212° DATA BOILER TECHNOLOGIES, LLC

BIG DATA | BIG PICTURE | BIG OPPORTUNITIES

We see big to continuously boil down the essential improvements until you achieve sustainable growth!

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

November 30, 2020

Via Electronic Mail (rule-comments@sec.gov)

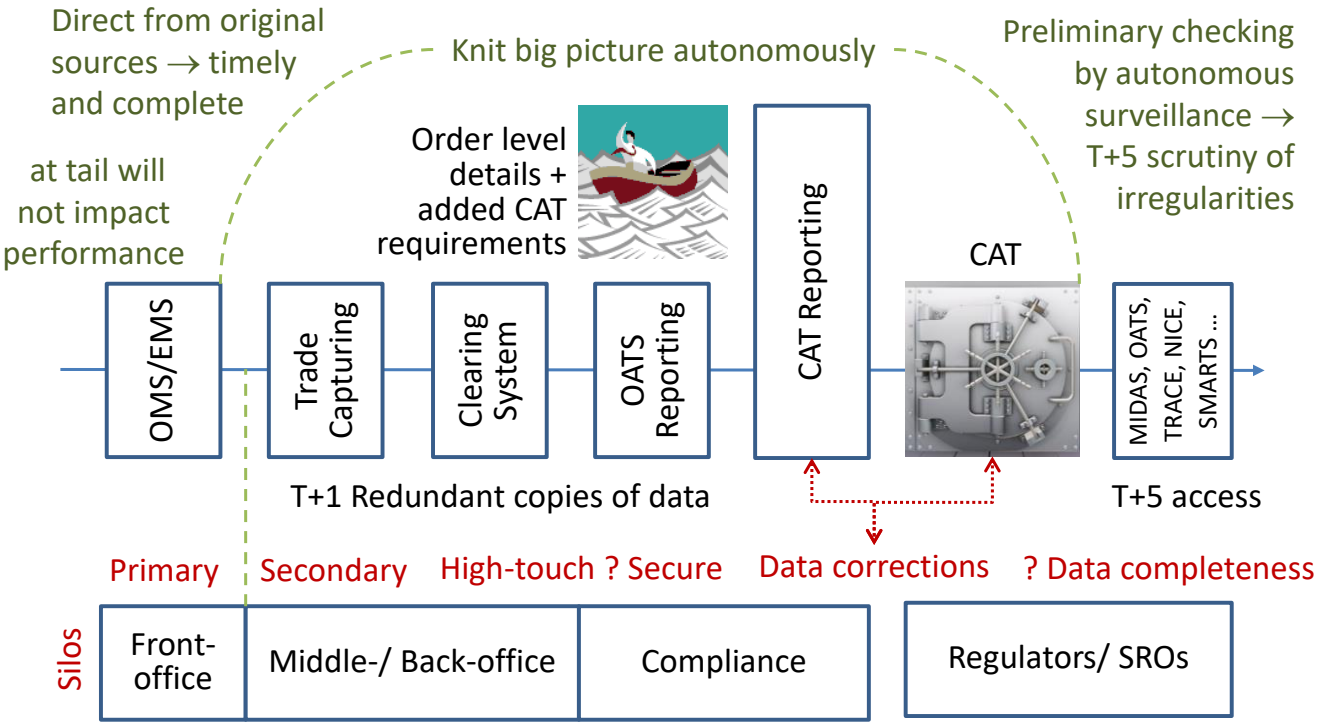
Ms. Vanessa Countryman, Secretary
U.S. Securities and Exchange Commission
100 F Street NE., Washington, DC 20549

Re: Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security[1] File No. S7-10-20 (Release #: 34-89632; RIN 3235-AM62)

Dear Ms. Countryman:

On behalf of Data Boiler Technologies, I am pleased to provide the U.S. Securities and Exchange Commission (SEC) with our comments on this release concerning enhance Data Security for the Consolidated Audit Trail (CAT) system. We applaud the SEC and the CAT processor – Financial Industry Regulatory Authority (FINRA) for recognizing the importance of information security and privacy protection over CAT data. While critical to many aspects of the CAT project since our initial comments in July 2016[2] (many concerns still remain as of today), we do hope to **make the best out of this 'less than ideal' system**.

