implements common security controls for SAWs more uniformly than they would be under the current approach, wherein each Participant would be allowed to implement selected security controls for its own analytic environment(s), security may improve by reducing variability in security control implementation, potentially preventing relatively weaker implementations. Second, because implementation of common security controls will be uniform, the proposed amendments may increase the ability of the Plan Processor to conduct centralized and uniform monitoring across all environments from which CAT Data is accessed and analyzed. Third, the Commission preliminarily believes that exceptions to the proposed SAW usage requirements may allow Participants to achieve or maintain the security standards required by the Plan more efficiently. Fourth, the Commission preliminarily believes that provisions in the proposed amendments that provide for a third-party annual review process for the continuance of any exceptions that are granted would provide a procedure and timeline for remedying security deficiencies in Excepted Environments.

Finally, to the extent that policies and procedures governing data security [624] are less rigorous in application than the security provisions for SAWs in the proposed amendments, data downloaded to SAWs would be more secure than it might be in other analytic environments permitted under the CAT NMS Plan.

As discussed below, each Participant will choose whether to access CAT Data from the Plan Processor provided SAW accounts or to obtain an exception from the SAW usage requirement.[625] The Commission cannot predict how each Participant will approach this decision, but it preliminarily believes approaches will vary across Participants due to differences in size, operations, use of RSAs and 17d–2 agreements to satisfy regulatory responsibilities, current AWS cloud presence, and membership in a Participant Group that controls multiple exchanges. Consequently, in its cost estimates the Commission includes the Plan Processor's costs of designing and implementing the SAWs, but estimates ongoing operational costs to the Participants as a range. At one end of the range, the Commission assumes that all Participants obtain exceptions to the SAW usage requirements. At the other end, the Commission assumes that all Participants work within the Plan Processor's SAWs.

The Commission recognizes that the costs the Participants incur due to the requirements of the proposed amendment is likely an overestimate

[616] The proposed amendments require the CISO to participate in the Security Working Group. Because the Participants have already formed a security working group that the Commission preliminarily believes meets weekly, some of the labor costs associated with this group are in the baseline. To estimate the costs attributable to the proposed amendments, the Commission assumes that on average the current security working groups' participants have hourly labor rates equivalent to a Compliance Manager ($317 per hour). To the extent that the current Security Working Group participants have hourly labor rates that are greater than this rate, the estimated additional costs of the amendments would be reduced. Consequently, the Commission preliminarily estimates that the incremental hourly labor cost of the proposed amendments would the difference between the estimated hourly rate of the CISO and a Compliance Manager ($543/hour − $317/hour) = $226 per hour. For the CISO hourly rate calculations, the Commission uses the hourly rate for Chief Compliance Officer. 7 hours per week × 52 weeks = 364 hours of CISO labor per Participant. (364 hours per Participant × 25 Participants × $226/hour) = $2,056,600.

[617] *See supra* note 495.

[618] *See* Simon Letter, *supra* note 52, at 4–5.

[619] *See id.*

[620] *See id.*

[621] *See https://aws.amazon.com/blogs/publicsector/finra-cat-selects-aws-for-consolidated-audit-trail/.*

[622] *See http://technology.finra.org/articles/video/trade-analytics-and-surveillance-on-aws.html* and *https://aws.amazon.com/solutions/case-studies/nasdaq-data-lake/.*

[623] *See* CAT NMS Plan, *supra* note 3 at Section 6.2(b)(vii).

[624] *See supra* text accompanying note 623.

[625] *See infra* Part IV.A.3.a.

because the Commission is unable to identify costs included in the analysis that would be incurred in the absence of the proposed amendments. For example, some Participants would likely work in the Plan Processor's planned analytic environments without the proposed amendments. For those Participants, some of the costs they incur to implement their operations within the SAWs under the proposed amendments would be incurred in the baseline case, as would at least some of their ongoing costs of using SAWs. Similarly, the Plan Processor's costs to implement SAWs under the proposed amendments may include costs that would have been incurred to implement similar analytic environments without the proposed amendments.

The Commission further believes that this range does not encompass the costs that Participants incur to perform their regulatory duties using CAT Data because Participants that seek exceptions will perform those duties in another manner, such as by working within their current analytic environments or through RSAs and 17d–2 agreements. Both of those approaches carry costs, but those costs are not consequences of the proposed amendments because the Participants currently perform their regulatory duties in a non-SAW environment. Consequently, those costs are part of the baseline.

Table 2 presents a summary of estimated costs for compliance with the proposed amendments' requirement that Participants work within a Plan Processor provided SAW or obtain an exception. The table summarizes $274,600 [626] in initial base costs and $860,200 in ongoing annual base costs that are required to develop and implement the SAWs; these costs must be incurred regardless of whether any Participants choose to work within SAWs. The table then presents marginal costs for all Participants working within SAWs versus all Participants working within Excepted Environments. The Commission preliminarily estimates a range of costs for the SAW or exception requirements.[627] All Participants working within a SAW would entail $61.6MM [628] in initial costs and $32.8MM [629] in ongoing annual costs including base costs. All Participants working in Excepted Environments would entail $4.9MM [630] in initial costs and $4.7MM [631] in ongoing annual costs. These costs are broken down and discussed further in the sections that follow.

TABLE 2—COSTS FOR SAW OR EXCEPTION REQUIREMENT ($)

Activity	Participants		Plan processor	
	Labor	External	Labor	External
Initial base costs				
Incorporate SAW requirements into CISP	.....	.....	89,000	27,000
Develop detailed design specifications for SAWs	.....	.....	56,200	47,000
Provide Participants with detailed design specifications	.....	.....	3,000	.....
Develop automated monitoring systems	.....	.....	52,400	.....
Total base initial costs	.....	.....	200,600	74,000
Annual Base Costs				
Maintain and monitor CISP SAW requirements	.....	.....	56,600	.....
Maintain detailed design specifications	.....	.....	48,300	.....
Additional costs for third party annual audit	.....	.....	150,000	.....
Maintain automated monitoring systems and monitor	.....	.....	605,300	.....
Total base annual costs	.....	.....	860,200	.....
Additional Costs for All Participants in SAWs				
Initial.				
Technical development costs	39,500,000	.....	.....	
Evaluate nine SAWs for compliance	.....	.....	167,000	.....
SAW operations implementation costs	21,700,000	.....	.....	.....
Total Additional Initial Costs	61,200,000	.....	167,000	.....
Annual.				
SAW usage costs	.....	12,900,000	.....	.....
Technical maintenance costs	19,000,000	.....	.....	.....
Total Annual Additional Costs	19,000,000	12,900,000	.....	.....
Additional Costs for All Participants Excepted				
Additional Initial Costs	1,289,600	2,250,000	1,048,800	.....
Additional Ongoing Costs	417,400	2,250,000	1,160,100	.....

[626] $200,600 + $74,000 = $274,600.

[627] It is possible that this range may overestimate the costs Participants incur if some Participants can comply with the proposed amendments at a lower cost by employing 17d–2 or RSAs to avoid obtaining an exception or contracting for a SAW.

[628] ($61,200,200 + $167,000 + $200,600 + $74,000) = $61,641,600.

[629] ($19,000,000 + $12,900,000 + $860,200) = $32,760,200.

[630] ($1,289,600 + $2,250,000 + $1,048,800 + $200,600 + $74,000) = $4,863,000.

[631] ($417,400 + $2,250,000 + $1,160,100 + $860,200) = $4,687,700.

a. SAW Versus Exception Decisions

Under the proposed amendments, each Participant will be required to limit some of its use of CAT Data to SAWs provided by the Plan Processor unless it obtains an exception to certain SAW usage requirements.[632] Consequently, each Participant will likely meet its regulatory obligations using one or more of three approaches. First, the Participant may decide to use the Plan Processor provided SAWs that would be established under the proposed amendments. Second, the Participant may decide to apply for an exception to allow it to use a different analytic environment to access and analyze CAT Data. Third, the Participant may decide to employ a 17d–2 or RSA to discharge its regulatory responsibilities. Each of these potential approaches has direct and indirect costs to the Participant that are discussed below.

In the first approach, a Participant may elect to use a SAW provided by the Plan Processor. The costs of operating and maintaining this SAW would be paid by the Participant, and the magnitude of these costs would be dependent on the resources used by the Participant within the SAW.[633] If a Participant adopts this approach, it may have lower expenses associated with maintaining its private analytic environment. However, to the degree that the Participant currently uses IT resources that it also uses for operational activities to perform its regulatory activities, this may create inefficiencies because those resources may be less utilized during hours when operational demands are lower, such as when exchanges are not operating, if it performs regulatory activities in the SAW. Under this approach, to the degree that the lack of excess operational resources limit the Participant's ability to perform its regulatory activities in-house, the Participant may be able to insource more of its regulatory activities when working in the SAW, reducing its dependence on and costs associated with 17d–2s and RSAs.[634] Utilizing a SAW may also open competitive opportunities to the Participant to perform regulatory services for other Participants within its SAW.[635] Moving regulatory activities to the SAW is likely to entail significant implementation costs: the Participant would need to develop or license analytic tools for that environment or adapt its current analytical tools to that environment, and train its regulatory staff in using the SAW environment. The Commission preliminarily believes this approach is more likely to be adopted by Participants in Participant Groups that operate multiple exchanges because these costs might be spread over more exchanges,[636] and by Participants that already have a significant cloud presence because their implementation costs would likely be lower than those for a Participant that did not have a cloud presence.

In the second approach, a Participant may apply to use a private analytical environment through the exception procedure. In this approach, the Participant would incur costs to document that its private analytic environment meets the security requirements of the proposed amendments, and to adapt its analytic tools to those requirements. Further, the Participant would incur costs associated with applying for and obtaining the exception, and complying with annual renewal requirements. The Participant may also encounter certain inefficiencies in accessing CAT Data to the extent that download speeds between the Central Repository and the private analytic environment are inferior to those within the SAW.[637] A Participant that adopts this approach may also choose to change the scope of its use of 17d–2s and RSAs as a provider or user of regulatory services through such agreements. For example, a Participant may choose to pursue an exception to the SAW use requirement and add additional 17d–2 and RSA coverage for functions that are more difficult to perform within its private analytic environment. Alternatively, there may be analytic tools that are more efficient to use outside of SAWs, allowing a Participant to provide regulatory services to other Participants that would be less efficient to provide in the SAWs. The Commission preliminarily believes this approach is more likely to be adopted by Participants that have a significant investment in private analytic workspaces, and proprietary tools for regulatory activities that are optimized for those workspaces.

In the third approach, a Participant would change its use of RSAs and 17d–2 agreements to avoid using a SAW or obtaining an exception to the SAW use requirement. This approach is likely to increase a Participant's expenses associated with RSAs and 17d–2 agreements, but may allow a Participant to avoid SAW expenses entirely. It is possible that even with maximal use of RSAs and 17d–2 agreements, a Participant may want to perform some regulatory functions that would not be possible with only use of the online targeted query tool. In this case, a minimal SAW would also have to be supported if the Participant did not wish to seek an exception to the SAW use requirement. The Commission preliminarily believes that this approach is most likely to be adopted by Participants that operate a single venue, and Participants that currently outsource much of their regulatory activities to other Participants. The Commission recognizes it is possible that many Participants will take this approach considering that many Participants make broad use of RSAs and 17d–2 agreements to discharge their regulatory responsibilities.

Finally, the Commission recognizes that a Participant may take a mixed approach to this decision. A Participant may elect to use the SAW for some regulatory activities, and outsource other activities that would significantly increase its use of resources in the SAW, and thus its costs of using the SAW. It is also possible that a Participant may choose to invest heavily in the SAW to compete in the market for regulatory services as an RSA provider, while also obtaining an exception to the SAW use requirement to allow it to capitalize on its current infrastructure.

b. Amendments for SAWs

The Commission is proposing amendments to the CAT NMS Plan that will require (1) the provision of SAW accounts; (2) data access and extraction policies and procedures, including SAW usage requirements; (3) security controls, policies, and procedures for SAWs; (4) implementation and operational requirements for SAWs.[638] The Commission preliminarily believes that the proposed amendments may improve the security of CAT Data in two ways.

First, to the extent that CISP security controls are implemented more uniformly than they would be under the CAT NMS Plan, security may improve

[632] Participants will be able to use the online direct query tool from their own analytic environments under certain restrictions, but the number of records of CAT Data they extract, and their access to Customer Information, would be limited for this manner of access. *See supra* Part II.C and Part II.D.

[633] The estimated costs of SAWs are discussed further below.

[634] RSAs are discussed further below.

[635] *See infra* Part IV.B.1.

[636] Participants that operate multiple exchanges often have commonalities in data structures and rules across their exchanges that allow economies of scale in performing regulatory activities.

[637] *See infra* Part IV.B.2.

[638] *See supra* Part II.C.

by reducing variability in security control implementation.[639] Currently, each Participant would be responsible for implementing security controls in their analytic environments and their approaches are likely to vary if each Participant designs those implementations to accommodate their current operations and analytic environments. This variability might result in some environments being more secure than others.[640] To the extent that having the Plan Processor provide SAWs that implement common security controls reduces this variability,[641] these provisions may increase CAT Data security by preventing relatively weaker implementations. The Commission recognizes it is also possible that the Plan Processor's implementation might be relatively less secure than an implementation designed by an individual Participant under the current CAT NMS Plan. The Commission preliminarily believes these provisions should improve security by reducing the variability of implementations as long as the Plan Processor's implementation of common security controls is relatively secure compared to other possible approaches. Further, the Commission preliminarily believes that the requirement that the Plan Processor must evaluate and notify the Operating Committee that each Participant's SAW has achieved compliance with the detailed design specifications before that SAW may connect to the Central Repository will further increase uniformity of security control implementations.[642]

Second, the proposed amendments may increase the uniformity of security monitoring across all environments from which CAT Data is accessed and analyzed.[643] By assigning this duty to a single entity, the Plan Processor, and making provisions for the uniformity of this monitoring through detailed design specifications, the proposed amendments may enhance the security of CAT Data by ensuring that security monitoring is uniform. Currently under the CAT NMS Plan, most security monitoring of environments other than the Central Repository would fall to the Participants that controlled those environments.[644] To the extent that the rigor of this monitoring and the manner in which requirements were implemented varied across Participants and the Plan Processor, some environments might be more robustly monitored than others, potentially delaying the identification of security issues within less robustly monitored environments. In addition, having a single entity perform this security monitoring may improve its quality by facilitating development of expertise of the single entity performing the monitoring. To the extent that the Security Working Group participates in the development of this monitoring, expertise from the wider group of Participants might also improve the quality of monitoring. Further, the Commission preliminarily believes that standardizing implementation of security protocols through the common detailed design specifications may be more efficient than having each Participant that implements a SAW or private environment for CAT Data do so independently because it avoids duplication of effort. This may also improve efficiency by reducing the complexity of security monitoring of environments from which CAT Data is accessed and analyzed because the detailed design specifications will include provisions that facilitate this central monitoring.

Finally, the Commission preliminarily believes that provisions of the proposed amendments that establish security controls, policies, and procedures for SAWs may improve CAT Data security. Currently, under the CAT NMS Plan, Participants must establish security protocols comparable to those required for the central repository for all environments from which Participants access CAT Data.[645] The proposed amendments require that SAWs comply with the same security standards as the Central Repository, including compliance with and common implementation of certain NIST SP 800–53 security controls, policies, and procedures. To the extent that the security controls, policies and procedures required for SAWs in the proposed amendments are more rigorous than what the Participants would implement under the current CAT NMS Plan, the security of CAT Data may be improved.

Table 3 summarizes the Commission's preliminarily cost estimates if all Participants were to work within SAWs. The Commission estimates that Participants would collectively incur $61.2MM in initial costs and $31.9MM[646] in ongoing annual costs, while the Plan Processor would incur $441,600[647] in initial costs and $860,200 in ongoing annual costs. These costs are discussed further in the analysis that follows.

TABLE 3—COSTS FOR ALL PARTICIPANTS TO USE SAWS ($)

Activity	Participants		Plan processor	
	Labor	External	Labor	External
Initial				
Incorporate SAW requirements into CISP	.....	.....	89,000	27,000
Develop detailed design specifications for SAWs	.....	.....	56,200	47,000
Provide Participants with detailed design specifications	.....	.....	3,000	.....
Evaluate nine SAWs for compliance	.....	.....	167,000	.....
Technical development costs	39,500,000	.....	.....	.....
Develop automated monitoring system	.....	.....	52,400	.....
SAW operations implementation costs	21,700,000	.....	.....	.....
Total initial costs	61,200,000	.....	367,600	74,000
Annual				
Maintain and monitor CISP SAW requirements	.....	.....	56,600	.....

[639] *See supra* Part II.C.3.

[640] The Commission preliminarily believes that different environments that satisfy the CISP might vary in their overall level of security due to differences in implementation, third-party software and policies and procedures for monitoring the security of the environments. To the extent that a bad actor would focus an incursion attempt upon the least secure environment, reducing variability between environments may improve CAT Data security by reducing vulnerabilities within environments from where CAT Data is accessed and analyzed.

[641] *See supra* Part II.C.1.

[642] *See supra* Part II.C.4

[643] *See supra* Part II.C.4.

[644] *See supra* Part IV.A.3.a.

[645] *See supra* text accompanying note 623.

[646] ($19,000,000 + $12,900,000) = $31,900,000.

[647] ($367,600 + $74,000) = $441,600.

TABLE 3—COSTS FOR ALL PARTICIPANTS TO USE SAWS ($)—Continued

Activity	Participants		Plan processor	
	Labor	External	Labor	External
Maintain detailed design specifications			48,300	
Maintain automated monitoring system and monitor			605,300	
Additional costs for third party annual audit			150,000	
Technical maintenance of SAWs	19,000,000			
SAW usage costs		12,900,000		
Total ongoing costs	19,000,000	12,900,000	860,200	

Under the proposed amendments, the Plan Processor would be required to incorporate SAW-specific additions into the CISP.[648] The Commission preliminarily estimates the Plan Processor will incur approximately $89,000[649] in initial labor and $27,000[650] in external consulting costs to fulfill this requirement. The Commission preliminarily estimates the Plan Processor will also incur $56,600[651] in recurring annual costs to meet those provisions.

The Commission preliminarily estimates that the Plan Processor will incur initial, one-time costs of approximately $56,200[652] in labor costs and $47,000[653] in external legal and consulting costs to develop detailed design specifications for the technical implementation of the access, monitoring and other controls required for SAWs.[654] The Commission preliminarily believes the Plan Processor will incur $3,000[655] in labor costs to make the required detailed design specifications available to the Participants, and will incur an additional $48,300[656] per year to maintain those detailed design specifications.

For the Plan Processor to evaluate each Participant Group's[657] SAW to confirm that the SAW has achieved compliance with the detailed design specifications and to notify the Operating Committee, the Commission preliminarily estimates that the Plan Processor would incur an initial, one-time expense of approximately $167,000.[658]

For the Plan Processor to build automated systems that will enable monitoring of the SAWs and Excepted Environments, the Commission preliminarily estimates that the Plan Processor would incur an initial, one-time expense of $52,400.[659] For the Plan Processor to maintain such systems and to monitor each Participant's SAW in accordance with the detailed design specifications, the Commission preliminarily estimates the Plan Processor would incur annual recurring costs of $605,300.[660] For each instance of non-compliance with the CISP or detailed design specifications, the Plan Processor would incur costs of $500 to notify the non-compliant Participant.[661]

The Plan currently requires that the Plan Processor conduct a third-party annual security audit.[662] The Commission preliminarily estimates the proposed amendments would increase the cost of that security assessment by $150,000 per year because of its increased scope and complexity due to the addition of the SAWs.

The Participants would incur additional technical implementation costs to set-up and configure their SAWs, develop tools for interacting with CAT Data, develop and implement cluster computing capabilities if applicable,[663] and implement technical monitoring. The Commission estimates the Participants will incur labor costs of $39.5MM[664] for these one-time development costs. These activities will also entail ongoing labor costs to the Participants that the Commission preliminarily estimates at $19.0MM[665] annually.

[648] *See supra* Part III.D.3.a.

[649] *See supra* note 498.

[650] *See supra* Part III.D.3.a.

[651] *See supra* note 501.

[652] *See supra* note 503.

[653] *See supra* Part III.D.3.a.

[654] *Id.*

[655] *See supra* note 506.

[656] *See supra* note 508.

[657] The Commission preliminarily believes that each Participant Group will contract for a single SAW because it preliminarily believes that each Participant Group largely centralizes its regulatory functions that would require CAT Data.

[658] *See supra* note 509. $18,550 per group × 9 groups = $166,950.

[659] *See supra* note 510.

[660] *See supra* note 511.

[661] *See supra* note 512.

[662] *See* CAT NMS Plan, *supra* note 3, at Section 6.2(a).

[663] The Commission preliminarily believes Participant Groups that operate a single exchange are unlikely to use cluster computing capabilities because these Participants tend to use RSA and 17d–2 agreements to satisfy their regulatory responsibilities that would require CAT Data.

[664] Setting up and configuring SAWs includes license procurement, development of the SAW environment, development of cluster computing capabilities if applicable, development of tools to interact with CAT Data, and implementation of technical monitoring. Costs for transitioning from a private analytic environment to the SAW are accounted for separately below. *See infra* note 674. Labor estimates include 900 hours from operations specialists and 900 hours from systems analysts. Labor estimates to develop tools include 2,700 hours from senior programmers and 2,700 hours from senior systems analysts. Labor costs to implement cluster computing capabilities include 7,200 hours from senior programmers and 7,200 hours from senior systems analysts. Labor estimates to implement technical monitoring include 2,700 hours from operations specialists. ((900 + 2,700) hours × $140/hour + (900 × $269/hour) + (2,700 + 7,200) hours × $339/hour + (2,700 + 7,200) × $291/hour = $6,983,100. The Commission preliminarily believes that Participant Groups that operate a single exchange are unlikely to implement cluster computing capabilities. Consequently, the Commission preliminarily estimates these single exchange Participant Groups will have technical development costs of ($6,983,100—(7,200 hours × $339/hour + 7,200 hours × $291/hour)) = $2,447,100. The Commission preliminarily believes that FINRA has already completed most of this technical development work because FINRA is already working within an AWS analytic cloud. Thus, the Commission preliminarily believes that FINRA's technical development costs will be approximate 25% of those of a Participant Group that operates multiple exchanges. Consequently, the Commission's estimate of total technical development costs for the nine Participant Groups is ((4 single exchange groups × $2,447,100/group) + (4 multiple exchange groups × $6,983,100/group) + ($6,983,100 × 25%)) = $39,466,575.

[665] Ongoing labor estimates to maintain the SAW's technical environment include 1 senior programmer and 1 senior systems analyst. Ongoing labor costs to maintain cluster computing capabilities include 1 senior programmer and 2 senior systems analysts. Labor estimates to maintain technical monitoring include 1.25 operations specialists. Assuming an 1,800 hour work year, for a Participant Group with multiple exchanges, these costs would total (1.25 × 1,800 hours × $140/hour + 2 × 1,800 hours × $339/hour + 3 × 1,800 hours × $291) = $3,106,800 annually. For a Participant Group with a single exchange that does not implement cluster computer capabilities, these costs would total (1.25 × 1,800 hours × $140/hour + 1 × 1,800 hours × $339/hour + 1 × 1,800 hours × $291) = $1,449,000 annually. The Commission preliminarily believes that FINRA is already maintaining most of this functionality in its current AWS environment, and thus believes its additional annual costs associated with maintaining its SAW technical environment would be approximate 25% of those incurred by a Participant Group that

Continued

The Participants would incur additional costs from their usage of the SAWs.[666] The Commission preliminarily believes these estimates may overestimate actual costs the Participants might incur in moving their operations to SAWs because it does not recognize cost savings that might be obtained by retiring redundant resources that they would no longer require for operations being conducted in SAWs.[667] The Commission preliminarily believes that the Plan Processor would be billed for SAW usage and would pass those costs on to Participants directly such that each Participant Group's SAW costs would reflect its own usage of SAW resources. To the extent that the Plan Processor marks up those costs before passing them on to Participant Groups, actual costs would exceed what the Commission estimates. To estimate the magnitude of these costs, the Commission assumes three scenarios of SAW use that vary in the types of instances employed within the SAW.[668] These estimates assume that supporting more advanced instances increases costs due to greater demands on computing resources. Certain general [669] and technical [670] assumptions are common across all SAW usage cost estimates.

The Commission assumes three levels of usage for its estimates. Participant Groups can be classified in their SAW usage as single-exchange, exchange group or association.[671] Table 4 presents preliminarily estimated Participant Group SAW use costs.[672] Consequently, the Commission preliminarily estimates that Participants will incur $12.9MM [673] annually in SAW use costs. The Commission further estimates that Participants will incur one-time costs of $21.7MM [674] to adapt current systems and train personnel to perform regulatory duties in the SAWs.

TABLE 4—ESTIMATED PARTICIPANT GROUP INCREMENTAL SAW USE COSTS ($)

	Single exchange		Exchange group		Association	
	Instances	Cost	Instances	Cost	Instances	Cost
Basic instance	5	6,000	25	26,000	150	154,000
Cluster compute instance	0	0	30	1,169,000	120	4,676,000
Advanced instance	0	0	15	942,000	30	1,912,000
Shared services & common charge	5	30,000	70	420,000	300	1,800,000
SAW storage	100 TB	31,000	2 PB	589,000	5 PB	1,463,000
Total		67,000		3,146,000		10,005,000

The Commission preliminarily believes that some provisions of the proposed amendments will entail indirect costs that regulators will incur to access and use CAT Data. The requirements that Participants work within SAWs and only access Customer and Account Attributes data through SAWs may raise the costs of regulatory access to CAT Data, or cause Participants to make operational changes to how they perform their regulatory duties in response to the decreased flexibility of the Plan under the proposed amendments. By

operates multiple exchanges. Consequently, to maintain their SAW's technical environment, the Commission preliminarily estimates that the nine Participant Groups would incur annual ongoing costs of ((4 single exchange groups × $1,449,000/group) + (4 multiple exchange groups×$3,106,800/group) + ($3,106,800 × 25%)) = $18,999,900.

666 The Commission estimated SAW usage costs through the AWS Simple Monthly Cost estimator at *https://calculator.s3.amazonaws.com/index.html.*

667 For example, Participants may maintain servers, cloud environments, and IT personnel that support operations such as surveillance and investigations. If these functions are performed within a SAW, such IT resources may be retired and personnel may be reassigned to support SAW technical operations. If Participants perform these functions using resources that cannot be retired, such as the servers they use to operate exchanges, such savings may be limited. The Commission notes that such savings would not apply to FINRA because its ongoing SAW costs are considered to be baseline costs.

668 For its cost estimates, the Commission assumes different virtual computers: a basic instance involves a single node on a AWS EC2-t2.2xlarge virtual computer; a cluster computing instance involves a group of AWS EC2—p2.16xlarge virtual computers; an advanced instance involves a AWS EC2- x1e.32xlarge virtual computer; and each instance is associated with a shared services and common charge of $6,000 per year.

669 Data transfers cost eliminated by hosting the SAWs in the same region as the Central Repository. AWS usage based on minimum and peak instance with daily spike traffic for 8.5 hours Monday through Friday using Compute Savings Plan. One AWS instance can support more than one user depending on the complexity of work when leveraging cluster computing.

670 The following technical options were used in all scenario estimates: Operating system (Linux), Storage for each EC2 instance (General Purpose SSD (gp2)), Snapshot Frequency (2x Daily), Data transfer cost (0), Pricing strategy (Compute Savings Plans 3 Year None upfront).

671 Single exchange usage assumes 5 basic instances and 100 terabytes of SAW storage. Exchange group assumes 25 basic instances, 30 cluster computing instances, and 15 advanced instances as well as 2 petabytes of SAW storage; 10 of these cluster instances and 10 of these advanced instances proxy for exchange groups' expected higher use of computing resources to conduct surveillance activities. Association assumes 150 basic instances, 120 cluster computing instances and 30 advanced instances as well as 5 petabytes of SAW storage. The Commission preliminarily believes FINRA, the sole national securities association, will have significantly higher CAT usage than exchange groups because the CAT NMS Plan anticipates the retirement of OATS, which is the data source FINRA currently uses to perform many of its regulatory activities, and many of those regulatory activities involve cross market data. With the retirement of OATS, FINRA will be unable to perform these activities without CAT Data.

672 The Commission preliminarily believes that the four Participant Groups that operate single exchanges are likely to outsource regulatory duties that would regularly require external data and thus use RSAs to fulfill those requirements. Consequently, their use of the SAW would be situational. The Commission preliminarily believes its cost estimate for FINRA is a significant overestimate because FINRA already has established and is working in an AWS environment. Consequently, the Commission preliminarily believes that FINRA's SAW usage costs would be in the baseline because FINRA is already performing its regulatory duties in an AWS workspace. Although FINRA's use might increase with the retirement of OATS, the Commission preliminarily believes this would be a consequence of the CAT NMS Plan rather than the proposed amendments.

673 (4 × $67,000 + 4 × $3,146,000) = $12,852,000.

674 In its economic analysis of the Plan, the Commission estimated the cost of the Plan as approximately $2.4 billion in initial aggregate implementation costs and recurring annual costs of $1.7 billion. *See* CAT NMS Plan Approval Order, *supra* note 3, at Part V.B. The Commission preliminarily estimates SAW implementation costs for all Participant Groups other than FINRA by using the same ratio of implementation to ongoing costs as estimated for the Plan. (2.4/1.7 × $12,852,000) = $18,144,000. The Commission preliminarily believes this approach is likely to significantly overestimate FINRA's implementation costs because FINRA is already working in an AWS environment and is thus unlikely to face many of the implementation costs that other Participants will face in implementing SAWs. Consequently, the Commission is reducing its estimate of FINRA's implementation costs by 75%. FINRA's share of implementation costs is (2.4/1.7 × $10,005,000 × 25%) = $3,531,176. Thus the Commission preliminary estimate of implementation costs would be $18,144,000 + $3,531,176 = $21,675,176.

restricting the use of most data access methods to SAWs or Excepted Environments, the CAT NMS Plan may make it more difficult or impossible for Participants to perform certain functions in the manner they currently do, for example by limiting the set of regulatory tools that are available to perform surveillance or enforcement investigations. This may result in some Participants developing new tools to perform these functions, or entering into RSAs and 17d–2 agreements with another regulator to avoid incurring such costs.

c. Amendments for Excepted Environments

The proposed amendments add provisions to the CAT NMS Plan that set forth a process by which Participants may be granted an exception from the requirement that Participants use their respective SAWs to access CAT Data through the user-defined direct query and bulk extract tools.[675] The Commission also proposes to add provisions to the CAT NMS Plan that would set forth implementation and operational requirements for any Excepted Environments.

The Commission preliminarily believes that providing for exceptions for the SAW usage requirements offers three benefits. First, the Commission preliminarily believes that provisions allowing for exceptions to the SAW usage requirements may allow Participants to achieve or maintain the security standards required by the CAT NMS Plan[676] more efficiently. Some Participants may have significant investments in private analytic environments and regulatory tools that they currently use or are developing to conduct regulatory activities in their analytic environments. To the extent that it would be impossible, impractical, or inefficient to adapt these processes to the SAWs, a mechanism for an exception to this policy may allow Participants to achieve the security standards required by the CAT NMS Plan without bearing the expense of redeveloping or implementing these processes within the SAWs. Further, if a Participant is able to conduct these activities with IT resources that would otherwise be idle if the Participant moved its activities to the SAW, an exception process may prevent the inefficiency of underutilizing existing resources.

Second, the Commission preliminarily believes that provisions in the proposed amendments that provide for an annual review process for the continuance of any exceptions that are granted would provide a procedure and timeline for remedying security deficiencies in Excepted Environments.[677] Although the CAT NMS Plan currently requires the CISO to review information security policies and procedures of the Participants that are related to the CAT, under the proposed amendments, this review will include a third-party security assessment and documentation of detailed design specifications of the Participant's security implementation. The Commission preliminarily believes that this additional information is likely to improve the quality of the review of the Participant's data security because it extends beyond information in the Participant's policies and procedures related to CAT. This may allow identification and remediation of security deficiencies that might not have been identified under the CAT NMS Plan. To the extent that these provisions identify security deficiencies that would otherwise not be identified, or identifies these deficiencies more rapidly, they may improve the security of CAT Data because the CAT NMS Plan does not currently establish procedures for periodic third-party review of Participants' private analytic environments, nor does it provide timelines for addressing any security deficiencies identified within these environments.

Third, the Commission preliminarily believes that provisions in the proposed amendments that require the Plan Processor to monitor some elements of security within Excepted Environments may improve CAT Data security by providing additional monitoring in Excepted Environments. The proposed amendments require Participants operating Excepted Environments to facilitate security monitoring within those environments by the Plan Processor. To the extent that this provides additional monitoring in Excepted Environments rather than substituting for monitoring by Participants with Excepted Environments, security monitoring of those environment may increase in effectiveness under the proposed amendments.

Finally, the Commission preliminarily believes that provisions of the proposed amendments that establish third-party security audits for Exempted Environments may improve CAT Data security. Currently, under the CAT NMS Plan, Participants are expected to establish comparable security protocols to those required for the central repository for all environments from which Participants access CAT Data. While the CAT NMS Plan currently requires the Plan Processor CISO to review Participants' policies and procedures to verify they are comparable to those for the central repository, the proposed amendments require that Exempted Environments undergo third-party security audits when they are first approved, and annually thereafter. Because these audits have a broader scope than the policy and procedure review required by the CAT NMS Plan, the Commission preliminarily believes they may provide a more comprehensive review of Participant security. To the extent that these third-party audits identify potential security concerns that would otherwise persist, security of CAT Data may improve.

The Commission preliminarily believes that Participants will make the decision to seek exceptions or work within the SAW at the Participant Group level.[678] The Commission estimates that if all nine Participant Groups were to obtain exceptions to the SAW use requirements, the Participants would incur initial costs of $3.5MM[679] to apply for exceptions and the Plan Processor would incur initial costs of $1.0MM to evaluate those applications and validate Excepted Environments. The Commission further estimates Participants would incur $2.7MM[680] in annual ongoing costs to update exception applications and the Plan Processor would incur $1.2MM in annual ongoing costs to process those applications and monitor Excepted Environments. Cost estimates are presented in Table 5 and discussed below.

[675] *See supra* Part II.C.5.

[676] *See supra* text accompanying note 623.

[677] *See supra* Part II.C.5.

[678] The Commission preliminarily believes that Participant Groups that operate multiple exchanges perform most regulatory duties that would require CAT Data centrally. Consequently, the Commission expects that application costs for multiple exchange Participant Groups would not be substantially more complex than those for a Participant Group that does not operate multiple exchanges.

[679] ($1,289,600 + $2,250,000) = $3,539,600.

[680] ($417,400 + $2,250,000) = $2,667,400.

TABLE 5—COSTS FOR NINE PARTICIPANT GROUPS TO OBTAIN EXCEPTIONS ($)

Activity	Participants		Plan processor
	Labor	External	Labor
Initial			
Third party security assessment	.....	2,250,000	.....
Prepare detailed design specification	801,200	.....	
Submit materials to CCO, CISO, SWG	16,800	.....	.....
Develop policies and procedures to review applications	.....	.....	56,000
Plan Processor review of exception application	.....	.....	825,800
Plan Processor validation of Excepted Environment	.....	.....	167,000
Implement Participant systems to enable monitoring	471,600	.....	.....
Total initial costs for nine Participant Groups	1,289,600	2,250,000	1,048,800
Annual			
Third party security assessment	.....	2,250,000	.....
Update application materials	400,600	.....	.....
Submit materials to CCO, CISO, SWG	16,800	.....	.....
Maintain and update application review policies	.....	.....	31,700
Plan Processor review of application	.....	.....	825,800
Plan Processor monitoring of Excepted Environments	.....	.....	302,600
Total ongoing costs for nine Participant Groups	417,400	2,250,000	1,160,100

The Commission estimates that each Participant Group would incur an initial, one-time cost of approximately $250,000[681] in external consulting costs to obtain the required security assessment from a named and independent third party security assessor. Providing the required detailed design specifications would result in an additional $89,000[682] in labor costs. Submitting those materials to the CCO, CISO, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group would entail an additional $1,900[683] in labor costs. Participants would face additional costs to implement processes required by the detailed design specifications that facilitate the Plan Processor's monitoring of Excepted Environments. The Commission preliminarily estimates each Participant Group seeking an exception would incur labor costs of approximately $52,400[684] to implement those processes.

In order to maintain the SAW exception, the Commission preliminarily believes that each Participant Group would incur costs of $250,000[685] to obtain an updated security assessment. The Commission preliminarily estimates that the costs associated with updating application materials would be approximately $44,500,[686] which is half of the cost to initially prepare the materials to support the exception application.[687] The Commission further estimates that each Participant Group would spend $1,900[688] in labor costs submitting these materials to the CCO, the CISO, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group.

The Plan Processor would incur costs to develop policies and procedures governing the review of applications for exceptions to the SAW use requirement. The Commission preliminarily estimates that the Plan Processor will incur labor costs of $56,000[689] to develop these policies and procedures, and annual ongoing costs of $31,700[690] to maintain and update these policies and procedures.

The Plan Processor will incur costs to review exception applications.[691] Each initial exception application would cause the Plan Processor to incur one-time labor costs of approximately $91,760.[692] Review of materials for continuation of exceptions would cause the Plan Processor to incur the same review costs annually.

The Plan Processor will incur costs to notify the Operating Committee that each Excepted Environment is compliant with the detailed design specifications that Participants provide as part of their application materials for an exception.[693] The Commission preliminarily estimates that the Plan Processor will incur $18,550[694] in labor costs to evaluate each Excepted Environment and notify the Operating Committee. Should the Plan Processor need to notify a Participant Group of an identified non-compliance with the detailed design specifications, additional costs would be incurred.[695]

The Plan Processor will incur costs to monitor the Excepted Environments in accordance with the detailed design

[681] *See supra* Part II.D.3.d.i. ($250,000 per group × 9 groups) = $2,250,000.

[682] Labor costs include 200 hours by a senior systems analyst, 40 hours by a compliance attorney, 20 hours by the chief compliance officer, and 10 hours by a director of compliance. (200 hours × $291/hour + 40 hours × $374/hour + 20 hours × $543 + 10 hours × $500) = $89,020. ($89,020 per group × 9 groups) = $801,180.

[683] Labor costs include 5 hours by a compliance attorney. (5 hours × $374/hour) = $1,870. ($1,870 per group × 9 groups) = $16,830.

[684] The Commission preliminarily believes that development costs for the processes that produce log files that support Plan Processor monitoring would require similar development activities to developing the automated monitoring processes themselves. *See supra* note 510. ($52,400 per group × 9 groups) = $471,600.

[685] *See supra* Part III.D.3.c.i.

[686] Costs for initial application materials are $89,020 to prepare detailed design specifications. $44,510 is half of this total. ($44,510 per group × 9 groups) = $400,590.

[687] *See supra* Part III.D.3.d.i.

[688] Labor costs include 5 hours by a compliance attorney. (5 hours × $374/hour) = $1,870. ($1,870 per group × 9 groups) = $16,830.

[689] *See supra* note 523.

[690] *See supra* note 524.

[691] *See supra* Part III.D.3.d.ii.

[692] *See supra* Part III.D.3.d.ii. The PRA estimates that the Plan Processor would incur $91,760 in labor costs to review each application. In this analysis, the Commission assumes all nine Participant Groups would apply for exceptions. (9 Participant Groups × $91,760 per application) = $825,840.

[693] *Id.*

[694] *See supra* note 531. The PRA estimates that the Plan Processor would incur $18,550 in labor costs to validate each Excepted Environments. In this analysis, the Commission assumes all nine Participant Groups would apply for exceptions. (9 Participant Groups × $18,550 per validation) = $166,950.

[695] *Id.*

specifications and notify the Participant of any identified non-compliance. The Commission preliminarily estimates the Plan Processor will incur annual ongoing costs of $302,600 [696] to perform these tasks.

The proposed amendments require that each Participant using a non-SAW environment simultaneously notify the Plan Processor, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group of any material changes to its security controls for the non-SAW environment. The Commission cannot predict how many such changes would occur because the Commission does not know how often each Participant Group would make changes to its Excepted Environment that would necessitate material changes to its security controls, but for each such instance, the Commission preliminarily estimates the notifying Participant Group would incur labor costs of approximately $5,200.[697]

The Commission recognizes that by providing an exception procedure to the requirement that Participants employ the user-defined direct query and bulk extract tools to access CAT Data within SAWs, variability across environments from where CAT Data is accessed and analyzed will necessarily increase. The amendments will provide for a level of security in Excepted Environments that will be similar but not identical to security within SAWs because Excepted Environments may implement security controls, policies, and procedures differently than SAWs. The Commission preliminarily believes the risk of individual Excepted Environments being less secure than SAWs is mitigated by the review process of applications for exceptions and Plan Processor verification and monitoring steps required by the proposed amendments.

4. OTQT and Logging

The CAT NMS Plan does not limit the amount of CAT Data a regulator can extract or download through the online targeted query tool (''OTQT''); the CAT NMS Plan only states that the Plan Processor must define the maximum number of records that can be viewed in the OTQT as well as the maximum number of records that can be downloaded.[698]

The proposed amendments would remove the ability of the Plan Processor to define the maximum number of records that can be downloaded via the OTQT, and instead limit the maximum number of records that can be downloaded via the OTQT to no more than 200,000 records per query request.[699] The Plan does not explicitly prevent use of the OTQT to download significant quantities of CAT Data, although the OTQT does not provide access to all fields in transactional CAT Data that are available through the user defined direct query tool, (''UDDQ''). Because the Plan does not currently distinguish between what types of analytic environments (SAWs versus Excepted Environments) may access particular tools (*i.e.,* OTQT versus UDDQ), this may not be a significant security distinction under the Plan because downloading such data through the OTQT would be merely less efficient than doing so with other data extraction tools if either approach were available in a given analytic environment. However, with the proposed amendments' provisions that restrict the use of the UDDQ and bulk extract methods to Plan Processor provided SAWs and Excepted Environments, some regulatory users may be incentivized to use a succession of queries to download larger samples of CAT Data using the OTQT to avoid the need to work within the SAWs or Excepted Environments.

The Commission preliminarily believes that by limiting the number of records of CAT Data that can be extracted from the OTQT, the proposed amendments are likely to result in more regulatory analysis of CAT Data being performed within the security perimeter established by the CISP of the Plan Processor because regulatory activities that require extraction of more than 200,000 records would need to be performed using the UDDQ or by bulk extraction, activities that would be limited to Plan Processer provided SAWs or Excepted Environments under the proposed amendments. The Commission preliminarily believes that this is likely to reduce the attack surface of CAT by reducing the magnitude of CAT Data accessed outside of these potentially more secure environments. The Commission recognizes, however, that limiting the use of the OTQT to queries that extract fewer than 200,000 records may also reduce regulatory use of CAT Data to the extent that a regulatory user may not have the technical skills that would be required to use other access methods.[700]

The proposed amendments extend the information in log files that the Participants are required under the Plan to submit to the Operating Committee monthly, specifically, by defining the term ''delivery of results'' and requiring the logging of access and extraction of CAT Data.[701] The Commission estimates that the Plan Processor will incur one-time labor costs of $87,960 [702] to make the initial necessary programming and systems changes to log delivery of results of queries of CAT Data and the access and extraction of CAT Data. In addition, the Plan Processor would incur an annual ongoing expense of $5,100 [703] to generate and provide the additional information in monthly reports required by the proposed amendments. The Commission preliminarily estimates that the Participants would incur ongoing annual labor costs of $970,200 [704] for the Operating Committee to review the additional information in the monthly reports. Further, the requirement that limits the number of records that can be extracted through use of the OTQT may make it impossible for some regulatory functions that are required only situationally (such as ad hoc queries to investigate trading by a single trader in all symbols or by multiple traders in a single symbol) to be performed outside the SAW (or Excepted Environments). This restriction may cause some Participants to establish SAWs, obtain an exception, or extend their use of RSAs for activities that are performed infrequently. This outcome may be more costly to these Participants than working less efficiently through the OTQT in ad hoc situations because it may be less costly to Participants to use the OTQT inefficiently than to make these alternative arrangements for only occasional use.

5. CAT Customer and Account Attributes

As noted above, the Commission granted the Participants' PII Exemption

[696] *See supra* note 534.

[697] Labor costs include 10 hour of Senior Systems Analyst labor, 3 hours by a compliance attorney, and 2 hours by the CISO. For the CISO, hourly rate calculations use the hourly rate for a Chief Compliance Officer. (10 hours × $291/hour + 3 hours × $374/hour + 2 hours × $543/hour) = $5,118.

[698] *See supra* Part II.D.

[699] *See supra* Part II.D.