That being said, if CAT were ever have a complete overhaul, we strongly suggest its design adopts Real-time Analytical Platform (RTAP) to directly conduct surveillance from the original source of the data. 'T+5' is way too late compared to modern standards. Especially, if the original intent or one of the **justifications for building CAT** was for enhanced market surveillance to mitigate and **prevent Flash Crashes**.[3] ***Figure 1*** below illustrates what can be done to augment the deficiencies of CAT.



[1] https://www.sec.gov/rules/sro/nms/2020/34-90096.pdf
[2] https://www.sec.gov/comments/4-698/4698-4.pdf
[3] https://youtu.be/dIq16lZBnDY

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

We despise unnecessary redundant copies of data as it affects data quality and exposes the information to higher chance of unauthorized access. CAT was designed as a gigantic vault, with an overemphasis on structure rather than embedding a dynamic analytical framework in the design. We favor RTAP to help conduct automated surveillance at high "velocity" efficiency rather than "subjective" to user defined queries or bulk data extraction. With regard to **big data, a timely early warning to facilitate analysis and good decisions is substantially superior than perfecting whatever 'golden-source' of data**. User Defined Direct Query (UDDQ) and bulk extraction increase the vulnerability of data being misused for impermissible purposes. Automated checking of trade irregularities according to certain "defined purposes" would improve "objectiveness" of the surveillance scan.

We believe that the **broker-dealer community would welcome a "clean-scan"** on data exhaust from their order management systems **(OMS)** or execution management systems **(EMS) than the burden of data submission** for CAT and **filing Suspicious Activity Reports (SAR)**. After the scan they can be provided with a percentage indicator that the broker/ dealer' trade activity may be "**certified clean**" or subjected to the SEC/ FINRA/ SROs exams. This method is indeed drawing a real-life analogy from the Internal Revenue Services (IRS)'s 'My Free Taxes' initiative.[4] The noteworthy fact is: designated private tax filing firms concurrently analyze the data for and on-behalf of the IRS. Allowing the IRS to only **focus on those high-risk candidates for scrutinized exams**, as a majority of good citizens can handle their annual tax return with ease. Please see this article[5] for how the analogy can be applied in context of CAT and market surveillance.

Again, analyzing the data directly at the original source avoids unnecessary making of redundant copies of data. By reducing the amount of 'data-in-motion'[6] it will make CAT much more **secure**, **effective** (OMS/EMS capture trade orders at nanoseconds rather than CAT data with 50± milliseconds tolerance[7]), and **efficient** (T+0). Based on the existing design of CAT, because it encompasses substantial data transmissions, its security and privacy controls must be fortified to the highest standards. Storing data other than evidence or symptoms of prosecutable crime may trigger **civic concerns**. According to a Stanford University's study about **massive government surveillance**[8],

"…most people in our society would object to this solution, not because they wish to commit any wrongdoings, but because it is invasive and prone to abuse."

"…fails to take into consideration a number of important issues when collecting personally identifiable data or recordings."

"…such practices create an archive of information that is vulnerable to abuse by trusted insiders."

"In addition, allowing surreptitious surveillance of one form, even limited in scope and for a particular contingency, encourages government to expand such surveillance programs in the future. It is our view that the danger of a 'slippery slope' scenario cannot be dismissed as paranoia."