[700] The Commission preliminarily believes that access to CAT Data through the UDDQ would require greater technical skills on the part of the user such as knowledge of a structured query language and an understanding of structured databases.

[701] *See supra* Part III.D.4.

[702] *See supra* Part III.D.4.

[703] *See supra* Part III.D.4.

[704] Cost estimate assumes each Participant would annually incur 12 hours of Operating Committee Member labor and 108 hours of Compliance Manager labor. (12 hours × $381/hour + 108 hours × $317/hour) = $38,808 per Participant. Collectively, Participants would incur ($38,808 per Participant × 25 Participants) = $970,200.

Request to allow for an alternative approach to generating a Customer-ID and to allow for an alternative approach which would exempt the reporting of dates of birth and account numbers associated with retail customers who are natural persons.[705] This exemptive relief allows the Participants to implement an alternative approach to generating Customer-ID(s), subject to certain conditions set forth in the exemptive relief, but does not bar the Participants from implementing the Plan's original Customer-ID approach.

The baseline for customer and account information availability in CAT assumes the implementation of the alternative approach described in the PII Exemption Order and the creation of the CCID Subsystem. The exemptive relief includes certain conditions that also are included in the baseline for the proposed amendments.[706] First, the exemptive relief requires that the Participants ''ensure the timeliness, accuracy, completeness, and integrity of interim value[s]'' in the CCID Subsystem.[707] Second, the Participants must assess the overall performance and design of the CCID Alternative process and the CCID Subsystem as part of each annual Regular Written Assessment of the Plan Processor.

The Commission proposes to amend the CAT NMS Plan to: (1) Delete the Industry Member reporting of ITINs/SSNs, dates of birth and account numbers for natural persons and require the reporting of year of birth; (2) establish a process for creating Customer-ID(s); (3) impose specific obligations on the Plan Processor that will support the revised reporting requirements and creation of Customer-ID(s); and (4) amend existing provisions of the CAT NMS Plan to reflect the new reporting requirements and process for creating Customer-ID(s), as further discussed below.[708] These provisions reflect the PII exemptive relief previously granted by the Commission.

The Commission preliminarily believes that the provisions of the proposed amendments discussed in this section largely reflect exemptive relief and current implementation specifications of the Participants, with the exception of the requirement that customer addresses reported to the CAIS have separate fields for street numbers and names. Because the specifications are still in development, the Commission preliminarily believes that the cost impact of this provision on Participants is likely to be de minimis. The Commission further preliminarily believes that CAT Reporters have not implemented an alternative street address specification and the costs to CAT Reporters to implement this change will be de minimis because the requirement does not require additional information to be reported.

The proposed amendments include provisions that by design, reduce certain options for future development of the Plan. For example, the Participants would not be able to decide at a later date to no longer use their exemptive relief and instead change the CAT implementation to conform to the Plan as it stands at that time. Although the Commission believes that the Participants would be unlikely to take such an approach in the future after incurring the costs to secure exemptive relief and implement alternative approaches required by such relief, it recognizes that the proposed amendments curtail that option to the Participants.

6. Customer Identifying Systems Workflow

The Commission is proposing to amend the CAT NMS Plan to define the workflow for accessing Customer and Account Attributes, and to establish access restrictions.[709] Accordingly, the Commission proposes to amend the CAT NMS Plan to (1) specify how existing data security requirements apply to Customer and Account Attributes; (2) define the Customer Identifying Systems Workflow and the General Requirements for accessing Customer Identifying Systems; (3) establish general requirements that must be met by Regulatory Staff before accessing the Customer Identifying Systems, which access will be divided between two types of access—manual access and programmatic access; and (4) establish the specific requirements for each type of access to the Customer Identifying Systems. Some of these provisions would reflect the PII exemptive relief previously granted by the Commission, making the alternative approach described in the PII Exemption Order a requirement of the Plan. The Commission discusses potential benefits of the proposed new provisions of the Plan relative to the baseline below.

The proposed amendments would replace the term ''PII'' with ''Customer and Account Attributes'' and to reflect that Customer Identifying Systems, including CAIS, now contain the information that identifies a Customer; prohibit Customer and Account Attributes from being included in the result sets to queries of transactional CAT Data; and update requirements related to the PII access audit trail to reflect the CAIS approach. These requirements mirror requirements for access to customer information already contained in the Plan or the PII Exemptive Order.[710] The Commission preliminarily believes that these provisions may avoid inefficiencies in implementation to the extent that Participants might make investments in implementation activities that do not reflect the approach to customer information and account attributes outlined in the exemptive relief.

The proposed amendments include provisions that limit access to the Customer Identifying Systems to two types of access—manual and programmatic. The Commission preliminarily believes that this may improve the security of CAT Data by limiting access to CAIS data to two defined access methods. The Commission preliminarily believes that by doing so the likelihood that customer information might be compromised in a potential breach will be decreased. To the extent that a bad actor would be limited in his or her ability to access customer information in a manner other than these two access pathways, customer information within the CAT System should be more secure.

The proposed amendments include 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.[711] The Commission preliminarily believes that this authorization step may reduce the risk of inappropriate use of customer and account information by ensuring that programmatic access that can potentially return information about a large group of customers is only granted when an appropriate regulatory use exists. Further, the Commission preliminarily believes this requirement may reduce the amount of CAT Data exposed to regulators as they perform their duties because it may increase regulatory use of manual as opposed to programmatic access to the CCID Subsystem and CAIS when manual access is sufficient for a regulatory purpose.

[705] *See supra* Part II.E.

[706] *See* PII Exemption Order, *supra* note 164, at 16157.

[707] *See id.*

[708] *See supra* Part II.E.

[709] *See supra* Part II.F.

[710] *See supra* Part II.F.1.

[711] *See supra* Part II.F.5.

The proposed amendments would establish programmatic access as a required element of the CAT NMS Plan.[712] The provision of programmatic access enables authorized Regulatory Staff to query the CAIS and CCID Subsystems to access information on multiple customers or accounts simultaneously.[713] The Commission recognizes that allowing programmatic access to CAIS and CCID data by authorized users potentially will allow Regulatory Staff to be exposed to a greater quantity of Customer and Account Attributes. To the extent that this exposure provides more opportunities for this data to be used inappropriately, this may reduce the confidentiality of CAIS and CCID data. However, the Commission preliminarily believes the Commission authorization step required before programmatic access can be exercised mitigates this risk because the application review process requires documentation establishing the regulatory purpose of the programmatic access, and provides for an approval process based on such access being generally consistent with specific standards that would justify such access.[714]

The Commission preliminarily estimates that the Plan Processor will incur labor costs of $620,200 [715] to establish programmatic access to the CCID Subsystem and CAIS.

Under the proposed amendments, Participants that require programmatic access to the CAIS or CCID Subsystems would need to apply for authorization from the Commission.[716] The Commission cannot estimate how many Participants would need to apply for authorization, or how many applications might be required for each Participant that would access these subsystems. The Commission preliminarily estimates that each application for authorization would cause a Participant to incur $19,100 [717] in labor costs.

The Commission preliminarily estimates that the requirements to maintain and provide to Participants, the Commission, and the Operating Committee monthly audit reports that track permissions for and access to Customer Identifying Systems will result in an aggregate ongoing annual cost to the Plan Processor of $373,500 [718] per year.

In addition, the requirement that regulators obtain Commission approval before exercising programmatic access to the CCID Subsystem or the CAIS may reduce or delay regulatory use of the customer data contained in these databases. The Commission recognizes that a possible indirect cost of the proposed amendments is less overall regulatory use of CAT Data. In the CAT NMS Plan Approval Order, the Commission discussed certain benefits that were likely to result from CAT, including benefits from analysis and reconstruction of market events.[719] To the extent that provisions of the proposed amendments complicate access to CAT Data, prohibit its use for purposes that are both regulatory and commercial, or make use of CAT Data more expensive to regulators, fewer of these benefits may accrue to investors.

7. Participants' Data Confidentiality Policies

To maintain CAT Data confidentiality, the Plan requires the Participants to implement policies related to information barriers, restricts access only to designated persons for regulatory purposes, and imposes penalties for non-compliance to these requirements.[720] The Plan currently requires each Participant to periodically review the effectiveness of these policies and procedures, and that they take prompt action to remedy deficiencies in such policies and procedures. The Plan does not require the Participants to make their policies related to data confidentiality publicly available. Although Participants may disclose data confidentiality policies relating to information collected from customers in the course of business, these policies do not generally extend to policies and procedures in place to deal with CAT Data.

As discussed below, the Commission is proposing amendments to modify and supplement the Plan to provide additional specificity concerning data usage and confidentiality policies and procedures and to make the policies publicly available.[721]

The proposed amendments would modify the existing Plan provisions designed to protect the confidentiality of CAT Data so that they apply to the Proposed Confidentiality Policies, and Participant-specific procedures and usage restriction controls.[722] As a result of this change, Participants would be required to report any instance of noncompliance with the data confidentiality policies, procedures, and usage restrictions adopted by such Participant to the Chief Compliance Officer within 24 hours of becoming aware. While the Plan currently requires reporting of a CAT security breach within 24 hours, it does not require reporting instances of noncompliance with the Proposed Confidentiality Policies or procedures and usage restriction controls adopted by such Participant pursuant to Section 6.5(g)(i). The Commission preliminarily believes that this requirement will improve the security of CAT Data in two ways. First, bringing any instance of noncompliance to the attention of the Chief Compliance Officer would provide an opportunity for such a weakness to be addressed and reduce the risk of future instances of noncompliance to the extent that an instance of noncompliance may demonstrate a weakness in the Proposed Confidentiality Policies, procedures, or usage restrictions, and such a weakness can then be addressed when it would not have otherwise been. Second, the Commission preliminarily believes that the notification requirement may elevate the profile of the Proposed Confidentiality Policies among the Participants because an instance of noncompliance could not be handled through solely internal channels, instead triggering review by the Chief Compliance Officer. This may incentivize the Participants to more effectively implement these policies to avoid instances of noncompliance.

The proposed amendments would require the Proposed Confidentiality Policies to be identical across Participants. While the proposed amendments allow for each Participant to establish its own procedures and usage restrictions to operationalize these policies, accommodating the Participants' organizational, technical and structural uniqueness, the overarching policies would be centrally established and common across Participants. The Commission preliminarily believes that having common data confidentiality policies

[712] *See supra* Part II.

[713] *See supra* Part II.F.7.

[714] *See supra* Part II.F.6.

[715] The estimates assumes 640 hours each of labor by a Senior Database Administrator, a Senior Programmer and a Senior Business Analyst. (640 hours × $349/hour + 640 hours × $339/hour + 640 hours × $281/hour) = $620,160.

[716] *Id.*

[717] Labor cost estimate assumes 15 hours of attorney labor, 10 hours of compliance manager labor, 10 hours of operations specialist labor and 15 hours by a chief compliance officer. (15 hours × $426/hour + 10 hours × $317/hour + 10 hours × $140/hour + 15 hours × $543/hour) = $19,105.

[718] *See supra* note 552.

[719] *See* CAT NMS Plan Approval Order, *supra* note 3, at Part V.E.2. For example, in the wake of a market event, a regulator might perform an analysis of cross-market trading before the event. To the extent that making such an analysis public is a commercial as well as regulatory activity under the proposed amendments, fewer such analyses are likely to be performed.

[720] *See supra* Part II.G.

[721] *See id.*

[722] *See supra* Part II.G.1.

across Participants may avoid unnecessary variation across Participants in how they meet the data confidentiality requirements of the Plan. However, the Commission recognizes it is also possible that the Participants could adopt relatively weak central policies that would ultimately reduce the security of CAT Data. The Commission preliminarily believes this outcome is unlikely because central development of these policies allows the Participants to access their collective expertise in creation of these policies. The Commission recognizes that in situations where policies are centrally developed, it is possible that an individual Participant might have developed stronger policies and procedures in the absence of the proposed amendments. However, the Commission believes this potential outcome is mitigated by the fact that having multiple Participants involved in the development of these policies is likely to result in more robust policies because more expertise can be incorporated into their development.

The proposed amendments would define ''Regulatory Staff'' and limit access to CAT Data to persons designated by Participants, which persons must be Regulatory Staff or technology and operations staff that require access solely to facilitate access to and usage of CAT Data stored in the Central Repository by Regulatory Staff.[723] Currently, the CAT NMS Plan has numerous references to ''regulatory staff,'' and outlines benefits and limitations on such regulatory staff, including the ability to access all CAT Data, but does not define the term or provide any guidance or limitations on how Participants may identify ''regulatory staff.'' [724] The Commission preliminarily believes that defining Regulatory Staff may improve the confidentiality of CAT Data by preventing expansive interpretations of this term (such as classifying staff members that have primarily business functions as Regulatory Staff) that could result in non-Regulatory Staff of Participants having exposure to CAT Data that might be used inappropriately.

The proposed amendments would require that the Proposed Confidentiality Policies limit non-Regulatory Staff access to CAT Data to circumstances in which there is a specific regulatory need for such access and a Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation), or designee, provides written approval for each instance of access by non-Regulatory Staff. The Plan has no provision that bars non-Regulatory Staff from accessing CAT Data, though it does limit the use of CAT Data to only regulatory or surveillance purposes. The Commission preliminarily believes that the proposed amendments would further limit the number of individuals that have access to CAT Data by barring access to non-Regulatory Staff members (subject to proposed exceptions) and that limiting the number of individuals that have access to CAT Data reduces the risk that it would ultimately be used inappropriately because fewer people would have the opportunity to engage in an inappropriate use. However, while the requirement that non-Regulatory Staff not have access to CAT Data may reduce the risk of CAT Data being used inappropriately, the Commission also recognizes that this restriction may slow a Participant's ability to respond to urgent situations such as a market event. A provision to allow a Participant's Chief Regulatory Officer to allow such access may mitigate inefficiencies such as a slowed response to a market event that could result from an absolute prohibition of staff other than Regulatory Staff accessing CAT Data. For example, in the case of a market event, a Participant's analysis of events may need access to expert staff in operations or business functions of the Participant, and the need for rapid analysis of CAT Data may warrant such an exception to further this regulatory purpose. The Commission recognizes that providing this access to staff other than Regulatory Staff may increase the risk that CAT Data would be used inappropriately because additional Participant Staff would necessarily be exposed to CAT Data in such a case. However, the Commission preliminarily believes this risk is mitigated by the requirement that the Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation) provide written permission for such access because it is likely to limit its use to exceptional situations because ensuring the confidentiality of CAT Data is among the Chief Regulatory Officer's (or similarly designated head(s) of regulation's) primary responsibilities and because the CAT NMS Plan requires CAT Data only to be accessed for surveillance or regulatory purposes. Furthermore, establishing documentation of such instances will facilitate the Plan Processor's and independent accountant's [725] review of the Participant's compliance with the Proposed Confidentiality Policies. This may further limit the use of and any additional risk posed by this provision only to exceptional circumstances because such use is likely to be reviewed by the independent auditor.

The proposed amendments would limit the extraction of CAT Data to the minimum amount necessary to achieve specific surveillance or regulatory purposes.[726] The Commission preliminarily believes that this provision may improve CAT Data security by reducing the attack surface of CAT because extracted data would reside outside of the scope of the CAT security provisions and would be beyond the Plan Processor's security monitoring scope.

The proposed amendments would require the Proposed Confidentiality Policies to define the individual roles and regulatory activities of specific users, including those users requiring access to Customer and Account Attributes, of the CAT.[727] The Commission preliminarily believes that this provision may improve the security of CAT Data by allowing the Participants to identify regulatory users whose roles do not regularly require access to more sensitive information stored in the CCID Subsystem and CAIS and restrict that access. To the extent that fewer users have access to this more sensitive data, the risk of inappropriate use of customer information may be reduced.

The proposed amendments require that Participants incorporate policies relating to the access of Customer and Account Attributes, Programmatic CAIS Access, and Programmatic CCID Subsystem Access in the Proposed Confidentiality Policies.[728] This requirement would result in the adoption of a common policy for access to Customer and Account Attributes across Participants. The Commission preliminarily believes that this may improve security of CAT Data by reducing variation among policies across Participants.[729] The proposed amendments also require that the Proposed Confidentiality Policies be reasonably designed to implement and satisfy the Customer and Account Attributes data requirements of Section 4.1.6 of Appendix D such that Participants must be able to demonstrate

[723] *See supra* Part II.G.2.

[724] *See, e.g.,* CAT NMS Plan, *supra* note 3, at Section 6.5(f)(ii) and Appendix D, Sections 6.1, 6.2, 8.1.

[725] The role of independent accountants in reviewing Participants' compliance is discussed further below.

[726] *See supra* Part II.G.3.a.

[727] *See supra* Part II.G.3.b.

[728] *See supra* Part II.G.3.c.

[729] *See supra* note 640.

that a Participant's ongoing use of Programmatic CAIS and/or CCID Subsystem access is in accordance with the Customer Identifying Systems Workflow.[730]

The proposed amendments would require that each Participant shall engage an independent accountant annually to perform an examination of compliance with the policies required by the Proposed Confidentiality Policies.[731] The Commission preliminarily believes that this provision may improve the security of CAT Data by facilitating external review of the Participants' compliance with the Proposed Confidentiality Policies by an independent third party. To the extent that this independent third party identifies deficiencies in the Participants' compliance with the Proposed Confidentiality Policies that would not otherwise be identified and the identification of such deficiencies leads to remediation that makes such deficiencies less likely to recur, the Commission preliminarily believes these provisions may improve CAT Data security.

The Commission preliminarily believes that provisions of the proposed amendments discussed in this section would entail one-time costs of $1.2MM,[732] and ongoing annual costs of $1.9MM.[733] These costs are summarized in Table 6 and discussed further below.

TABLE 6—SUMMARY OF COSTS FOR POLICIES AND PROCEDURES ($)

Activity	Participants		Plan processor	
	Labor	External	Labor	External
Initial				
Develop central Proposed Confidentiality Policies	254,900	50,000	.....	.....
Review and approve Proposed Confidentiality Policies	.....	.....	10,900	.....
Develop procedures to implement the PCP	901,000	.....	.....	.....
Total	1,155,900	50,000	10,900	.....
Annual				
Review Proposed Confidentiality Policies and remediate	51,000	5,000	.....	.....
Review and approve Proposed Confidentiality Policies	.....	.....	5,400	.....
Maintain and remediate procedures	289,700	.....	.....	.....
Annual third party audit	139,900	1,437,500	.....	.....
Total	480,600	1,442,500	5,400	.....

The proposed amendments would require that the Participants jointly develop the Proposed Confidentiality Policies. The Commission preliminarily estimates the Participants will incur labor costs of $254,900[734] to develop these policies.[735]

The Commission preliminarily estimates that it would require 10 hours by the CCO and 10 hours by the CISO, both employees of the Plan Processor, to review the Proposed Confidentiality Policies. The Commission preliminarily estimates that this would result in the Plan Processor incurring $10,900[736] in labor costs.[737] The Commission also preliminarily believes that the Participants will consult with outside legal counsel in the drafting of the Proposed Confidentiality Policies, and estimates this external cost to be $50,000.[738]

The proposed amendments would require the Participants to jointly review the effectiveness of the Proposed Confidentiality Policies annually and take prompt action to remedy deficiencies in such policies.[739] The Commission preliminarily estimates that this review would require approximately 20% of the labor of the initial effort to jointly draft those policies because presumably many of the policies would not need revision annually. Consequently, the Commission preliminarily estimates that the Participants would annually incur $51,000[740] in labor costs and outside legal costs of $5,000[741] to complete these tasks. In addition, the Commission preliminarily estimates the Plan Processor would incur annual labor costs of $5,400[742] to review updates to the Proposed Confidentiality Policies.[743]

After the Participants jointly develop the Proposed Confidentiality Procedures, each Participant would incur costs to develop procedures and usage restriction controls to implement those policies. The Commission preliminarily believes that Participants will perform this task at the Participant Group level of organization: For example, a Participant Group that controls four exchanges will centrally develop those policies and then individualize them as necessary across its exchanges.

[730] *See supra* Part II.F.7 and Part II.F.8.

[731] *See supra* Part II.G.4.

[732] ($1,115,900 + $50,000 + $10,900) = $1,216,800.

[733] ($480,600 + $1,442,500 + $5,400) = $1,928,500.

[734] Labor cost estimate assumes 150 hours by Chief Regulatory Officers, 150 hours by Chief Compliance Officers, 100 hours by Compliance Managers, 50 hours by Compliance Attorneys, 20 hours by Sr. Operations Managers and 10 hours by Deputy General Counsels. An additional 20 hours would be required for Operating Committee members to review and approve the policies. Labor costs for Operating Committee members assume an hourly rate for a Vice President of Operations. Hourly rate estimated by using the median annual salary from *www.payscale.com*, multiplying by 5.35 to account for other compensation, benefits and overhead and adjusting for 1800 hours of labor per year. (($128,159 × 5.35/1800 = $381/hour). The Commission estimates the hourly rate of a Chief Regulatory Officer as 125% of the rate of a Chief Compliance Officer, or $543/hour × 1.25 = $679/hour. (150 hours × $679/hour + 150 hours × $543/hour + 100 hours × $317/hour + 50 hours × $374/hour + 20 × $374/hour + 10 hours × $612/hour + 20 hours × $381/hour) = $254,920.

[735] *See supra* Part III.D.7.

[736] Labor cost estimate assumes 10 hours of CCO labor and 10 hours of CISO labor. (10 hours × $543/hour + 10 × $543/hour) = $10,860.

[737] *See supra* Part III.D.7.

[738] *Id.*

[739] *Id.*

[740] $254,900 × 20% = $50,980.

[741] *See supra* Part III.D.7.

[742] *See supra* Part III.D.7. The Commission assumes review of the Proposed Confidentiality Policies would require half the labor of initial review of the policies. *See supra* note 736. $10,860 × 50% = $5,430.

[743] *See supra* Part III.D.7. The Commission is assuming that such updates would occur annually. If updates were more frequent, costs would be proportionately higher.

The Commission preliminarily estimates that the Participants collectively would incur labor costs of $901,000[744] to initially develop and draft the procedures and usage restriction controls. The Commission preliminarily estimates that the ongoing annual labor cost to Participants of maintaining and reviewing the procedures and usage restriction controls and taking prompt action to remedy deficiencies in such policies, procedures and usage restriction controls would be approximately $289,700.[745]

The proposed amendments would require each Participant to engage an independent accounting firm annually to perform an examination of compliance with the policies required by Section 6.5(g)(i) and submit the examination report to the Commission.[746] The Commission preliminarily estimates that each Participant would incur labor costs of $5,600[747] to satisfy this requirement, as well as $57,500[748] in external consulting costs.

8. Regulator & Plan Processor Access

The Plan does not specify any restrictions on data sources used in the development of CAT systems, tools and applications. Currently, Plan Processor staff and contractors are not prohibited from using any CAT Data during development and testing activities.

The proposed amendments would restrict such development and testing activities to non-production data in all cases for CAIS data. Further, they would restrict such development activities to non-production data for transactional data, unless it were not possible to do so. In such a case, development work could access the oldest available production data. The Commission preliminarily believes that these provisions may improve the confidentiality of CAT Data by preventing Plan Processor employees and contractors having exposure to CAT Data that might be used inappropriately.

The Commission preliminarily believes that test transactional data has already been prepared and used in the implementation of CAT reporting. However, the Plan Processor may need to prepare test data to be used in development work for systems, tools and applications that would access the CAIS. The Commission preliminarily estimates that the Plan Processor will incur costs of $10,270[749] to create this data and make it available to Plan Processor staff and contractors performing this development and testing work.

The Commission preliminarily believes that provisions of the proposed amendments that prohibit any use of CAT Data that has both regulatory and other uses may reduce Participants' use of CAT Data. While the Plan already prohibits commercial use of CAT Data, it does not specifically prohibit a regulatory use that also serves a non-regulatory purpose. This proposed amendment may prevent some Participants from using CAT Data in a rule filing that might lead the Commission to approve or disapprove a filing that could reduce trading costs to some investors. The Commission preliminarily believes that it is unlikely that such a rule filing would be approved or disapproved due to the Participants' inability to support their rule filings with CAT Data because Participants retain the ability to analyze their own in-house data in support of their rule filings, and to provide both quantitative arguments based on that in-house data as well as qualitative arguments that support those rule filings.

9. Secure Connectivity

The Plan allows CAT Data reporters and users to connect over private lines or secured public lines.[750] There is no specific requirement that any reporters use private lines and connectivity requirements do not differentiate between Participants and Industry Members in this regard.[751] Since approval of the Plan, the Participants have determined that they will connect to the CAT infrastructure using only private lines. However, the Commission recognizes that no language in the Plan requires that Participants will use only private lines in the future.

The Plan Processor requires two-factor authentication for connection to CAT. Authentication incorporates a geolocation blacklist including 16 countries.[752]

Currently, the CAT NMS Plan imposes requirements on data centers housing CAT Systems (whether public or private), but does not impose any geographical restrictions or guidelines. The Commission believes that all current CAT Data centers are located in the United States.

The proposed amendments would require Participants to connect to CAT infrastructure using private lines, and Industry Members to connect to CAT using secure methods such as private lines for machine-to-machine interfaces or encrypted Virtual Private Network connections over public lines for manual web-based submissions.[753] The proposed amendments would also require the Plan Processor to implement capabilities to restrict access through an ''allow list'' that would only allow access to CAT from countries where CAT reporting or regulatory use is both necessary and expected.[754] In addition, the proposed amendments would require that CAT Data centers be located in the United States.[755]

The Commission preliminarily believes these provisions of the proposed amendments will improve the security of CAT Data in two ways. First, although all Participants currently plan to connect to CAT using private lines,

[744] *See supra* note 568. Labor cost estimate includes 96 hours by an Attorney, 96 hours by a Compliance Manager, 30 hours by a Senior Systems Analyst, 30 hours by an Operations Specialist, 20 hours by a Chief Compliance Officer and 10 hours by a Director of Compliance. (96 hours × $426/hour + 96 hours × $317/hour + 30 hours × $291/hour + 30 hours × $140/hour + 20 hours × $543/hour + 10 hours × $500/hour) = $100,118. ($100,118 per group × 9 groups) = $901,062.

[745] *See supra* note 569. Labor cost estimate includes 28 hours by an Attorney, 28 hours by a Compliance Manager, 8 hours by a Senior Systems analyst, 8 hours by an Operations Specialist, 10 hours by a Chief Compliance Officer and 5 hours by a Director of Compliance. (28 hours × $426/hour + 28 hours × $317/hour + 8 hours × $291/hour + 8 hours × $140/hour + 10 hours × $543/hour + 5 hours × $500/hour) = $32,182. ($32,182 × 9) = $289,638.

[746] *See supra* Part III.D.7. It is possible that Participants may realize economies of scale by engaging for this review at the Participant Group level. However, because the third party audit is required for each Participant regardless of Participant Group membership, the Commission preliminarily believes that it is appropriate to estimate this expense at the Participant level because efficiencies in third-party reviews is not under the Participants' direct control.

[747] Labor cost estimate assumes 3 hours of Chief Compliance Officer labor, 5 hours of Compliance Manager labor, 3 hours of Compliance Attorney labor, 2 hours of Senior Systems Analyst labor, and 2 hours of Senior Programmer labor. (3 hours × $543/hour + 5 hours × $317/hour + 3 hours × $374/hour + 2 hours × $291/hour + 2 hours × $339/hour) = $5,596. ($5,596 per Participant × 25 Participants) = $139,900.

[748] *See supra* note 574. ($57,500 per Participant × 25 Participants) = $1,437,500.

[749] Estimate assumes 20 hours of Senior Programmer labor and 10 hours of Senior Database Administrator labor. (20 hours × $339/hour + 10 hours × $349/hour) = $10,270.

[750] *See supra* Part II.I.

[751] The distinction between Industry Members and Participants may be significant because while Participants are reporters of CAT Data, they are also users of CAT Data in their regulatory roles and thus have the ability to access and extract CAT Data. Industry Members are not potential users of CAT Data.

[752] *See* FINRA CAT Industry Member Onboarding Guide at *https://www.catnmsplan.com/sites/default/files/2020-02/FINRA-CAT-Onboarding-Guide-v1.5.pdf,* item 7, page 19.

[753] *See supra* Part II.I.

[754] An ''allow list'' could be based on geography, server or IP. This is discussed further below.

[755] *See supra* Part II.I.

codifying this decision reduces the risk that, at a later date, one or more Participants might elect to connect with CAT in a less secure manner than with private lines, as they currently plan to connect to CAT. Furthermore, the Commission preliminarily believes that because Participants are not only reporters, but also users of CAT Data in their regulatory roles, ensuring that they connect to CAT in the most secure manner may further safeguard CAT Data by making the normal access mode for CAT Data be through private lines.[756] The Commission recognizes that this restriction may also prevent the Participants from electing to connect to CAT through a more secure method developed in the future that does not rely upon private lines. The Commission preliminarily believes this concern is mitigated by the Participants' ability to amend the Plan at a later date to allow such an access method.

Second, the Commission preliminarily believes that the requirement to establish ''allow listing'' procedures to allow connections to CAT only to those countries where CAT reporting or regulatory use is both necessary and expected might reduce the risk of a security breach by limiting connections from other sources.

The Commission preliminarily estimates that provisions of the proposed amendments concerning secure connectivity will cause the Plan Processor to incur initial one-time labor costs of $33,100[757] and ongoing annual labor costs of $3,100.[758]

The Commission preliminarily estimates that requiring the Plan Processor to develop ''allow listing'' capability will cause the Plan Processor to incur initial one-time implementation labor costs of $13,700.[759] Maintaining this list will cause the Plan Processor to incur $1,200[760] in ongoing annual costs. In addition, the Plan Processor is estimated to incur $19,400[761] in one-time labor costs to implement procedures to allow access to CAT if the source location for a particular instance of access request cannot be determined technologically. The Commission estimates that the Plan Processor will incur $1,900[762] in annual ongoing costs to maintain and enforce this restriction.

The Commission recognizes that the requirement that CAT data centers be located in the United States may prevent the Plan Processor from locating CAT data centers in other areas that might reduce the costs associated with maintaining CAT data centers. This could cause future costs of CAT to be higher than they might be otherwise.[763]

10. Breach Management Policies and Procedures

The Plan includes a requirement for reporting noncompliance incidents and security breaches to the Chief Compliance Officer.[764] The Plan also requires the Plan Processor to develop policies and procedures governing its responses to systems or data breaches, including a formal cyber incident response plan, and documentation of all information relevant to breaches.[765] CAT LLC has stated that in the event of unauthorized access to CAT Data that it will ''. . .take all reasonable steps to investigate the incident, mitigate potential harm from the unauthorized access and protect the integrity of the CAT System. CAT LLC also will report unauthorized access to law enforcement, the SEC and other authorities as required or as it deems appropriate. CAT LLC will notify other parties of unauthorized access to CAT Data where required by law and as it otherwise deems appropriate. CAT LLC will maintain insurance that is required by law.''[766]

The proposed amendments would require the formal cyber incident response plan to incorporate corrective actions and breach notifications, modeled after similar provisions in Regulation SCI.[767] Because of the lack of specificity in requirements for the cyber incident response in the Plan, it is possible that Participants might satisfy the existing provisions without providing for breach notifications to affected CAT Reporters, the Participants and the Commission, and prompt remediation of security threats. While the Commission believes it is unlikely the Participants would leave a security threat unaddressed, it also preliminarily believes that requiring procedures to be in place to deal with an incident ahead of time facilitates a quicker response should such an incident occur because procedures can specify who is to be involved in the response and in what capacity, and where authority lies in making the response.

The proposed amendments would require the formal cyber incident response plan to include taking appropriate corrective action that includes, at a minimum, mitigating potential harm to investors and market integrity, and devoting adequate resources to remedy the systems or data breach as soon as reasonably practicable. While the Commission preliminarily believes that the Participants are likely to take corrective action in the wake of a security breach without this explicit provision in the Plan, to the extent that this provision hastens the Participants' corrective action in the wake of a cyber incident, this provision may improve the security of CAT Data by reducing potential harm to investors and market integrity that may accrue if such a response were delayed.

In addition, the proposed amendments would require the Plan Processor to provide breach notifications of systems or data breaches to CAT Reporters that it reasonably estimates may have been affected, as well as to the Participants and the Commission, promptly after any responsible Plan Processor personnel have a reasonable basis to conclude that a systems or data breach has occurred. In addition, the proposed amendments state that the cyber incident response plan must provide for breach notifications. The Commission preliminarily believes that breach notifications in the wake of a cyber incident may reduce harm to CAT reporters and investors whose data was exposed through a cyber incident. While the proposed amendments allow for delay in breach notification when such notification could expose environments from which CAT Data is accessed and analyzed to greater security risks, or compromise an investigation into the breach, the proposal would require the affirmative documentation of the reasons for the Plan Processor's determination to temporarily delay a breach notification, which is important to prevent the Plan Processor from improperly invoking this exception.

The proposed amendments would provide an exception to the requirement for breach notifications for systems or data breaches ''that the Plan Processor reasonably estimates would have no or

[756] The Commission preliminarily believes that use of the Online Targeted Query Tool through encrypted connections over public lines may still occur, but because of the 200,000 row limit to OTQT queries, it would be more difficult for a bad actor that gained access through a public line to access CAT Data if the Plan Processor is able to make other tools only available to users connecting through private lines. To the extent that the Plan Processor does not restrict access to other tools to users not connecting through public lines, this potential benefit would not be realized.

[757] ($13,700 + $19,400) = $33,100.

[758] ($1,200 + $1,900) = $3,100.

[759] *See supra* note 577.

[760] *See supra* note 579.

[761] *See supra* note 581.

[762] *See supra* note 583.

[763] *See supra* Part II.I for policy discussion of this requirement.

[764] *See supra* Part II.J.

[765] *See supra* Part II.J.

[766] *See* CAT NMS Plan website frequently asked questions, ''What happens if there is unauthorized access to CAT Data?'' #S.11 at *https://www.catnmsplan.com/faq.*

[767] *See supra* Part II.J.

a de minimis impact on the Plan Processor's operations or on market participants.'' The Commission preliminarily believes that the exception to the breach notification requirement may help to focus the Plan Processor's resources on security issues with more significant impacts. Importantly, even for a breach that the Plan Processor believes to be a de minimis breach, the Plan Processor would be required to document all information relevant to such a breach. This would increase the likelihood that the Plan Processor has all the information necessary should its initial determination that a breach is de minimis prove to be incorrect, so that it could promptly provide breach notifications as required. In addition, maintaining documentation for all breaches, including de minimis breaches, would be helpful in identifying patterns among systems or data breaches. While the Commission preliminarily believes that these limitations on the breach notification requirement may slightly limit the benefits of breach notification in the wake of a breach, it preliminarily believes these modifications may reduce the potential impact of a breach in the case of the delay notification provision because it would facilitate accurate later notification if deemed necessary.

The Commission preliminarily believes that requiring breach management policies and procedures and the cyber incident response plan to incorporate new elements required by the proposed amendments would result in a one-time labor cost of $49,800 [768] for the Plan Processor.[769] Further, the Commission estimates that the Plan Processor will incur an ongoing labor cost of $42,200 [770] to maintain, update and enforce these policies and procedures and the cyber incident response plan. The Commission believes that the Participants would incur initial labor costs of $9,500 [771] for review and approval of the updated cyber incident response plan by the Operating Committee.[772]

11. Firm Designated ID and Allocation Reports

Prior to approval of the CAT NMS Plan, the Commission granted exemptive relief related to allocations of orders, which relieved the Participants from the requirement to link allocations to orders and allowed the usage of ''Allocation Reports.'' [773] This exemptive relief is conditioned on, among other things, the Central Repository having the ability to use information provided in Allocation Reports to link the subaccount holder to those with authority to trade on behalf of the account. However, the CAT NMS Plan as approved does not currently explicitly require Customer and Account Attributes be reported for Firm Designated IDs that are submitted in Allocation Reports, as it does for Firm Designed IDs that are submitted in connection with the original receipt or origination of an order.[774]

The proposed amendments would require that Customer and Account Attributes must be reported for Firm Designated IDs submitted in connection with Allocation Reports, and not just for Firm Designated IDs submitted in connection with the original receipt or origination of an order.[775] The Commission preliminarily believes that these provisions of the proposed amendments are unlikely to have significant economic benefits and costs because implementation of the exemptive relief is already underway and thus its benefits and costs are included in the baseline.

B. Impact on Efficiency, Competition, and Capital Formation

The Commission preliminarily believes that the proposed amendments are likely to have effects on efficiency and competition, with minimal if any effects on capital formation. The Commission anticipates moderate mixed effects on efficiency due to negative effects on the efficiency with which Participants perform their regulatory tasks but positive effects on the efficiency by which the CAT NMS Plan is implemented by Participants by standardizing policies and procedures across Participants and improving efficiencies in how Participants perform some regulatory activities. The Commission preliminarily believes that the proposed amendments will have minor mixed effects on competition. In the case of the market for regulatory services, the Commission preliminarily believes that competition may increase due to additional Participants seeking out RSAs if the amendments are adopted. In the case of the market to serve as Plan Processor, the Commission preliminarily believes the proposed amendments may serve to increase the switching costs Participants would face in replacing the Plan Processor, thus reducing competition in this market. The Commission preliminarily believes that the proposed amendments would not significantly affect capital formation.

1. Baseline for Efficiency, Competition and Capital Formation in the Market for Regulatory Services

There are currently nine Participant Groups.[776] The 24 national securities exchanges are each Plan Participants. The exchanges are currently controlled by eight separate entities and thus comprise eight Participant Groups; four of these operate a single exchange.[777] The sole national securities association, FINRA, is also a CAT NMS Plan Participant and comprises its own Participant Group.

Participants compete in the market for regulatory services. These services include conducting market surveillance, cross-market surveillance, oversight, compliance, investigation, and enforcement, as well as the registration, testing, and examination of broker-dealers. Although the Commission oversees exchange Participants' supervision of trading on their respective venues, the responsibility for direct supervision of trading on an exchange resides in the Participant that operates the exchange. Currently, Participants compete to provide regulatory services in at least two ways.

First, because Participants are responsible for regulating trading within venues they operate, their regulatory services are bundled with their operation of the venue. Consequently, for a broker-dealer, selecting a trading venue also entails the selection of a provider of regulatory services surrounding the trading activity.

Second, Participants could provide this supervision not only for their own venues, but for other Participants' venues as well through the use of RSAs

[768] *See supra* note 585.

[769] *See supra* Part III.D.9.

[770] *See supra* note 588.

[771] Labor costs include one hour per Participant of Vice President of Operations labor. Hourly rate estimated by using the median annual salary from *www.payscale.com,* multiply by 5.35 to account for other compensation, benefits and overhead and adjusting for 1800 hours of labor per year. (($128,159 × 5.35/1800 = $381/hour). (25 hours × $381/hour) = $9,525.

[772] *Id.*

[773] *See supra* Part II.K.

[774] *See* CAT NMS Plan, *supra* note 3, at Section 6.5(d)(ii)(C). However while the CAT NMS Plan does require such information for Firm Designated IDs that are submitted in Allocation Reports, it is required in a separate provision, Section 6.5(d)(iv). *See supra* Part II.K.

[775] *See supra* Part II.K.

[776] *See supra* note 611.

[777] Cboe Global Markets, Inc. controls BYX, BZX, C2, EDGA, EDGX, and Cboe; Miami Internal Holdings, Inc. controls Miami International, MIAX Emerald, and MIAX PEARL; Nasdaq, Inc. controls BX, GEMX, ISE, MRX, PHLX, and Nasdaq; Intercontinental Exchange, Inc. controls NYSE, Arca, American, Chicago, and National. The four entities that control a single-exchange are IEX Group which controls IEX, a consortium of broker-dealers which controls BOX, Long Term Stock Exchange, Inc. which controls LTSE, and MEMX Holdings LLC, which controls MEMX LLC.

or a plan approved pursuant to Rule 17d–2 under the Exchange Act.

Consequently, Participants compete to provide regulatory services to venues they do not operate. Because providing trading supervision is characterized by high fixed costs (such as significant IT infrastructure and specialized personnel), some Participants could find that another Participant could provide some regulatory services more efficiently or at a lower cost than they would incur to provide this service in-house. Currently, nearly all the Participants that operate equity and option exchanges contract with FINRA for some or much of their trading surveillance and routine inspections of members' activity. FINRA provides nearly 100% of the cross-market surveillance for equity markets. Within options markets, through RSAs FINRA provides approximately 50% of cross-market surveillance. As a result, the market for regulatory services in the equity and options markets currently has one dominant competitor: FINRA. This may provide relatively uniform levels of surveillance across trading venues.

As discussed in the CAT NMS Plan Approval Order,[778] as exchanges provide data to the Central Repository to comply with requirements of the Plan, it will become less costly from an operational standpoint for Participants to contract with other Participants to conduct both within market and cross-market surveillance of members because data will already be centralized and uniform due to Plan requirements.

2. Efficiency

The Commission preliminarily believes that the proposed amendments will have moderate and mixed effects on efficiency. The Commission preliminarily believes that improvements to CAT Data security from the proposed amendments may improve efficiency by reducing the likelihood of a CAT Data breach. To the extent that the likelihood of a data breach is reduced, the Commission preliminarily believes that taking measures that may prevent a data breach is inherently more efficient than remediating the consequences of a data breach after it has occurred. The Commission preliminarily believes that provisions of the proposed amendments that require the creation and use of SAWs and set forth requirements that will apply to such workspaces may have negative effects on the efficiency with which Participants perform their regulatory tasks. To the extent that participants implement the current CAT NMS Plan in a manner that is efficient for them individually, provisions increasing uniformity may reduce efficiency by requiring some Participants to abandon decisions that were efficient for them in favor of a potentially less efficient mandated alternative. Finally, the Commission preliminarily believes that the relatively more standardized SAW environments may also enable efficiencies in how Participants perform regulatory activities by facilitating commercial opportunities to license tools between Participants.

The Commission preliminarily believes that improvements to CAT Data security from the proposed amendments may improve efficiency by reducing the likelihood of a CAT Data breach. Because the costs of a data breach are potentially high and would be borne primarily by investors and CAT Data reporters and because the economic impact of a significant data breach is likely to exceed the costs of measures in the proposed amendments that are designed to prevent such a data breach, the Commission preliminarily believes that to the extent that the likelihood of a data breach is reduced, taking measures that may prevent a data breach is inherently more efficient than remediating the consequences of a data breach after it occurred.

The Commission preliminarily believes that provisions of the proposed amendments that require the creation and use of SAWs and set forth requirements that will apply to such workspaces are likely to have negative effects on the efficiency with which Participants perform their regulatory tasks. The CAT NMS Plan as it currently stands does not include provisions for the manner in which Participants access and work with CAT Data beyond the security provisions discussed previously.[779] Currently, Participants discharge their regulatory duties through a number of approaches, with some Participants performing those duties in their private analytic workspaces while others outsource many of their regulatory duties, particularly those requiring data that is not collected by their normal operations, to other Participants through the use of RSAs or under a plan approved pursuant to Rule 17d–2 under the Exchange Act.[780] The Commission believes this diversity of approaches represents strategic choices on the part of Participants.

Rule 613 requires that Participants update their surveillance and oversight activities to make use of CAT Data that will be made available through the Plan.[781] Planned approaches for incorporating CAT Data into regulatory activities that may currently be optimal for a Participant, such as performing most of its regulatory duties in-house, may become more difficult for Participants. For example, a Participant's regulatory staff may be proficient in technical infrastructure that may not be available or might be less efficient in the SAWs. Consequently, adapting to the requirements of the proposed amendments may reduce the efficiency with which a Participant can discharge its regulatory duties with staff and infrastructure already in place.

Further, working within the SAW may be less efficient than alternative environments Participants might have selected to access and analyze CAT Data. The proposed amendments impose some uniformity across SAWs and the Commission preliminarily believes that this uniformity reduces the flexibility of design options for Participants in designing their analytic environments, which may result in more costly or less efficient solutions.[782] The Commission preliminarily believes that these reductions in efficiency are partially mitigated by provisions in the proposed amendments that provide for exceptions to the SAW use requirement although it recognizes that exercising these provisions is also costly to Participants.[783]

In addition, the Commission preliminarily believes that provisions of the proposed amendments that require regulators to secure Commission approval before exercising programmatic access to the Customer Information Subsystems will impose costs [784] upon regulators. These provisions are likely to delay regulators' access to such data as well, further reducing the efficiency with which regulators perform duties that rely upon programmatic access of Customer Identifying Systems.

While the Commission recognizes that provisions of the proposed amendments that reduce the options Participants have (for example, by requiring use of a SAW or an Exempted Environment)

[778] *See* CAT NMS Plan Approval Order, *supra* note 3, at Part IV.G.1.c.

[779] *See supra* Part IV.B.1.

[780] *See supra* Part IV.D.1.

[781] *See* discussion of the adoption of Rule 613(a)(3)(iv), 77 FR 45788 (Aug. 1, 2012), available at: *https://www.govinfo.gov/content/pkg/FR-2012-08-01/pdf/2012-17918.pdf.*

[782] *See supra* Part IV.A.

[783] *See supra* Part IV.D.

[784] *See supra* Part IV.A.6.

are likely to impact how regulators perform their regulatory duties, the Commission preliminarily believes security improvements to CAT Data may partially mitigate these inefficiencies. The proposed amendments are intended to reduce the likelihood of a CAT Data breach. To the extent that security in environments from which Participants access and analyze CAT Data is improved, the likelihood that investors and CAT Data reporters are harmed by a data breach and the likelihood that Participants will need to address the consequences of a data breach, are likely to be reduced. While Participants are likely to see reductions in the efficiency with which they perform their regulatory duties, investors and CAT Data reporters, the parties likely to experience the greatest harm in the event of a data breach, directly benefit from improvements to security from the proposed amendments.

The Commission preliminarily believes other provisions of the proposed amendments are likely to increase efficiency. The Commission preliminarily believes that standardizing implementation of security protocols through the common detailed design specifications may be more efficient than having each Participant that implements a SAW or Excepted Environment for CAT Data because it avoids duplication of effort. This may also improve efficiency by reducing the complexity of security monitoring of environments from which CAT Data is accessed and analyzed.

The Commission preliminarily believes that the relatively more standardized SAW environments may also lead to efficiencies in how Participants perform regulatory activities. To the extent that Participants will be working in similar environments on similar regulatory tasks, tools developed to facilitate one Participant's activities in the SAW may be potentially useful to others. This may facilitate commercial opportunities to license tools between Participants, possibly improving efficiency to the extent that licensing agreements are less costly than development activities. Such tools may also be superior to those developed by a Participant in isolation because there may be opportunities over time for common tools to be updated to reflect evolving best practices.

3. Competition

The Commission preliminarily believes that the proposed amendments will have minor mixed effects on competition. In the case of the market for regulatory services, the Commission preliminarily believes that competition may increase due to additional Participants seeking out RSAs if the amendments are adopted.

In the CAT NMS Plan Approval Order, the Commission discussed potential changes to competition in the market for regulatory services.[785] The Commission preliminarily believes that the proposed amendments could further increase competition in the market of regulatory services because the proposed amendments' provisions requiring the creation and use of SAWs and limiting access to Customer Identifying Systems to SAWs may incentivize other Participants to enter such agreements as providers of regulatory services or as customers of other Participants that provide such services. Participants are likely to face additional operational challenges in performing regulatory duties using CAT Data because of the proposed amendments, particularly in the case of a Participant that elects to work in an Exempted Environment and thus cannot access Customer Identifying Systems from their primary analytic environment without also maintaining a SAW. Consequently, it is possible some Participants that otherwise would have performed some of these duties in house may instead choose to outsource. An increase in the market for these services may incentivize Participants to enter into or increase their competition within this market as providers of regulatory services.

4. Capital Formation

Because the proposed amendments concern the security of data used by regulators to reconstruct market events, monitor market behavior, and investigate misconduct, the Commission preliminarily does not anticipate that the proposed rules would encourage or discourage assets being invested in the capital markets and thus do not expect the rules will significantly affect capital formation.

C. Alternatives

1. Private Contracting for Analytic Environments

The Commission considered an alternative wherein the Participants would be required to work in analytic environments that would be provided by individual Participants, instead of SAWs provided by the Plan Processor, unless they sought exceptions so they could work in Excepted Environments. This alternative approach would differ from the baseline by requiring Participants to obtain an exception if they did not choose to work within the analytic environments currently being developed by the Plan Processor.

Under the alternative approach, security monitoring of the analytic environments might be less uniform. Responsibility for the implementation of security controls and monitoring compliance of those controls would reside with the Participant that provided the analytic environment.[786] This would be likely to result in the security of some implementations being greater than others, for example if security monitoring in some analytic environments occurred more frequently than in others. This could result in some implementations being less secure than they would be under the proposed approach where the Plan Processor is responsible for security monitoring in the SAWs and has more involvement in the configuration of the SAWs.[787] The Commission recognizes that this variability could also lead to some analytic environments being more secure than they would be under the proposed approach.

The Commission also preliminarily believes that the alternative approach might be less efficient than the proposed approach. Under the alternative, each Participant would need to configure its analytic environment and develop security protocols within its analytic environment. Under the current proposal, some of these tasks would be performed by the Plan Processor.[788] This duplication of effort across Participants may be inefficient.

The Commission preliminarily believes that the alternative approach may also be more costly to Participants. Cloud computing resources exhibit volume pricing discounts. Under the proposed approach, the Plan Processor would presumably contract for all the cloud computing resources required by the Participants collectively. This may reduce not only recurring operating costs for the SAWs, but implementation costs including costs incurred to contract with the cloud services provider. The Commission cannot determine if the Plan Processor would share any savings that result with individual Participants that contracted for SAWs through the Plan Processor, but the potential for favorable pricing exists.

[785] *See* CAT NMS Plan Approval Order, *supra* note 3, at Part V.G.1.c.

[786] *See supra* Part IV.B.2.

[787] To the extent that a bad actor would focus an incursion attempt upon the least secure environment, reducing variability between environments may improve CAT Data security by reducing vulnerabilities within environments from where CAT Data is accessed and analyzed.

[788] *See supra* Part II.C.

2. Not Allowing for Exceptions to the SAW Use Requirement

The Commission considered an alternative approach that would not provide an exception process to the requirement that Participants use SAWs when employing the UDDQ and bulk extract tools to access and analyze CAT Data. Under the alternative approach, each Participant would use a SAW provided by the Plan Processor to perform its regulatory duties with CAT Data.

The Commission preliminarily believes that under the alternative approach, there would necessarily be less variability in the security of environments from which CAT Data is accessed and analyzed. To the extent that variation results in some environments being more secure than others, the proposed approach could potentially lead to the existence of relatively weaker security controls within some environments. On the other hand, it is not necessarily true that Excepted Environments would have weaker security than SAWs because an Excepted Environment could have security controls that exceed those within SAWs. However, the Commission recognizes that under the alternative approach, variability between environments that access and analyze CAT Data is likely to be minimized because security controls for all SAWs would be configured by the Plan Processor.

The alternative approach prevents participants from seeking exceptions to the requirement that CAT data be analyzed in a SAW, which may be suboptimal for some participants because they have alternative analytic environments and in which they plan to access and analyze CAT Data. The Commission preliminarily believes that under this alternative approach, Participants may achieve or maintain the security standards required by the CAT NMS Plan less efficiently than they might under the proposed amendments because Participants have significant investments in private analytic environments and regulatory tools that could not be used in the absence of an exception process.[789]

3. Alternative Download Size Limits for the Online Targeted Query Tool

The Commission considered alternative download size limits for the OTQT. Under the proposed approach, downloads through the OTQT are limited to extracting no more than 200,000 records per query result.[790] Under the alternative approach, downloads through the OTQT would be limited to a different number of maximum records.

The Commission preliminarily believes that increasing the proposed download size limit such that more records could be downloaded through a single OTQT query might reduce inefficiencies that may result from the 200,000 record download limit.[791] However, increasing this limit would also allow more CAT Data to be extracted from CAT, increasing the attack surface of CAT.

The Commission preliminarily believes that decreasing the download size limit such that fewer records could be downloaded through a single OTQT query might potentially increase inefficiencies that may result from the 200,000 download limit. However, decreasing this limit would also allow less CAT Data to be extracted through OTQT, decreasing the attack surface of CAT.

4. Allowing Access to Customer Identifying Systems From Excepted Environments

The Commission considered an alternative approach where Participants would be able to access data in Customer Identifying Systems from Excepted Environments. Under the proposed approach, access to Customer Identifying Systems is only available through SAWs.

The Commission preliminarily believes that the alternative approach might reduce inefficiencies that Participants working within Excepted Environments are likely to experience under the proposed amendments. It is possible that under the proposal, some Participants may seek exceptions to work within Excepted Environments and may have no need of a SAW outside of their need to access data within the CAIS. The proposed restriction on Customer Identifying Systems access from SAWs may reduce efficiency by forcing some Participants to maintain a minimal SAW that they do not use other than to access Customer Identifying Systems, or cause them to enter into 17d–2s or RSAs in order to satisfy those regulatory duties they cannot otherwise perform in their Excepted Environments. The Commission preliminarily believes that the alternative approach may provide less security for sensitive customer and account information contained in Customer Identifying Systems. As discussed previously, Customer and Account Attribute data is among the most sensitive data in CAT.[792] To the extent that Excepted Environments increase the variability of security across environments that access and analyze CAT Data,[793] restricting Customer Identifying Systems access to within SAWs provides more uniform security across environments accessing this data and thus may improve its security to the extent that one or more Excepted Environments exist that are not as secure as SAWs.

D. Request for Comment on the Economic Analysis

The Commission is sensitive to the potential economic effects, including the costs and benefits, of the proposed amendments to the CAT NMS Plan. The Commission has identified above certain costs and benefits associated with the proposal and requests comment on all aspects of its preliminary economic analysis. The Commission encourages commenters to identify, discuss, analyze, and supply relevant data, information, or statistics regarding any such costs or benefits. In particular, the Commission seeks comment on the following:

179. Please explain whether you believe the Commission's analysis of the potential effects of the proposed amendments to the CAT NMS Plan is reasonable.

180. The Commission preliminarily believes that the proposed amendments may improve the efficiency of CAT implementation by explicitly defining the scope of the information security program required by the CAT NMS Plan. Do you agree? Are there other economic effects of defining the scope of the information security program that the Commission should consider?

181. Please explain if you agree or disagree with the Commission's assessment of the benefits of the proposed amendments. Are there additional benefits that the Commission should consider?

182. Do you believe the Commission's cost estimates are reasonable? If not, please provide alternative estimates where possible. Are there additional costs that the Commission should consider?

183. Please explain whether you agree with the Commission's assessment of potential conflicts of interests involving the Security Working Group. Are there further conflicts of interest that the Commission should consider? Are there factors that the Commission has not considered that may further mitigate

[789] *See supra* Part IV.A.3.c.

[790] *See supra* Part II.D.

[791] *See supra* Part IV.A.4.

[792] *See supra* Part II.C.2.

[793] *See supra* Part IV.C.2.

potential conflicts of interest involving the Security Working Group?

184. In its calculations of cost estimates, the Commission assumes that the hourly labor rate for the CISO is equivalent to that of a Chief Compliance Officer. Do you agree with this assumption? If not, please provide an alternative estimate if possible.

185. In its calculation of cost estimates, the Commission assumes that the hourly rate of a Chief Regulatory Officer as 125% of the rate of a Chief Compliance Officer. Do you agree with this assumption? If not, please provide an alternate estimate if possible.

186. In its calculation of cost estimates, the Commission estimates the hourly rate of an Operating Committee member using an adjusted hourly rate for a Vice President of Operations of $381 per hour. Is this estimate reasonable? If not, please provide an alternate estimate if possible.

187. Do you agree or disagree with the Commission's assessment of the benefits of providing for exceptions for the SAW usage requirements? Are there additional benefits of the SAW exception provision that the Commission should consider?

188. The Commission preliminarily believes that each Participant Group will establish a single SAW or Excepted Environment because it preliminarily believes that each Participant Group largely centralizes its regulatory functions that would require CAT Data. Are there reasons why a single Participant Group may wish to have multiple SAWs? Are there reasons some Participant Groups may decide to maintain both a SAW and an Excepted Environment?

189. The Commission preliminarily believes that the proposed amendments' provisions related to the CISP may improve the security of CAT Data because, to the extent that security controls are implemented more uniformly than they would be under the current CAT NMS Plan, they reduce variability in security control implementation. Do you agree? Are there additional economic effects of provisions of the proposed amendments related to the CISP that the Commission should consider?

190. The Commission preliminarily believes that the requirement that the Plan Processor must evaluate and notify the Operating Committee that each Participant's SAW has achieved compliance with the detailed design specifications before that SAW may connect to the Central Repository will further increase uniformity of security control implementations. Do you agree? Are there other economic effects of this provision that the Commission should consider?

191. Do you agree that provisions allowing for exceptions to the SAW usage requirement may allow Participants to achieve or maintain the security standards required by the CAT NMS Plan more efficiently? Are there other economic effects of this provision that the Commission should consider?

192. The proposed amendments require that each Participant using a non-SAW environment simultaneously notify the Plan Processor, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group of any material changes to its security controls for the non-SAW environment. How often would a Participant Group make changes to its Excepted Environment that would necessitate material changes to its security controls?

193. The proposed amendments require that Participants would need to implement processes in Excepted Environments to enable Plan Processor security monitoring. The Commission preliminarily believes that development costs for the processes that produce log files that support Plan Processor monitoring would require similar development activities to developing the automated monitoring processes themselves. Do you agree? Please provide alternate estimates of the costs of these development activities if possible.

194. The Commission believes that by limiting the number of records of CAT Data that can be extracted through the OTQT will increase security by limiting the data that is accessed outside of secure environments. Do you agree? Are there other economic effects of limiting the number of records that can be extracted through the OTQT that the Commission should consider?

195. The Commission preliminarily believes that limiting the number of records of CAT Data that can be extracted through the OTQT this may reduce the regulatory use of CAT Data. Do you agree with this assessment? Are there additional indirect costs to regulators from this provision that the Commission should consider?

196. The Commission preliminarily believes that requiring the Plan Processor to evaluate and validate each Participant's SAW before that SAW may connect to the Central Repository will further increase uniformity of security control implementations. Do you agree? Are there other economic effects of requiring the Plan Processor to perform this evaluation and validation that the Commission should consider?

197. The Commission preliminarily believes that standardizing implementation of security protocols through the common detailed design specifications may be more efficient than having each Participant that implements a SAW or private environment for CAT Data do so independently because it avoids duplication of effort. Do you agree? Are there other economic effects of these provisions that the Commission should consider?

198. The Commission preliminarily believes that the requirement that customer addresses be reported to CAIS with separate fields for street number and street name is likely to have a de minimis economic impact upon both Participants and CAT Reporters. Do you agree? If possible, please provide cost estimates for providing this information in separate fields.

199. Do you agree with the Commission's cost estimates for the Plan Processor to establish programmatic access to the Customer Identifying Systems? Please provide alternative estimates if possible. Are there additional direct or indirect costs to providing this programmatic access that the Commission should consider?

200. Do you agree that placing restrictions on access to Customer Identifying Systems to Regulatory Staff will reduce the risk of inappropriate use of customer and account information? Are there additional economic effects of these restrictions that the Commission should consider?

201. Do you agree with the Commission's analysis of the economic effects of provisions of the proposed amendments that prohibit any use of CAT Data that has both regulatory and commercial uses? Are there additional economic effects of these provisions that the Commission should consider?

202. The proposed amendments would require the Participants to periodically review the effectiveness of the Proposed Confidentiality Policies and take prompt action to remedy deficiencies in such policies. The Commission preliminarily estimates that this review would require approximately 20% of the labor of the initial effort to jointly draft those policies because presumably many of the policies would not need revision with each review. Do you agree? Please provide alternative cost estimates if possible.

203. The Commission preliminarily believes that providing an exception allowing non-regulatory staff to access CAT data in certain circumstances may help avoid inefficiencies where a Participant's response to a market event

is slowed due to prohibitions on staff other than Regulatory Staff having access to CAT Data. Do you agree? Are there additional economic effects of providing this exception that the Commission should consider?

204. The Commission preliminarily believes the risk that CAT data will be misused by allowing non-regulatory staff to use the data in certain circumstances is mitigated by the requirement that the Participant's Chief Regulatory Officer provide written permission for such access. Do you agree? Are there additional security risks or economic effects of these provisions that the Commission should consider?

205. The Commission preliminarily believes that the Plan Processor has transactional test data available for its staff and contractors to use for development activities. Do you agree? If not, please provide an estimate of the costs the Plan Processor would incur to create such test data.

206. The Commission believes that the ability to amend the plan in the future mitigates the concern that participants may be prevented in the future from using more secure methods to connect to CAT that have yet to be developed. Do you agree? Are there other indirect costs of these provisions that the Commission should consider?

207. The Commission preliminarily believes that the proposed amendments are likely to have moderate mixed effects on efficiency. Do you agree? Are there other effects of the proposed amendments on efficiency that the Commission should consider?

208. The Commission preliminarily believes that the proposed amendments are likely to have minor mixed effects on competition. Do you agree? Are there other effects of the proposed amendments on competition that the Commission should consider?

209. The Commission preliminarily believes that the proposed amendments' effects on capital formation likely won't be significant. Do you agree? Are there other effects of the proposed amendments on capital formation that the Commission should consider?

210. Do you believe that provisions of the proposed amendments that require the creation and use of SAWs and set forth requirements that will apply to such workspaces may have negative effects on the efficiency with which Participants perform their regulatory tasks? Are there other economic effects of these provisions that the Commission should consider?

211. The Commission preliminarily believes that the relatively more standardized SAW environments may also enable efficiencies in how Participants perform regulatory activities by facilitating commercial opportunities to license tools between Participants. Do you agree? Are there other economic effects of these provisions that the Commission should consider?

212. The Commission preliminarily believes that provisions of the proposed amendments that require the creation and use of SAWs and set forth requirements that will apply to such workspaces are likely to have negative effects on the efficiency with which Participants perform their regulatory tasks. Do you agree? Are there other economic effects on how Participants perform their regulatory tasks that the Commission should consider?

213. The Commission preliminarily believes that the uniformity across SAWs imposed by the plan reduces the flexibility of design options for Participants potentially resulting in in more costly and/or less efficient solutions. Do you agree with this assessment? In what manner could the flexibility of design options available to Participants be affected by the proposed amendments?

214. Do you agree that the potential reductions in efficiency due to the imposed uniformity across SAWs are partially mitigated by provisions in the proposed amendments that providing for exceptions to the SAW use requirement?

215. The Commission preliminarily believes that the proposed amendments could further increase competition in the market of regulatory services because the proposed amendments' provision requiring the creation and use of secure analytical workspaces may incentivize other Participants to enter such agreements as providers of regulatory services or as customers of other Participants that provide such services. Are there likely to be additional economic effects on how Participants provide and use 17d–2 and RSA agreements?

216. Do you believe that the alternative approach of private contracting for analytic environments would likely lead to some implementations to be less secure than they would be under the proposed approach? Are there additional economic effects of the alternative approach that the Commission should consider?

217. Do you agree with the Commission's analysis of the alternative approach of not allowing exceptions to the SAW use requirement? Are there additional economic effects of the alternative approach that the Commission should consider?

218. The proposed amendments would limit downloads through the OTQT to 200,000 records. Would an alternative limit to download size have security or efficiency benefits?

219. Do you agree with the Commission's analysis of the alternative approach of allowing access to CAIS from Exempted Environments? Are there additional economic effects of the alternative approach that the Commission should consider?

V. Consideration of Impact on the Economy

For purposes of the Small Business Regulatory Enforcement Fairness Act of 1996 (''SBREFA''),[794] the Commission requests comment on the potential effect of this proposal on the United States economy on an annual basis. The Commission also requests comment on any potential increases in costs or prices for consumers or individual industries, and any potential effect on competition, investment, or innovation. Commenters are requested to provide empirical data and other factual support for their views, to the extent possible.

VI. Regulatory Flexibility Act Certification

The Regulatory Flexibility Act (''RFA'') [795] requires Federal agencies, in promulgating rules, to consider the impact of those rules on small entities. Section 603(a) [796] of the Administrative Procedure Act,[797] as amended by the RFA, generally requires the Commission to undertake a regulatory flexibility analysis of all proposed rules, or proposed rule amendments, to determine the impact of such rulemaking on ''small entities.'' [798] Section 605(b) of the RFA states that this requirement shall not apply ''to any proposed or final rule if the head of the agency certifies that the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities.'' [799]

The proposed amendments to the CAT NMS Plan would only impose requirements on national securities

[794] Public Law 104–121, Title II, 110 Stat. 857 (1996) (codified in various sections of 5 U.S.C., 15 U.S.C. and as a note to 5 U.S.C. 601).

[795] 5 U.S.C. 601 *et seq.*

[796] 5 U.S.C. 603(a).

[797] 5 U.S.C. 551 *et seq.*

[798] The Commission has adopted definitions for the term ''small entity'' for purposes of Commission rulemaking in accordance with the RFA. Those definitions, as relevant to this proposed rulemaking, are set forth in 17 CFR 240.0–10. *See* Securities Exchange Act Release No. 18451 (January 28, 1982), 47 FR 5215 (February 4, 1982) (File No. AS–305).

[799] 5 U.S.C. 605(b).

exchanges registered with the Commission under Section 6 of the Exchange Act and FINRA. With respect to the national securities exchanges, the Commission's definition of a small entity is an exchange that has been exempt from the reporting requirements of Rule 601 of Regulation NMS, and is not affiliated with any person (other than a natural person) that is not a small business or small organization.[800] None of the national securities exchanges registered under Section 6 of the Exchange Act that would be subject to the proposed amendments are ''small entities'' for purposes of the RFA. In addition, FINRA is not a ''small entity.'' [801] For these reasons, the proposed rule will not apply to any ''small entities.'' Therefore, for the purposes of the RFA, the Commission certifies that the proposed amendments would not have a significant economic impact on a substantial number of small entities.

The Commission requests comment regarding this certification. In particular, the Commission solicits comment on the following:

220. Do commenters agree with the Commission's certification that the proposed amendments would not have a significant economic impact on a substantial number of small entities? If not, please describe the nature of any impact on small entities and provide empirical data to illustrate the extent of the impact.

VI. Statutory Authority and Text of the Proposed Amendments to the CAT NMS Plan

Pursuant to the Exchange Act and, particularly, Sections 2, 3(b), 5, 6, 11A(a)(3)(B), 15, 15A, 17(a) and (b), 19 and 23(a) thereof, 15 U.S.C. 78b, 78c(b), 78e, 78f, 78k–1, 78o, 78o–3, 78q(a) and (b), 78s, 78w(a), and pursuant to Rule 608(a)(2) and (b)(2),[802] the Commission proposes to amend the CAT NMS Plan in the manner set forth below.

Additions are *italicized;* deletions are [bracketed].

* * * * *

Section 1.1. Definitions

As used throughout this Agreement (including, for the avoidance of doubt, the Exhibits, Appendices, Attachments, Recitals and Schedules identified in this Agreement):

* * * * *

''[Customer]Account [Information]*Attributes*'' shall include, but not be limited to, [account number,] account type, customer type, date account opened, and large trader identifier (if applicable); except, however, that (a) in those circumstances in which an Industry Member has established a trading relationship with an institution but has not established an account with that institution, the Industry Member will (i) provide the Account Effective Date in lieu of the ''date account opened''[; (ii) provide the relationship identifier in lieu of the ''account number'';] and ([i]ii) identify the ''account type'' as a ''relationship''; (b) in those circumstances in which the relevant account was established prior to the implementation date of the CAT NMS Plan applicable to the relevant CAT Reporter (as set forth in Rule 613(a)(3)(v) and (vi)), and no ''date account opened'' is available for the account, the Industry Member will provide the Account Effective Date in the following circumstances: (i) Where an Industry Member changes back office providers or clearing firms and the date account opened is changed to the date the account was opened on the new back office/clearing firm system; (ii) where an Industry Member acquires another Industry Member and the date account opened is changed to the date the account was opened on the post-merger back office/clearing firm system; (iii) where there are multiple dates associated with an account in an Industry Member's system, and the parameters of each date are determined by the individual Industry Member; and (iv) where the relevant account is an Industry Member proprietary account.

* * * * *

''*CAIS*'' *refers to the Customer and Account Information System within the CAT System that collects and links Customer-ID(s) to Customer and Account Attributes and other identifiers for queries by Regulatory Staff.*

''*CAIS/CCID Subsystem Regulator Portal*'' *refers to the online tool enabling Manual CAIS access and Manual CCID Subsystem access.*

* * * * *

''*CCID Subsystem*'' *refers to the subsystem within the CAT System which will create the Customer-ID from a Transformed Value(s), as set forth in Section 6.1(v) and Appendix D, Section 9.1.*

''*CCID Transformation Logic*'' *refers to the mathematical logic identified by the Plan Processor that accurately transforms an individual tax payer identification number(s)(ITIN(s))/social security number(s)(SSN(s))/Employer Identification Number (EIN(s)) into a Transformed Value(s) for submission into the CCID Subsystem, as set forth in Appendix D, Section 9.1.*

* * * * *

''*Comprehensive Information Security Program*'' *includes the organization-wide and system-specific controls and related policies and procedures required by NIST SP 800–53 that address information security for the information and information systems that support the operations of the Plan Processor and the CAT System, including those provided or managed by an external organization, contractor, or source, inclusive of Secure Analytical Workspaces.*

* * * * *

''*Customer and Account Attributes*'' *shall mean the data elements in Account Attributes and Customer Attributes.*

* * * * *

''Customer [Identifying Information] *Attributes*'' means information of sufficient detail to identify a Customer, including, but not limited to, (a) with respect to individuals: Name, address, [date] *year* of birth, [individual tax payer identification number (''ITIN'')/social security number (''SSN'')], individual's role in the account (*e.g.,* primary holder, joint holder, guardian, trustee, person with the power of attorney); and (b) with respect to legal entities: Name, address, Employer Identification Number (''EIN''), *and* [/]Legal Entity Identifier (''LEI'') or other comparable common entity identifier, if applicable; provided, however, that an Industry Member that has an LEI for a Customer must submit the Customer's LEI in addition to other information of sufficient detail to identify a Customer.

* * * * *

''*Customer Identifying Systems*'' *means CAIS and the CCID Subsystem.*

* * * * *

''*Customer Identifying Systems Workflow*'' *describes the requirements and process for accessing Customer Identifying Systems as set forth in Appendix D, Data Security.*

* * * * *

''*Manual CAIS Access*'' *when used in connection with the Customer Identifying Systems Workflow, as defined in Appendix D, shall mean the Plan Processor functionality to manually query CAIS, in accordance with Appendix D, Data Security, and the Participants' policies as set forth in Section 6.5(g).*

* * * * *

''*Manual CCID Subsystem Access*'' *when used in connection with the Customer Identifying Systems Workflow, as defined in Appendix D, shall mean the Plan Processor functionality to manually query the CCID Subsystem, in accordance with Appendix D, Data Security, and the Participants' policies as set forth in Section 6.5(g).*

* * * * *

[''PII'' means personally identifiable information, including a social security number or tax identifier number or similar information; Customer Identifying Information and Customer Account Information.]

* * * * *

''*Programmatic CAIS Access*'' *when used in connection with the Customer Identifying Systems Workflow, as defined in Appendix D, shall mean the Plan Processor functionality to programmatically query, and return results that include, data from the CAIS and transactional CAT Data, in support of the regulatory purpose of an inquiry or set of inquiries, in accordance with Appendix D, Data Security, and the Participants' policies as set forth in Section 6.5(g).*

---

[800] *See* 17 CFR 240.0–10(e).

[801] *See* 13 CFR 121.201

[802] 17 CFR 242.608(a)(2) and (b)(2). These provisions enable the Commission to propose amendments to any effective NMS Plan by ''publishing the text thereof, together with a statement of the purpose of such amendment,'' and providing ''interested persons an opportunity to submit written comments.''

''*Programmatic CCID Subsystem Access*'' *when used in connection with the Customer Identifying Systems Workflow, as defined in Appendix D, shall mean the Plan Processor functionality to programmatically query the CCID Subsystem to obtain Customer-ID(s) from Transformed Value(s), in support of the regulatory purpose of an inquiry or set of inquiries, in accordance with Appendix D, Data Security, and the Participants' policies as set forth in Section 6.5(g).*

* * * * *

''*Regulatory Staff*'' *means the Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation) and staff within the Chief Regulatory Officer's (or similarly designated head(s) of regulation's) reporting line. In addition, Regulatory Staff must be specifically identified and approved in writing by the Chief Regulatory Officer (or similarly designated head(s) of regulation).*

* * * * *

''*Secure Analytical Workspace*'' *or* ''*SAW*'' *means an analytic environment account that is part of the CAT System, and subject to the Comprehensive Information Security Program, where CAT Data is accessed and analyzed by Participants pursuant to Section 6.13. The Plan Processor shall provide a SAW account for each Participant that implements all common technical security controls required by the Comprehensive Information Security Program.*

* * * * *

''*Secure File Sharing*'' *means a capability that allows files to be extracted and shared outside of the SAW in a manner consistent with the provisions of Section 6.13(a)(i)(D).*

* * * * *

''*Transformed Value*'' *refers to the value generated by the CCID Transformation Logic, as set forth in Section 6.1(v) and Appendix D, Section 9.1.*

* * * * *

Section 4.12. Subcommittees and Working Groups

* * * * *

(c) The Operating Committee shall establish and maintain a security working group composed of the Chief Information Security Officer, and the chief information security officer or deputy chief information security officer of each Participant (the ''*Security Working Group*''*). Commission observers shall be permitted to attend all meetings of the Security Working Group, and the CISO and the Operating Committee may invite other parties to attend specific meetings. The Security Working Group's purpose shall be to advise the Chief Information Security Officer (who shall directly report to the Operating Committee in accordance with Section 6.2(b)(iii)) and the Operating Committee, including with respect to issues involving:*

(i) Information technology matters that pertain to the development of the CAT System;

(ii) the development, maintenance, and application of the Comprehensive Information Security Program;

(iii) the review and application of the confidentiality policies and procedures required by Section 6.5(g);

(iv) 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

(v) emerging cybersecurity topics.

The Chief Information Security Officer shall apprise the Security Working Group of relevant developments and provide it with all information and materials necessary to fulfill its purpose.

* * * * *

Section 6.1. Plan Processor

* * * * *

(d) The Plan Processor shall:

* * * * *

(v) provide Secure Analytical Workspaces in accordance with Section 6.13.

* * * * *

(v) The Plan Processor shall develop, with the prior approval of the Operating Committee, the functionality to implement the process for creating a Customer-ID(s), consistent with this Section and Appendix D, Section 9.1. With respect to the CCID Subsystem, the Plan Processor shall develop functionality to:

(i) Ingest Transformed Value(s) and any other required information and convert the Transformed Value(s) into an accurate and reliable Customer-ID(s);

(ii) Validate that the conversion from the Transformed Value(s) to the Customer-ID(s) is accurate; and

(iii) Transmit the Customer-ID(s), consistent with Appendix D, Section 9.1, to CAIS or a Participant's SAW.

* * * * *

Section 6.2. Chief Compliance Officer and Chief Information Security Officer

(a) Chief Compliance Officer.

* * * * *

(v) The Chief Compliance Officer shall:

* * * * *

(H) regularly review the *Comprehensive I*[i]nformation *S*[s]ecurity *P*[p]rogram developed and maintained by the Plan Processor pursuant to Section 6.12 and determine the frequency of such reviews;

* * * * *

(Q) oversee the Plan Processor's compliance with applicable laws, rules and regulations related to the CAT system, in its capacity as Plan Processor[.]*;*

(R) in collaboration with the Chief Information Security Officer, review the Participants' policies developed pursuant to Section 6.5(g)(i), and, if the Chief Compliance Officer, in consultation with the Chief Information Security Officer, finds that such policies are inconsistent with the requirements of the Plan, notify the Operating Committee of such deficiencies;

(S) in collaboration with the Chief Information Security Officer, determine, pursuant to Section 6.13(d), whether a Participant should be granted an exception from Section 6.13(a)(i)(B) and, if applicable, whether such exception should be continued; and

(T) as required by Section 6.6(b)(ii)(B)(3), in collaboration with the Chief Information Security Officer, review CAT Data that has been extracted from the CAT System to assess the security risk of allowing such CAT Data to be extracted.

(b) Chief Information Security Officer.

* * * * *

(v) Consistent with Appendices C and D, the Chief Information Security Officer shall be responsible for creating and enforcing appropriate policies, procedures, and control structures to monitor and address data security issues for the Plan Processor and the Central Repository including:

* * * * *

(F) [PII] *Customer and Account Attributes* data requirements, including the standards set forth in Appendix D, [PII Data Requirements] *Customer Identifying Systems Requirements and Customer Identifying Systems Workflow;*

* * * * *

(viii) In collaboration with the Chief Compliance Officer, the Chief Information Security Officer shall review the Participants' policies developed pursuant to Section 6.5(g)(i). If the Chief Information Security Officer, in consultation with the Chief Compliance Officer, finds that such policies are inconsistent with the requirements of the Plan, they will be required to notify the Operating Committee of such deficiencies.

(ix) In collaboration with the Chief Compliance Officer, the Chief Information Security Officer shall determine, pursuant to Section 6.13(d), whether a Participant should be granted an exception from Section 6.13(a)(i)(B) and, if applicable, whether such exception should be continued.

(x) As required by Section 6.6(b)(ii)(B)(3), in collaboration with the Chief Compliance Officer, review CAT Data that has been extracted from the CAT System to assess the security risk of allowing such CAT Data to be extracted.

* * * * *

Section 6.4. Data Reporting and Recording by Industry Members

* * * * *

(d) Required Industry Member Data.

* * * * *

(ii) Subject to Section 6.4(c) and Section 6.4(d)(iii) with respect to Options Market Makers, and consistent with Appendix D, Reporting and Linkage Requirements, and the Technical Specifications, each Participant shall, through its Compliance Rule, require its Industry Members to record and report to the Central Repository the following, as applicable (''Received Industry Member Data'' and collectively with the information referred to in Section 6.4(d)(i) ''Industry Member Data''):

* * * * *

(C) for original receipt or origination of an order *and Allocation Reports,* the Firm Designated ID for the relevant Customer, and in accordance with Section 6.4(d)(iv), Customer *and* Account *Attributes* [Information and Customer Identifying Information] for the relevant Customer[.]*; and*

(D) for all Customers with an ITIN/SSN/EIN, the Transformed Value.

* * * * *

Section 6.5. Central Repository

* * * * *

(b) Retention of Data

* * * * *

(i) Consistent with Appendix D, Data Retention Requirements, the Central Repository shall retain the information collected pursuant to paragraphs (c)(7) and (e)(7) of SEC Rule 613 in a convenient and usable standard electronic data format that is directly available and searchable electronically without any manual intervention by the Plan Processor for a period of not less than six (6) years. Such data when available to the Participant*'s R*[r]egulatory *S*[s]taff and the SEC shall be linked.

* * * * *

(f) Data Confidentiality

(i) The Plan Processor shall, without limiting the obligations imposed on Participants by this Agreement and in accordance with the framework set forth in, Appendix D, Data Security, and Functionality of the CAT System, be responsible for the security and confidentiality of all CAT Data received and reported to the Central Repository. Without limiting the foregoing, the Plan Processor shall:

* * * * *

(C) develop and maintain a *C*[c]omprehensive *I*[i]nformation *S*[s]ecurity *P*[p]rogram with a dedicated staff for the [Central Repository, consistent with Appendix D, Data Security] *CAT System,* that employs state of the art technology, which program will be regularly reviewed by the Chief Compliance Officer and Chief Information Security Officer;

* * * * *

(ii) [Each Participant shall adopt and enforce policies and procedures that:

(A) implement effective information barriers between such Participant's regulatory and non-regulatory staff with regard to access and use of CAT Data stored in the Central Repository;

(B) permit only persons designated by Participants to have access to the CAT Data stored in the Central Repository; and

(C) impose penalties for staff non-compliance with any of its or the Plan Processor's policies or procedures with respect to information security.

(iii) Each Participant shall as promptly as reasonably practicable, and in any event within 24 hours, report to the Chief Compliance Officer, in accordance with the guidance provided by the Operating Committee, any instance of which such Participant becomes aware of: (A) noncompliance with the policies and procedures adopted by such Participant pursuant to Section 6.5(e)(ii); or (B) a breach of the security of the CAT.

(iv)] The Plan Processor shall:

* * * * *

(B) require the establishment of secure controls for data retrieval and query reports by Participants*' R*[r]egulatory *S*[s]taff; and

* * * * *

([v]*iii*) The Company shall endeavor to join the FS–ISAC and comparable bodies as the Operating Committee may determine.

(g) Participants*'* Confidentiality Policies and Procedures.

(i) The Participants shall establish, maintain and enforce *identical* written policies [and procedures] *that apply to each Participant. Each Participant shall establish, maintain and enforce procedures and usage restriction controls in accordance with these policies. The policies must:*

(A) be reasonably designed to (1) ensure the confidentiality of [the]CAT Data[obtained from the Central Repository]; and (2) limit the use of CAT Data *to* [obtained from the Central Repository] solely [for]surveillance and regulatory purposes[.]*;* [Each Participant shall periodically review the effectiveness of the policies and procedures required by this paragraph, and take prompt action to remedy deficiencies in such policies and procedures.]

(B) limit extraction of CAT Data to the minimum amount of data necessary to achieve a specific surveillance or regulatory purpose;

(C) limit access to CAT Data to persons designated by Participants, who must be (1) Regulatory Staff or (2) technology and operations staff that require access solely to facilitate access to and usage of the CAT Data by Regulatory Staff;

(D) implement effective information barriers between such Participants' Regulatory Staff and non-Regulatory Staff with regard to access and use of CAT Data;

(E) limit access to CAT Data by non-Regulatory Staff, by allowing such access only where there is a specific regulatory need for such access and requiring that a Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation), or his or her designee, document his or her written approval of each instance of access by non-Regulatory Staff;

(F) require all Participant staff who are provided access to CAT Data to: (1) sign a ''Safeguard of Information'' affidavit as approved by the Operating Committee pursuant to Section 6.5(f)(i)(B); and (2) participate in the training program developed by the Plan Processor that addresses the security and confidentiality of information accessible in the CAT pursuant to Section 6.1(m), provided that Participant staff may be provided access to CAT Data prior to meeting these requirements in exigent circumstances;

(G) define the individual roles and regulatory activities of specific users;

(H) impose penalties for staff non-compliance with the Participant's or the Plan Processor's policies, procedures, or usage restriction controls with respect to information security, including, the policies required by Section 6.5(g)(i);

(I) be reasonably designed to implement and satisfy the Customer and Account Attributes data requirements of Section 4.1.6 of Appendix D such that Participants must be able to demonstrate that a Participant's ongoing use of Programmatic CAIS and/or CCID Subsystem access is in accordance with the Customer Identifying Systems Workflow; and

(J) document monitoring and testing protocols that will be used to assess Participant compliance with the policies.

(ii) The Participants shall periodically review the effectiveness of the policies and procedures and usage restriction controls required by Section 6.5(g)(i), including by using the monitoring and testing protocols documented within the policies pursuant to Section 6.5(g)(i)(J), and take prompt action to remedy deficiencies in such policies, procedures and usage restriction controls.

(iii) Each Participant shall as promptly as reasonably practicable, and in any event within 24 hours of becoming aware, report to the Chief Compliance Officer, in accordance with the guidance provided by the Operating Committee: (A) any instance of noncompliance with the policies, procedures, and usage restriction controls adopted by such Participant pursuant to Section 6.5(g)(i); or (B) a breach of the security of the CAT.

(iv) The Participants shall make the policies required by Section 6.5(g)(i) publicly available on each of the Participant websites, or collectively on the CAT NMS Plan website, redacted of sensitive proprietary information.

(v) On an annual basis, each Participant shall engage an independent accountant to perform an examination of compliance with the policies required by Section 6.5(g)(i) in accordance with attestation standards of the AICPA (referred to as U.S. Generally Accepted Auditing Standards or GAAS) or the PCAOB, and with Commission independence standards based on SEC Rule 2–01 of Regulation S–X. The independent accountant's examination report shall be submitted to the Commission upon completion, in a text-searchable format (e.g. a text-searchable PDF). The examination report provided for in this paragraph shall be considered submitted with the Commission when electronically received by an email address provided by Commission staff.

(vi) The policies required by Section 6.5(g)(i) are subject to review and approval by the Operating Committee, after such policies are reviewed by the Chief Compliance Officer and Chief Information Security Officer pursuant to Sections 6.2(a)(v)(R) and 6.2(b)(viii).

* * * * *

Section 6.6 [Regular] Written Assessments, Audits and Reports.

* * * * *

(b) Regular Written Assessment of the Plan Processor's Performance.

* * * * *

(ii) Contents of Written Assessment. The annual written assessment required by this Section 6.6 shall include:

* * * * *

(B) a detailed plan, based on the evaluation conducted pursuant to Section 6.6(b)(i), for any potential improvements to the performance of the CAT with respect to the items specified in SEC Rule 613(b)(6)(ii), as well as:

* * * * *

(3) an evaluation of the *Comprehensive I*[i[nformation *S*[s]ecurity *P*[p]rogram to ensure that the program is consistent with the highest industry standards for the protection of data[;], *as part of which, the CCO, in collaboration with the CISO, shall review 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;

* * * * *

Section 6.10 Surveillance

* * * * *

(c) Use of CAT Data by Regulators.

* * * * *

(ii) Extraction of CAT Data shall be consistent with all permission rights granted by the Plan Processor. All CAT Data returned shall be encrypted, and [PII] *Customer and Account Attributes* data shall be [masked]*unavailable* unless users have permission to view the CAT Data that has been requested.

* * * * *

Section 6.12. Comprehensive Information Security Program

The Plan Processor shall develop and maintain the *C*[c]omprehensive *I*[i]nformation *S*[s]ecurity *P*[p]rogram [for the Central Repository], to be approved and reviewed at least annually by the Operating Committee, and which contains at a minimum the specific requirements detailed in Appendix D, Data Security *and Section 6.13.*

* * * * *

Section 6.13. Secure Analytical Environments

(a) SAW Environments. The Comprehensive Information Security Program shall apply to every Participant's SAW and must, at a minimum:

(i) Establish data access and extraction policies and procedures that include the following requirements:

(A) Participants shall use SAWs as the only means of accessing and analyzing Customer and Account Attributes.

(B) Participants shall use SAWs when accessing and analyzing CAT Data through the user-defined direct query and bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2, unless receiving an exception as set forth in Section 6.13(d).

(C) Participants shall only extract from SAWs the minimum amount of CAT Data necessary to achieve a specific surveillance or regulatory purpose.

(D) Secure file sharing capability provided by the Plan Processor shall be the only mechanism for extracting CAT Data from SAWs.

(ii) Establish security controls, policies, and procedures for SAWs that require all NIST SP 800–53 security controls and associated policies and procedures required by the Comprehensive Information Security Program to apply to the SAWs, provided that:

(A) For the following NIST SP 800–53 control families, at a minimum, security controls, policies, and procedures, shall be applied by the Plan Processor and shall be common to both the SAWs and the Central Repository in accordance with Section 2.4 of NIST SP 800–53, unless technologically or organizationally not possible: audit and accountability, security assessment and authorization, configuration management, incident response, system and communications protection, and system and information integrity; and

(B) SAW-specific security controls, policies, and procedures shall be implemented to cover any remaining NIST SP 800–53 security controls for which common security controls, policies, and procedures are not possible.

(b) Detailed Design Specifications.

(i) The Plan Processor shall develop, maintain, and make available to the Participants detailed design specifications for the technical implementation of the access, monitoring, and other controls required for SAWs by the Comprehensive Information Security Program controls.

(ii) The Plan Processor shall notify the Operating Committee that each Participant's SAW has achieved compliance with the detailed design specifications before that SAW may connect to the Central Repository.

(c) SAW Operations.

(i) In accordance with the detailed design specifications developed pursuant to Section 6.13(b)(i), the Plan Processor shall monitor each Participant's SAW, for compliance with the Comprehensive Information Security Program and the detailed design specifications developed pursuant to Section 6.13(b)(i) only, and notify the Participant of any identified non-compliance with the Comprehensive Information Security Program or with the detailed design specifications developed pursuant to Section 6.13(b)(i).

(ii) Participants shall comply with the Comprehensive Information Security Program, comply with the detailed design specifications developed pursuant to Section 6.13(b)(i), and promptly remediate any identified non-compliance.

(iii) Each Participant may provide and use its choice of software, hardware configurations, and additional data within its SAW, so long as such activities comply with the Comprehensive Information Security Program.

(d) Non-SAW Environments.

(i) A Participant may seek an exception from the requirements of Section 6.13(a)(i)(B). If such exception is granted, the Participant may employ the user-defined direct query or bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2 in a non-SAW environment.

(A) To seek an exception from Section 6.13(a)(i)(B), the requesting Participant shall provide the Chief Information Security Officer, the Chief Compliance Officer, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group with:

(1) A security assessment of the non-SAW environment, conducted within the last twelve (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 Comprehensive Information Security Program pursuant to Section 6.13(a)(ii), (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; and

(2) 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).

(B) Within 60 days of receipt of the materials described in Section 6.13(d)(i)(A), the Chief Information Security Officer and the Chief Compliance Officer must simultaneously notify the Operating Committee and the requesting Participant of their determination.

(1) The Chief Information Security Officer and the Chief Compliance Officer may jointly grant an exception if they 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 pursuant to Section 6.13(d)(i)(A) 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. If an exception is granted, the Chief Information Security Officer and the Chief Compliance Officer shall provide the requesting Participant with a detailed written explanation setting forth the reasons for that determination.

(2) If the Chief Information Security Officer and the Chief Compliance Officer decide not to grant an exception to the requesting Participant, they must provide the Participant with a detailed written explanation setting forth the reasons for that determination and specifically identifying the deficiencies that must be remedied before an exception could be granted.

(C) If a request for an exception from Section 6.13(a)(i)(B) is denied, the requesting Participant may attempt to re-apply, after remedying the deficiencies identified by the Chief Information Security Officer and the Chief Compliance Officer, by submitting a new security assessment that complies with the requirements of Section 6.13(d)(i)(A)(1) and up-to-date versions of the materials specified in Section 6.13(d)(i)(A)(2).

(ii) Continuance of any exception granted pursuant to Section 6.13(d)(i) is dependent upon an annual review process.

(A) To continue an exception, the requesting Participant shall provide a new security assessment that complies with the requirements of Section 6.13(d)(i)(A)(1) and up-to-date versions of the materials required by Section 6.13(d)(i)(A)(2) to the Chief Information Security Officer, the Chief Compliance Officer, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group at least once a year, as measured from the date that the initial

application materials were submitted. If these materials are not provided by the specified date, the Chief Information Security Officer and the Chief Compliance Officer must revoke the exception in accordance with remediation timelines developed by the Plan Processor.

(B) Within 60 days of receipt of the updated application materials, the Chief Information Security Officer and the Chief Compliance Officer must simultaneously notify the Operating Committee and the requesting Participant of their determination.

(1) The Chief Information Security Officer and the Chief Compliance Officer may jointly continue an exception if they 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 pursuant to Section 6.13(d)(ii)(A) 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. If the exception is continued, the Chief Information Security Officer and the Chief Compliance Officer shall provide the requesting Participant with a detailed written explanation setting forth the reasons for that determination.

(2) If the Chief Information Security Officer and the Chief Compliance Officer decide not to continue an exception, they must provide the requesting Participant with a detailed written explanation setting forth the reasons for that determination and specifically identifying the deficiencies that must be remedied before an exception could be granted anew.

(C) If a request for a renewed exception from Section 6.13(a)(i)(B) is denied, or if an exception is revoked pursuant to Section 6.13(d)(ii)(A), the CISO and the CCO must require the requesting Participant to cease employing the user-defined direct query or bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2 in its non-SAW environment in accordance with the remediation timeframes developed by the Plan Processor. The requesting Participant may attempt to re-apply for an exception, after remedying the deficiencies identified by the Chief Information Security Officer and the Chief Compliance Officer, by submitting a new security assessment that complies with the requirements of Section 6.13(d)(i)(A)(1) and up-to-date versions of the materials specified in Section 6.13(d)(i)(A)(2).

(iii) Non-SAW Operations. During the term of any exception granted by the Chief Information Security Officer and the Chief Compliance Officer:

(A) The Participant shall not employ the non-SAW environment to access CAT Data through the user-defined direct query or bulk extract tools described in Section 6.10(c)(i)(B) and Appendix D, Section 8.2 until the Plan Processor notifies the Operating Committee that the non-SAW environment has achieved compliance with the detailed design specifications provided by the Participant pursuant to Section 6.13(d)(i) or (ii).

(B) The Plan Processor shall monitor the non-SAW environment in accordance with the detailed design specifications provided by the Participant pursuant to Section 6.13(d)(i) or (ii), for compliance with those detailed design specifications only, and shall notify the Participant of any identified non-compliance with these detailed design specifications. The Participant shall comply with such detailed design specifications and promptly remediate any identified non-compliance.

(C) The Participant shall simultaneously notify the Plan Processor, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group of any material changes to its security controls for the non-SAW environment.

(D) The Participant may provide and use its choice of software, hardware, and additional data within the non-SAW environment, so long as such activities comply with the detailed design specifications provided by the Participant pursuant to Section 6.13(d)(i) or (ii).

* * * * *

Appendix C

Appendix C was filed with the CAT NMS Plan that was published for comment on May 17, 2016.[803] *As required by Rule 613, Appendix C includes discussion of various considerations related to how the Participants propose to implement the requirements of the CAT NMS Plan, cost estimates for the proposed solution, and the costs and benefits of alternate solutions considered but not proposed. Because these discussions were intended to ensure that the Commission and the Participants had sufficiently detailed information to carefully consider all aspects of the national market system plan that would ultimately be submitted by the Participants, these discussions have not been updated to reflect the subsequent amendments to the CAT NMS Plan and Appendix D.*

Discussion of Considerations

SEC Rule 613(a)(1) Considerations

* * * * *

Appendix D

* * * * *

4.1 Overview

* * * * *

The Plan Processor must provide to the Operating Committee a *C*[c]omprehensive *Information S*[s]ecurity *P*[p]lan that covers all components of the CAT System, including physical assets and personnel, and the training of all persons who have access to the Central Repository consistent with Article VI, Section 6.1(m). The *Comprehensive Information S*[s]ecurity *P*[p]lan must be updated annually. The *Comprehensive Information S*[s]ecurity *P*[p]lan must include an overview of the Plan Processor's network security controls, processes and procedures pertaining to the CAT Systems. Details of the *Comprehensive Information S*[s]ecurity *P*[p]lan must document how the Plan Processor will protect, monitor and patch the environment; assess it for vulnerabilities as part of a managed process, as well as the process for response to security incidents and reporting of such incidents. The *Comprehensive Information S*[s]ecurity *P*[p]lan must address physical security controls for corporate, data center, and leased facilities where Central Repository data is transmitted or stored. The Plan Processor must have documented ''hardening baselines'' for systems that will store, process, or transmit CAT Data or [PII] *Customer and Account Attributes* data.

4.1.1 Connectivity and Data Transfer

[The CAT System(s) must have encrypted internet connectivity. CAT Reporters] *Industry members* must connect to the CAT infrastructure using secure methods such as private lines *for machine-to machine interfaces* or [(for smaller broker-dealers)] *encrypted* Virtual Private Network connections over public lines *for manual web-based submissions. Participants must connect to the CAT infrastructure using private lines. 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. Where possible, more granular ''allow listing'' should be implemented (e.g., by IP address). The Plan Processor must establish policies and procedures to allow access if the location cannot be determined technologically.*

* * * * *

4.1.2 Data Encryption

All CAT Data must be encrypted at rest and in flight using industry standard best practices (*e.g.,* SSL/TLS) including archival data storage methods such as tape backup. Symmetric key encryption must use a minimum key size of 128 bits or greater (*e.g.,* AES–128), larger keys are preferable. Asymmetric key encryption (*e.g.,* PGP) for exchanging data between Data Submitters and the Central Repository is desirable.

Storage of unencrypted [PII] *Customer and Account Attributes* data is not permissible. [PII] *Customer and Account Attributes* encryption methodology must include a secure documented key management strategy such as the use of HSM(s). The Plan Processor must describe how [PII] *Customer and Account Attributes* encryption is performed and the key management strategy (*e.g.,* AES–256, 3DES).

* * * * *

4.1.3 Data Storage and Environment

Data centers housing CAT Systems (whether public or private) must, at a minimum, be AICPA SOC 2 certified by a qualified third-party auditor that is not an affiliate of any of the Participants or the CAT Processor, *and be physically located in the United States.* The frequency of the audit must be at least once per year.

* * * * *

4.1.4 Data Access

The Plan Processor must provide an overview of how access to [PII] *Customer and Account Attributes* and other CAT Data by

[803] *See* Securities Exchange Act Release No. 77724 (April 27, 2016), 81 FR 30613.

Plan Processor employees and administrators is restricted. This overview must include items such as, but not limited to, how the Plan Processor will manage access to the systems, internal segmentation, multi-factor authentication, separation of duties, entitlement management, background checks, etc.

The Plan Processor must develop and maintain policies and procedures reasonably designed to prevent, detect, and mitigate the impact of unauthorized access or usage of data in the Central Repository. Such policies and procedures must be approved by the Operating Committee, and should include, at a minimum:

- Information barriers governing access to and usage of data in the Central Repository;
- Monitoring processes to detect unauthorized access to or usage of data in the Central Repository; and
- Escalation procedures in the event that unauthorized access to or usage of data is detected.

A Role Based Access Control (''RBAC'') model must be used to permission user*s* with access to different areas of the CAT System. The CAT System must support [an arbitrary number of]*as many* roles *as required by Participants and the Commission to permit* [with]access to different types of CAT Data, down to the attribute level. The administration and management of roles must be documented. Periodic reports detailing the current list of authorized users and the date of their most recent access must be provided to Participants, the SEC and the Operating Committee. The reports *provided to*[of] the Participants and the SEC will include only their respective list of users. The Participants must provide a response to the report confirming that the list of users is accurate. The required frequency of this report will be defined by the Operating Committee. The Plan Processor must log every instance of access to Central Repository data by users.

Following ''least privileged'' practices, separation of duties, and the RBAC model for permissioning users with access to the CAT System, all Plan Processor employees and contractors that develop and test Customer Identifying Systems shall only develop and test with non-production data and shall not be entitled to access production data (i.e., Industry Member Data, Participant Data, and CAT Data) in CAIS or the CCID Subsystem. All Plan Processor employees and contractors that develop and test CAT Systems containing transactional CAT Data shall use non-production data for development and testing purposes; if it is not possible to use non-production data, such Plan Processor employees and contractors shall use the oldest available production data that will support the desired development and testing, subject to the approval of the Chief Information Security Officer.

Passwords stored in the CAT System must be stored according to industry best practices. Reasonable password complexity rules should be documented and enforced, such as, but not limited to, mandatory periodic password changes and prohibitions on the reuse of the recently used passwords.

Password recovery mechanisms must provide a secure channel for password reset, such as emailing a one-time, time-limited login token to a pre-determined email address associated with that user. Password recovery mechanisms that allow in-place changes or email the actual forgotten password are not permitted.

Any login to the system that is able to access [PII] *Customer and Account Attributes* data must follow [non-PII password] rules *that do not allow personally identifiable information to be used as part of a password* and must be further secured via multi-factor authentication (''MFA''). The implementation of MFA must be documented by the Plan Processor. MFA authentication capability for all logins is required to be implemented by the Plan Processor.

* * * * *

4.1.5 Breach Management

The Plan Processor must develop *written* policies and procedures governing its responses to systems or data breaches. Such policies and procedures will include a formal cyber incident response plan *(which must include taking appropriate corrective action that includes, at a minimum, mitigating potential harm to investors and market integrity, and devoting adequate resources to remedy the systems or data breach as soon as reasonably practicable),* and documentation of all information relevant to breaches. *The Plan Processor must provide breach notifications of systems or data breaches to CAT Reporters that it reasonably estimates may have been affected, as well as to the Participants and the Commission, promptly after any responsible Plan Processor personnel have a reasonable basis to conclude that a systems or data breach has occurred. Such breach notifications, which must include a summary description of the systems or data breach, including a description of the corrective action taken and when the systems or data breach has been or is expected to be resolved: (a) may be delayed if the Plan Processor determines that dissemination of such information would likely compromise the security of the CAT System or an investigation of the systems or data breach, and documents the reasons for such determination; and (b) do not apply to systems or data breaches that the Plan Processor reasonably estimates would have no or a de minimis impact on the Plan Processor's operations or on market participants.*

The cyber incident response plan will provide guidance and direction during security incidents *and must provide for breach notifications.* The plan will be subject to approval by the Operating Committee. The plan may include items such as:

* * * * *

4.1.6 [PII Data Requirements] Customer Identifying Systems Requirements and Customer Identifying Systems Workflow

Customer and Account Attributes data must be stored separately from other CAT Data within the CAIS. It cannot be stored with the transactional CAT Data in the Central Repository, and it must not be accessible from public internet connectivity.

[PII data] *Customer and Account Attributes* must not be included in the result set(s) from online or direct query tools, reports or bulk data extraction *tools used to query transactional CAT Data.* Instead, *query* results *of transactional CAT Data* will display [existing non-PII] unique identifiers (*e.g.,* Customer-ID or Firm Designated ID). The [PII] *Customer and Account Attributes* corresponding to these identifiers can be gathered [using the PII] *by accessing CAIS in accordance with the Customer Identifying Systems* [w]*W*orkflow described *below* [in Appendix D, Data Security, PII Data Requirements]. By default, users entitled to query CAT Data are not authorized *to access* [for PII] *Customer Identifying Systems* access. The process by which someone becomes entitled [for PII] *to Customer Identifying Systems[* access], and how [they]*an authorized person* then [go about accessing PII data] *can access Customer Identifying Systems,* must be documented by the Plan Processor. The chief regulatory officer *(or similarly designated head(s) of regulation), or his or her designee,* [or other such designated officer or employee] at each Participant must, at least annually, review and certify that people with [PII] *Customer Identifying Systems* access have the appropriate level of access for their role, *in accordance with the Customer Identifying Systems Workflow, as described below.*

[Using the RBAC model described above, access to PII data shall be configured at the PII attribute level, following the ''least privileged'' practice of limiting access as much as possible.

PII data must be stored separately from other CAT Data. It cannot be stored with the transactional CAT Data, and it must not be accessible from public internet connectivity. A full audit trail of PII access (who accessed what data, and when) must be maintained. The Chief Compliance Officer and the Chief Information Security Officer shall have access to daily PII reports that list all users who are entitled for PII access, as well as the audit trail of all PII access that has occurred for the day being reported on.]

A full audit trail of access to Customer Identifying Systems by each Participant and the Commission (who accessed what data and when) must be maintained by the Plan Processor, and the Plan Processor must provide to each Participant and the Commission the audit trail for their respective users on a monthly basis. The Chief Compliance Officer and the Chief Information Security Officer shall have access to daily reports that list all users who are entitled to Customer Identifying Systems access, such reports to be provided to the Operating Committee on a monthly basis.

Customer Identifying Systems Workflow

Access to Customer Identifying Systems

Access to Customer Identifying Systems are subject to the following restrictions:

- *Only Regulatory Staff may access Customer Identifying Systems and such access must follow the ''least privileged'' practice of limiting access to Customer Identifying Systems as much as possible.*
- *Using the RBAC model described above, access to Customer and Account Attributes shall be configured at the Customer and Account Attributes level.*

• *All queries of Customer Identifying Systems must be based on a ''need to know'' data in the Customer Identifying Systems, and queries must be designed such that query results contain only the Customer and Account Attributes that Regulatory Staff reasonably believes will achieve the regulatory purpose of the inquiry or set of inquiries, consistent with Article VI, Section 6.5(g) of the CAT NMS Plan.*

• *Customer Information Systems must be accessed through a Participant's SAW.*

• *Access to Customer Identifying Systems will be limited to two types of access: manual access (which shall include Manual CAIS Access and Manual CCID Subsystem Access) and programmatic access (which shall include Programmatic CAIS Access and Programmatic CCID Subsystem Access).*

• *Authorization to use Programmatic CAIS Access or Programmatic CCID Subsystem Access must be requested and approved by the Commission, pursuant to the provisions below.*

• *Manual CAIS Access*

If Regulatory Staff have identified a Customer(s) of regulatory interest through regulatory efforts and now require additional information from CAT regarding such Customer(s), Manual CAIS Access will be used. Additional information about Customer(s) may be accessed through Manual CAIS Access by (1) using identifiers available in the transaction database (e.g., Customer-ID(s) or industry member Firm Designated ID(s)) to identify Customer and Account Attributes associated with the Customer-ID(s) or industry member Firm Designated ID(s), as applicable; or (2) using Customer Attributes in CAIS to identify a Customer-ID(s) or industry member Firm Designated ID(s), as applicable, associated with the Customer Attributes, in order to search the transaction database. Open-ended searching of parameters not specific to a Customer(s) is not permitted.

Manual CAIS Access will provide Regulatory Staff with the ability to retrieve data in CAIS via the CAIS/CCID Subsystem Regulator Portal with query parameters based on data elements including Customer and Account Attributes and other identifiers available in the transaction database (e.g., Customer-ID(s) or Firm Designated ID(s)).

Performance Requirements for Manual CAIS Access shall be consistent with the criteria set out in Appendix D, Functionality of the CAT System, Online Targeted Query Tool Performance Requirements.

• *Manual CCID Subsystem Access*

Manual CCID Subsystem Access will be used when Regulatory Staff have the ITIN(s)/SSN(s)/EIN(s) of a Customer(s) of regulatory interest obtained through regulatory efforts outside of CAT and now require additional information from CAT regarding such Customer(s). Manual CCID Subsystem Access must allow Regulatory staff to convert ITIN(s)/SSN(s)/EIN(s) into Customer-ID(s) using the CCID Subsystem. Manual CCID Subsystem Access will be limited to 50 ITIN(s)/SSN(s)/EIN(s) per query.

Manual CCID Subsystem Access must provide Regulatory Staff with the ability to retrieve data from the CCID Subsystem via the CAIS/CCID Subsystem Regulator Portal based on ITIN(s)/SSN(s)/EIN(s) where the CCID Transformation Logic is embedded in the client-side code of the CAIS/CCID Subsystem Regulator Portal.

Performance Requirements for the conversion of ITIN(s)/SSN(s)/EIN(s) to Customer-ID(s) shall be consistent with the criteria set out in Appendix D, Functionality of the CAT System, Online Targeted Query Tool Performance Requirements.

Programmatic Access—Authorization for Programmatic CAIS Access and Programmatic CCID Subsystem

A Participant must submit an application, approved by the Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation) to the Commission for authorization to use Programmatic CAIS Access or Programmatic CCID Subsystem Access if a Participant requires programmatic access. The application must explain:

• *Which programmatic access is being requested: Programmatic CAIS Access and/or Programmatic CCID Subsystem Access;*

• *Why Programmatic CAIS Access or Programmatic CCID Subsystem is required, and why Manual CAIS Access or Manual CCID Subsystem Access cannot achieve the regulatory purpose of an inquiry or set of inquiries;*

• *The Participant's rules that require Programmatic Access for surveillance and regulatory purposes;*

• *The regulatory purpose of the inquiry or set of inquires requiring programmatic access;*

• *A detailed description of the functionality of the Participant's system(s) that will use data from CAIS or the CCID Subsystem;*

• *A system diagram and description indicating architecture and access controls to the Participant's system that will use data from CAIS or the CCID Subsystem; and*

• *The expected number of users of the Participant's system that will use data from CAIS or the CCID Subsystem.*

SEC staff shall review the application and may request supplemental information to complete the review prior to Commission action.

The Commission shall approve Programmatic CAIS Access or Programmatic CCID Subsystem Access if it finds that such access is generally consistent with one or more of the following standards: that such access is designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in securities, to remove impediments to and perfect the mechanism of a free and open market and a national market system, and, in general, to protect investors and the public interest.

The Commission shall issue an order approving or disapproving a Participant's application for Programmatic CAIS Access or Programmatic CCID Subsystem Access within 45 days, which can be extended for an additional 45 days if the Commission determines that such longer period of time is appropriate and provides the Participant with the reasons for such determination.

• *Programmatic CAIS Access*

The Plan Processor will provide Programmatic CAIS Access by developing and supporting an API that allows Regulatory Staff to use analytical tools and ODBC/JDBC drivers to access the data in CAIS.

Programmatic CAIS Access may be used when the regulatory purpose of the inquiry or set of inquiries by Regulatory Staff requires the use of Customer and Account Attributes and other identifiers (e.g., Customer-ID(s) or Firm Designated ID(s)) to query the Customer and Account Attributes and transactional CAT Data.

Performance Requirements for Programmatic CAIS Access shall be consistent with the criteria set out in Appendix D, Functionality of the CAT System, User-Defined Direct Query Performance Requirements.

• *Programmatic CCID Subsystem Access*

The Plan Processor will provide Programmatic CCID Subsystem Access by developing and supporting the CCID Transformation Logic and an API to facilitate the submission of Transformed Values to the CCID Subsystem for the generation of Customer-ID(s).

Programmatic CCID Subsystem Access allows Regulatory Staff to submit multiple ITIN(s)/SSN(s)/EIN(s) of a Customer(s) of regulatory interest identified through regulatory efforts outside of CAT to obtain Customer-ID(s) in order to query CAT Data regarding such Customer(s).

Performance Requirements for the conversion of ITIN(s)/SSN(s)/EIN(s) to Customer-ID(s) shall be consistent with the criteria set out in Appendix D, Functionality of the CAT System, User-Defined Direct Query Performance Requirements.

* * * * *

6.1 Data Processing

CAT order events must be processed within established timeframes to ensure data can be made available to Participants' *R*[r]egulatory *S*[s]taff and the SEC in a timely manner. The processing timelines start on the day the order event is received by the Central Repository for processing. Most events must be reported to the CAT by 8:00 a.m. Eastern Time the Trading Day after the order event occurred (referred to as transaction date). The processing timeframes below are presented in this context. All events submitted after T+1 (either reported late or submitted later because not all of the information was available) must be processed within these timeframes based on the date they were received.

The Participants require the following timeframes (Figure A) for the identification, communication and correction of errors from the time an order event is received by the processor:

Noon Eastern Time T+1 (transaction date + one day)—Initial data validation, lifecycle linkages and communication of errors to CAT Reporters;

8:00 a.m. Eastern Time T+3 (transaction date + three days)—Resubmission of corrected data; and

8:00 a.m. Eastern Time T+5 (transaction date

+ five days)—Corrected data available to Participants' *R*[r]egulatory *S*[s]taff and the SEC.

* * * * *

6.2 Data Availability Requirements

Prior to 12:00 p.m. Eastern Time on T+1, raw unprocessed data that has been ingested by the Plan Processor must be available to Participants' *R*[r]egulatory *S*[s]taff and the SEC.

Between 12:00 p.m. Eastern Time on T+1 and T+5, access to all iterations of processed data must be available to Participants' *R*[r]egulatory *S*[s]taff and the SEC.

The Plan Processor must provide reports and notifications to Participants' *R*[r]egulatory *S*[s]taff and the SEC regularly during the five-day process, indicating the completeness of the data and errors. Notice of major errors or missing data must be reported as early in the process as possible. If any data remains un-linked after T+5, it must be available and included with all linked data with an indication that the data was not linked.

If corrections are received after T+5, Participants' *R*[r]egulatory *S*[s]taff and the SEC must be notified and informed as to how re-processing will be completed. The Operating Committee will be involved with decisions on how to re-process the data; however, this does not relieve the Plan Processor of notifying the Participants' *R*[r]egulatory *S*[s]taff and the SEC.

Figure B: Customer and Account *Attributes* [Information (Including PII)]

* * * * *

CAT [PII] *Customer and Account Attributes* data must be processed within established timeframes to ensure data can be made available to Participants' *R*[r]egulatory *S*[s]taff and the SEC in a timely manner. Industry Members submitting [new or modified] *Transformed Values and* Customer *and Account Attributes* [information] must provide [it] *them* to the *CCID Subsystem and* Central Repository *respectively* no later than 8:00 a.m. Eastern Time on T+1. The *CCID Subsystem and* Central Repository must validate the data and generate error reports no later than 5:00 p.m. Eastern Time on T+1. The *CCID Subsystem and* Central Repository must process the resubmitted data no later than 5:00 p.m. Eastern Time on T+4. Corrected data must be resubmitted no later than 5:00 p.m. Eastern Time on T+3. The Central Repository must process the resubmitted data no later than 5:00 p.m. Eastern Time on T+4. Corrected data must be available to regulators no later than 8:00 a.m. Eastern Time on T+5.

Customer information that includes [PII data] *Customer and Account Attributes and Customer-ID(s)* must be available to regulators immediately upon receipt of initial data and corrected data, pursuant to security policies for retrieving [PII] *Customer and Account Attributes and Customer-IDs.*

* * * * *

8.1 Regulator Access

The Plan Processor must provide Participants' [r]*R*egulatory [s]*S*taff and the SEC with access to [all]CAT Data *based on a roles-based access control model that follows* ''*least privileged*'' *practices and only* for *surveillance and* regulatory purposes[only] *consistent with Participants Confidentiality Policies and Procedure as set forth in Article VI, Section 6.5(g).* Participants' [r]*R*egulatory [s]*S*taff and the SEC [will access CAT Data to]*must be* perform*ing regulatory* functions *when using CAT Data,* including *for* economic analyses, market structure analyses, market surveillance, investigations, and examinations, *and 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.*

* * * * *

8.1.1 Online Targeted Query Tool

* * * * *

The tool must provide a record count of the result set, the date and time the query request is submitted, and the date and time the result set is provided to the users. In addition, the tool must indicate in the search results whether the retrieved data was linked or unlinked (*e.g.,* using a flag). In addition, the online targeted query tool must not display any [PII] *Customer and Account Attributes* data. Instead, it will display existing [non-PII] unique identifiers (*e.g.,* Customer-ID or Firm Designated ID). The [PII] *Customer and Account Attributes* corresponding to these identifiers can be gathered using the [PII] *Customer Identifying Systems* [w]*W*orkflow described in Appendix D, Data Security, [PII] *Customer and Account Attributes* Data Requirements. The Plan Processor must define the maximum number of records that can be viewed in the online tool as well as the maximum number of records that can be downloaded *(which may not exceed 200,000 records per query request).* Users must have the ability to download the results to .csv, .txt, and other formats, as applicable. These files will also need to be available in a compressed format (*e.g.,* .zip, .gz). Result sets that exceed the maximum viewable or download limits must return to users a message informing them of the size of the result set and the option to choose to have the result set returned via an alternate method.

The Plan Processor must define a maximum number of records that the online targeted query tool is able to process. The minimum number of records that the online targeted query tool is able to process is 5,000 (if viewed within the online query tool) or 10,000 (if viewed via a downloadable file). *The maximum number of records that can be viewed via downloadable file is 200,000.*

Once query results are available for download, users are to be given the total file size of the result set and an option to download the results in a single or multiple file(s), *if the download does not exceed 200,000 records.* Users that select the multiple file option will be required to define the maximum file size of the downloadable files *subject to the download restriction of 200,000 records per query result.* The application will then provide users with the ability to download the files. This functionality is provided to address limitations of end-user network environment that may occur when downloading large files.

The tool must log submitted queries and parameters used in the query, the user ID of the submitter, the date and time of the submission, as well as the delivery of results *(the number of records in the result(s) and the time it took for the query to be performed). The tool must log the same information for data accessed and extracted, when applicable.* The Plan Processor will use this logged information to provide monthly reports to each Participant and the SEC of its respective metrics on query performance and data usage of the online query tool. The Operating Committee must receive all monthly reports in order to review items, including user usage and system processing performance.

* * * * *

8.1.3 Online Targeted Query Tool Access and Administration

Access to CAT Data is limited to authorized regulatory users from the Participants and the SEC. Authorized regulators from the Participants and the SEC may access all CAT Data, with the exception of [PII] *Customer and Account Attributes* data. A subset of the authorized regulators from the Participants and the SEC will have permission to access and view [PII] *Customer and Account Attributes* data. The Plan Processor must work with the Participants and SEC to implement an administrative and authorization process to provide regulator access. The Plan Processor must have procedures and a process in place to verify the list of active users on a regular basis.

A two-factor authentication is required for access to CAT Data. [PII] *Customer and Account Attributes* data must not be available via the online targeted query tool or the user-defined direct query interface.

* * * * *

8.2 User-Defined Direct Queries and Bulk Extraction of Data

The Central Repository must provide for direct queries, bulk extraction, and download of data for all regulatory users. Both the user-defined direct queries and bulk extracts will be used by regulators to deliver large sets of data that can then be used in internal surveillance or market analysis applications. The data extracts must use common industry formats.

Direct queries must not return or display [PII] *Customer and Account Attributes* data. Instead, they will return existing [non-PII] unique identifiers (*e.g.,* Customer-ID or Firm Designated ID). The [PII] *Customer and Account Attributes* corresponding to these identifiers can be gathered using the [PII] *Customer Identifying Systems* [w]*W*orkflow described in Appendix D, Data Security, [PII] *Customer and Account Attributes* Data Requirements.

* * * * *

8.2.1 User-Defined Direct Query Performance Requirements

The user-defined direct query tool is a controlled component of the production environment made available to allow the Participants' *R*[r]egulatory *S*[s]taff and the SEC to conduct queries. The user-defined direct query tool must:

Provide industry standard programmatic interface(s) that allows Participants' *R*[r]egulatory *S*[s]taff and the SEC with the ability to create, save, and run a query;

* * * * *

8.2.2 Bulk Extract Performance Requirements

* * * * *

Extraction of data must be consistently in line with all permissioning rights granted by the Plan Processor. Data returned must be encrypted, password protected, and sent via secure methods of transmission. In addition, [PII] *Customer and Account Attributes* data *will be unavailable* [must be masked] unless users have permission to view the data that has been requested.

* * * * *

The user-defined direct query and bulk extraction tool must log submitted queries and parameters used in the query, the user ID of the submitter, the date and time of the submission, and the date and time of the delivery of results. The Plan Processor will use this logged information to provide monthly reports to the Operating Committee, Participants and the SEC of their respective usage of the [online query tool]*user-defined direct query and bulk extraction tool.*

* * * * *

8.3 Identifying Latency and Communicating Latency Warnings to CAT Reporters

The Plan Processor will measure and monitor Latency within the CAT network. Thresholds for acceptable levels of Latency will be identified and presented to the Operating Committee for approval. The Plan Processor will also define policies and procedures for handling and the communication of data feed delays to CAT Reporters, the SEC, and Participants' *R*[r]egulatory *S*[s]taff that occur in the CAT. Any delays will be posted for public consumption, so that CAT Reporters may choose to adjust the submission of their data appropriately, and the Plan Processor will provide approximate timelines for when system processing will be restored to normal operations.

* * * * *

9. [CAT Customer and Customer Account Information] CAIS, the CCID Subsystem and the Process for Creating Customer-IDs

9.1 The CCID Subsystem

The Plan Processor will generate a Customer-ID using a two-phase transformation process that does not require ITIN(s)/SSN(s)/EIN(s) to be reported to the CAT. In the first phase, Industry Members or Regulatory Staff will transform the ITIN(s)/SSN(s)/EIN(s) of a Customer using the CCID Transformation Logic, as further outlined below, into a Transformed Value which will be submitted to the CCID Subsystem with any other information and additional elements required by the Plan Processor to establish a linkage between the Customer-ID and Customer and Account Attributes. The CCID Subsystem will perform a second transformation to create the globally unique Customer-ID for each Customer. From the CCID Subsystem, the Customer-ID will be sent to CAIS separately from any other CAT Data (e.g., Customer and Account Attributes) required by the Plan Processor to identify a Customer. The Customer-ID will be linked to the associated Customer and Account Attributes and made available to Regulatory Staff for queries in accordance with Appendix D, 4.1.6 (Customer Identifying Systems Workflow) and Appendix D, Section 6 (Data Availability). The Customer-ID may not be shared with the Industry Member.

The CCID Transformation Logic will be provided to Industry Members and Participants (pursuant to the provisions of Appendix D, Section 4.1.6 (Customer Identifying Systems Workflow), as described below.

Industry Members: The CCID Transformation Logic will be embedded in the CAT Reporter Portal or used by Industry Member in machine-to-machine processing.

Regulatory Staff: Regulatory Staff may receive ITIN(s)/SSN(s)/EIN(s) of Customers from outside sources (e.g., via regulatory data, a tip, complaint, or referral) and require the conversion of ITIN(s)/SSN(s)/EIN(s) to Customer-ID(s). Consistent with the provisions of Appendix D, Section 4.1.6 (Customer Identifying Systems Workflow), for conversion of fifty or fewer ITIN(s)/SSN(s)/EIN(s), the Plan Processor will embed the CCID Transformation Logic in the client-side code of the CAIS/CCID Subsystem Regulator Portal. For Programmatic CCID Access, Participants and the SEC will use the CCID Transformation Logic pursuant to the provisions of Appendix D, Section 4.1.6 (Customer Identifying Systems Workflow).

The CCID Subsystem must be implemented using network segmentation principles to ensure traffic can be controlled between the CCID Subsystem and other components of the CAT System, with strong separation of duties between the CCID Subsystem and all other components of the CAT System. The design of the CCID Subsystem will maximize automation of all operations of the CCID Subsystem to prevent, if possible, or otherwise minimize human intervention with the CCID Subsystem and any data in the CCID Subsystem.

The Participants must ensure the timeliness, accuracy, completeness, and integrity of a Transformed Value(s), and must ensure the accuracy and overall performance of the CCID Subsystem to support the creation of a Customer-ID that uniquely identifies each Customer. The Participants also must assess the overall performance and design of the CCID Subsystem and the process for creating Customer-ID(s) as part of each annual Regular Written Assessment of the Plan Processor, as required by Article VI, Section 6.6(b)(i)(A). Because the CCID Subsystem is part of the CAT System, all provisions of the CAT NMS Plan that apply to the CAT System apply to the CCID Subsystem.

9.[1]2 Customer and [Customer] Account Attributes in CAIS and Transformed Values [Information Storage]

The CAT must [capture] *collect* and store Customer and [Customer Account Information] *Account Attributes* in a secure database physically separated from the transactional database. The Plan Processor will maintain information of sufficient detail to uniquely and consistently identify each Customer across all CAT Reporters, and associated accounts from each CAT Reporter. The following attributes, at a minimum, must be captured:

- [Social security number (SSN) or Individual Taxpayer Identification Number (ITIN);
- Date of birth;
- Current n]*N*ame *(including first, middle and last name);*
- [Current a]*A*ddress *(including street number, street name, street suffix and/or abbreviation (e.g., road, lane, court, etc.), city, state, zip code, and country;*
- [Previous name] *Year of Birth;* and
- [Previous address] *Role in the Account.*

For legal entities, the CAT must [capture] *collect* the following attributes:

- [Legal Entity Identifier (LEI) (if available);
- Tax identifier;
- [Full legal name; [and]
- Address[.] *(including street number, street name, street suffix and/or abbreviation (e.g., road, lane, court, etc.), city, state, zip code, and country;*
- *Employer Identification Number (EIN); and*
- *Legal Entity Identifier (LEI), or other comparable common entity identifier (if available), provided that if an Industry Member has an LEI for a Customer, the Industry Member must submit the Customer's LEI.*

For the account of a Customer, the Plan Processor must collect, at a minimum, the following data:

- *Account Owner Name*
- *Account Owner Mailing Address*
- *Account type;*
- *Customer type;*
- *Date Account Opened, or Account Effective Date, as applicable;*
- *Large Trader Identifier (if applicable);*
- *Prime Broker ID;*
- *Bank Depository ID; and*
- *Clearing Broker.*

The Plan Processor must maintain valid Customer and [Customer] Account *Attributes* [Information] for each trading day and provide a method for Participants' [r]*R*egulatory [s]*S*taff and [the]SEC *staff* to easily obtain historical changes to [that information (*e.g.,* name changes, address changes, etc.)] *Customer-IDs, Firm Designated IDs, and all other Customer and Account Attributes.*

[The Plan Processor will design and implement a robust data validation process for submitted Firm Designated ID, Customer Account Information and Customer Identifying Information, and must continue to process orders while investigating Customer information mismatches. Validations should:

- Confirm the number of digits on a SSN,

- Confirm date of birth, and
- Accommodate the situation where a single SSN is used by more than one individual.]

The Plan Processor will use the [Customer information submitted by all broker-dealer CAT Reporters] *Transformed Value* to assign a unique Customer-ID for each Customer. The Customer-ID must be consistent across all [broker-dealers] *Industry Members* that have an account associated with that Customer. This unique [CAT-]Customer-ID will not be returned to [CAT Reporters and will only be used internally by the CAT] *Industry Members.*

[Broker-Dealers] *Industry Members* will initially submit full [account] lists *of Customer and Account Attributes, Firm Designated IDs, and Transformed Values* for all [a]*A*ctive [a]*A*ccounts to the Plan Processor and subsequently submit updates and changes on a daily basis. In addition, the Plan Processor must have a process to periodically receive [full account lists] *updates, including a full refresh of all Customer and Account Attributes, Firm Designated IDs, and Transformed Values* to ensure the completeness and accuracy of the [account database] *data in CAIS.* The Central Repository must support account structures that have multiple account owners and associated Customer *and Account Attributes* [information] (joint accounts, managed accounts, etc.), and must be able to link accounts that move from one [CAT Reporter] *Industry Member* to another (*e.g.,* due to mergers and acquisitions, divestitures, etc.).

[9.2 Required Data Attributes for Customer Information Data Submitted by Industry Members

At a minimum, the following Customer information data attributes must be accepted by the Central Repository:

- Account Owner Name;
- Account Owner Mailing Address;
- Account Tax Identifier (SSN, TIN, ITIN);
- Market Identifiers (Larger Trader ID, LEI);
- Type of Account;
- Firm Identifier Number;
  - The number that the CAT Reporter will supply on all orders generated for the Account;
- Prime Broker ID;
- Bank Depository ID; and
- Clearing Broker.]

9.3. Customer-ID Tracking

The Plan Processor will assign a [CAT-]Customer-ID for each unique Customer. The Plan Processor will [determine] *create* a unique Customer-*ID* using [information such as SSN and DOB] *the Transformed Value* for natural persons *Customers* or *an EIN for legal* entity [identifiers for]-Customers [that are not natural persons] and will resolve *discrepancies in Transformed Values).* Once a [CAT-]Customer-ID is assigned, it will be added to each linked (or unlinked) order record for that Customer.

Participants and the SEC must be able to use the unique [CAT-]Customer-ID to track orders from, *and allocations to,* any Customer or group of Customers *over time,* regardless of what brokerage account was used to enter the order.

9.4 Error Resolution for [Customer Data] the CCID Subsystem and CAIS

The CCID Subsystem and CAIS shall support error resolution functionality which includes the following components: validation of submitted data, notification of errors in submitted data, resubmission of corrected data, validation of corrected data, and an audit trail of actions taken to support error resolution.

Consistent with Section 7.2, the Plan Processor will design and implement a robust data validation process for all ingested values and functionality including, at a minimum:

- *The ingestion of Transformed Values and the creation of Customer-IDs through the CCID Subsystem;*
- *The transmission of Customer-IDs from the CCID Subsystem to CAIS or a Participant's SAW; and*
- *The transmission and linking of all Customer and Account Attributes and any other identifiers (e.g., Industry Member Firm Designated ID) required by the Plan Processor to be reported to CAIS.*

For example, the validation process should at a minimum identify and resolve errors with an Industry Member's submission of Transformed Values, Customer and Account Attributes, and Firm Designated IDs including where there are identical Customer-IDs associated with significantly different names, and identical Customer-IDs associated with different years of birth, or other differences in Customer and Account Attributes for identical Customer-IDs.

These validations must result in notifications to the Industry Member to allow for corrections, resubmission of corrected data and revalidation of corrected data. As a result of this error resolution process there will be accurate reporting within a single Industry Member as it relates to the submission of Transformed Values and the linking of associated Customer and Account Attributes reported.

The Plan Processor must design and implement procedures and mechanisms to handle both minor and material inconsistencies in Customer information. The Central Repository needs to be able to accommodate minor data discrepancies such as variations in road name abbreviations in searches. Material inconsistencies such as two different people with the same [SSN] *Customer-ID* must be communicated to the submitting [CAT Reporters] *Industry Members* and resolved within the established error correction timeframe as detailed in *Appendix D,* Section [8]*6.2.*

The Central Repository must have an audit trail showing the resolution of all errors *including material inconsistencies, occurring in the CCID Subsystem and CAIS.* The audit trail must, at a minimum, include the:

- [CAT Reporter] *Industry Members and Participants (pursuant to the provisions of Appendix D, Section 4.1.6 (Customer Identifying Systems Workflow) submitting the [data] Transformed Value or Customer and Account Attributes and other identifiers, as applicable;*
- Initial submission date and time;
- Data in question or the ID of the record in question;
- Reason identified as the source of the [issue]*error,* such as:
  - *Transformed Value outside the expected range of values;*
  - duplicate [SSN]*Customer-ID,* significantly different Name;
  - duplicate [SSN]*Customer-ID,* different [DOB]*year of birth;*
  - discrepancies in LTID; or
  - others as determined by the Plan Processor;
- Date and time *notification of* the [issue] *error* was transmitted to the [CAT Reporter]*Industry Member or Participant (pursuant to the provisions of Appendix D, Section 4.1.6 (Customer Identifying Systems Workflow),* include[ed]*ing* each time the issue was re-transmitted, if more than once;
- Corrected submission date and time, including each corrected submission if more than one, or the record ID(s) of the corrected data or a flag indicating that the issue was resolved and corrected data was not required; and
- Corrected data, the record ID, or a link to the corrected data.

10. User Support

10.1 CAT Reporter Support

The Plan Processor will provide technical, operational and business support to CAT Reporters for all aspects of reporting *including, but not limited to, issues related to the CCID Transformation Logic and reporting required by the CCID Subsystem.* Such support will include, at a minimum:

- Self-help through a web portal;
- Direct support through email and phone;
- Support contact information available through the internet; and
- Direct interface with Industry Members and Data Submitters via industry events and calls, industry group meetings and informational and training sessions.

The Plan Processor must develop tools to allow each CAT Reporter to:

- Monitor its submissions;
- View submitted transactions in a non-bulk format (*i.e.,* non-downloadable) to facilitate error corrections;
- Identify and correct errors;
- Manage Customer and [Customer]Account *Attributes*[Information];
- Monitor its compliance with CAT reporting requirements;[and]
- Monitor system status[.]*; and*
- *Monitor the use of the CCID Transformation Logic including the submission of Transformed Values to the CCID Subsystem.*

* * * * *

10.2 CAT User Support

The Plan Processor will develop a program to provide technical, operational and business support to CAT users, including Participants' *R*[r]egulatory *S*[s]taff and the SEC. The CAT help desk will provide technical expertise to assist regulators with questions and/or functionality about the content and structure of the CAT query capability.

The Plan Processor will develop tools, including an interface, to allow users to monitor the status of their queries and/or

reports. Such website will show all in-progress queries/reports, as well as the current status and estimated completion time of each query/report.

The Plan Processor will develop communication protocols to notify regulators of CAT System status, outages and other issues that would affect Participants' *R*[r]egulatory *S*[s]taff and the SEC's ability to access, extract, and use CAT Data. At a minimum, Participants' *R*[r]egulatory *S*[s]taff and the SEC must each have access to a secure website where they can monitor CAT System status, receive and track system notifications, and submit and monitor data requests.

The Plan Processor will develop and maintain documentation and other materials as necessary to train regulators in the use of the Central Repository, including documentation on how to build and run reporting queries.

10.3 CAT Help Desk

The Plan Processor will implement and maintain a help desk to support broker-dealers, third party CAT Reporters, and Participant CAT Reporters (the ''CAT Help Desk''). The CAT Help Desk will address business questions and issues, as well as technical and operational questions and issues. The CAT Help Desk will also assist Participants' regulatory staff and the SEC with questions and issues regarding obtaining and using CAT Data for regulatory purposes.

The CAT Help Desk must go live within a mutually agreed upon reasonable timeframe after the Plan Processor is selected, and must be available on a 24x7 basis, support both email and phone communication, and be staffed to handle at minimum 2,500 calls per month. Additionally, the CAT Help Desk must be prepared to support an increased call volume at least for the first few years. The Plan Processor must create and maintain a robust electronic tracking system for the CAT Help Desk that must include call logs, incident tracking, issue resolution escalation.

CAT Help Desk support functions must include:

- Setting up new CAT Reporters, including the assignment of CAT-Reporter-IDs and support prior to submitting data to CAT;
- Managing CAT Reporter authentication and entitlements;
- Managing CAT Reporter and third party Data Submitters testing and certification;
- Managing Participants and SEC authentication and entitlements;
- Supporting CAT Reporters with data submissions and data corrections, including submission of Customer and [Customer] Account *Attributes* [Information];
- Coordinating and supporting system testing for CAT Reporters;
- Responding to questions from CAT Reporters about all aspects of CAT reporting, including reporting requirements, technical data transmission questions, potential changes to SEC Rule 613 that may affect the CAT, software/hardware updates and upgrades, entitlements, reporting relationships, and questions about the secure and public websites;
- Responding to questions from Participants' regulatory staff and the SEC about obtaining and using CAT Data for regulatory purposes, including the building and running of queries; [and]
- Responding to administrative issues from CAT Reporters, such as billing*; and*
- *Responding to questions from and providing support to CAT Reporters regarding all aspects of the CCID Transformation Logic and CCID Subsystem.*

By the Commission.

Dated: August 21, 2020.

Vanessa A. Countryman,

Secretary.

[FR Doc. 2020–18801 Filed 10–15–20; 8:45 am]

BILLING CODE 8011–01–P