"When data is collected, whether such data remains used for its stated purpose after its collection has been called into question… even when two databases of information are created for specific, distinct purposes, in a phenomenon known as 'function creep' they could be combined with one another to form a third with a purpose for which the first two were not built… This non-uniqueness and immutability of information provides great potential for abuse…"

[4] https://www.myfreetaxes.com/
[5] https://www.linkedin.com/pulse/hr-block-analogy-cat-combating-fraud-kelvin-to/
[6] https://www.databoiler.com/index_htm_files/DataBoilerInMotion.pdf
[7] https://tabbforum.com/opinions/is-clock-synch-the-cats-fatal-flaw/
[8] https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/ethics.html

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

The Stanford study also includes a list of questions suggested by a MIT professor that one should evaluate the proposed methods before implementing surveillance. We would be happy to assist the SEC and FINRA to address these questions if given the opportunity. In the meanwhile, we came up with ***Table 1*** below, which showcases the **'A through Z' security and privacy clauses**. We recommend the SEC to adopt these clauses as part of the minimum requirements for principle based rules rather than making specific reference to revision 4 of SP800-53 by the NIST.[9]

#	Suggested Clauses	Rationale/ Justifications
A	CAT should minimize 'data-in-motion' whenever and wherever possible;	The more frequent the transmittal of data in-and-out and within CAT, the more vulnerable it is.
B	Whenever and wherever the data is consumed or 'in-use', it has to serve 'defined purpose(s)' and be at a 'secured environment';	Civic concern of massive government surveillance. 'Data-in-use' is more vulnerable than 'at-rest'. The more users/ devices access to data, the greater the risk hackers may alter/ add/ insert/ use the data abusively.
C	The appropriate eradication or removal of data as soon as data has been transmitted or used to avoid 'function creep';	Omission or incomplete or untimely eradication would introduce opportunities for hackers.
D	No usage or possession outside of 'defined purposes';	'Function creep' = abuse of CAT related tech or data.
E	When data is 'at-rest', it must be stored at designated 'secured environments';	Data-vault, data-lake, and 'golden source of data' are indeed targets attracting hackers to treasure hunt.
F	'Secured environments' must be segregated in accordance to 'sensitivity' of stored data;	Minimize vulnerability to specific range of data fields and/or records.
G	If data is considered 'sensitive', it must be obfuscated at all times ('at-rest'/ 'in-motion') except when it is 'in-use'; whenever 'alternate' surveillance methods are available, CAT users should refrain from querying 'sensitive' data.	Personal identifiable information (PII) or any data similar to that nature is deemed sensitive. If there is a way(s) to enable surveillance intelligence[10] without crossing the line of privacy[11] hazard, CAT must adopt.
H	'Defined purposes' are limited to 'market surveillance', 'specific case investigation' and/or 'rule enforcement' only;	Again, the Civic concern as stated in "B". No-one wants his/her data be used by regulator(s) to develop policies that potentially may discriminative against him/her.
I	If using metadata can achieve the 'defined purpose', CAT should by all mean avoid collecting or creating repetitive copies of raw data;	Prevent information leakage. Somehow metadata is more useful than raw data, especially when raw data is inherited with imperfect quality (50±ms tolerance).
J	If using 'integrated' data can achieve the 'defined purpose', CAT should avoid collecting data at lower domain;	Roll-up aggregation is another technique similar to masking or obfuscation that helps prevent leakage.

[9] We are glad that the Commission and the CAT processor are pointing to the special publication 800-53 by the National Institute of Standards and Technology (NIST), which we have very high regards for its comprehensiveness. However, when considering the development of Comprehensive Information Security Policy (CISP), revision 4 of SP800-53 has been superseded by revision 5 since September 2020. Also, NIST's recommended best practices alongside other Cybersecurity and Privacy protection standards/ guidelines, such as ISO/IEC 27001 and 27032, Gramm-Leach-Bliley Act §6801, and FINRA's cybersecurity rules and guidance, etc. may continue to have updates and new added contents. We have multiple concerns if CISP is referencing to a particular NIST publication, including: (1) potential of complying with the bear minimal requirements rather than pursuing the best practices; (2) new emerging cyber threats that the corresponding mitigation method(s) have yet to be incorporated in newer standard – i.e. the in-between time awaiting to adopt new policy; (3) non-synchronize with international rules, such as the EU's General Data Protection Regulation (GDPR).

[10] https://people.eecs.berkeley.edu/~jfc/'mender/IEEESP02.pdf

[11] https://www.fdic.gov/regulations/examinations/financialprivacy/handbook/

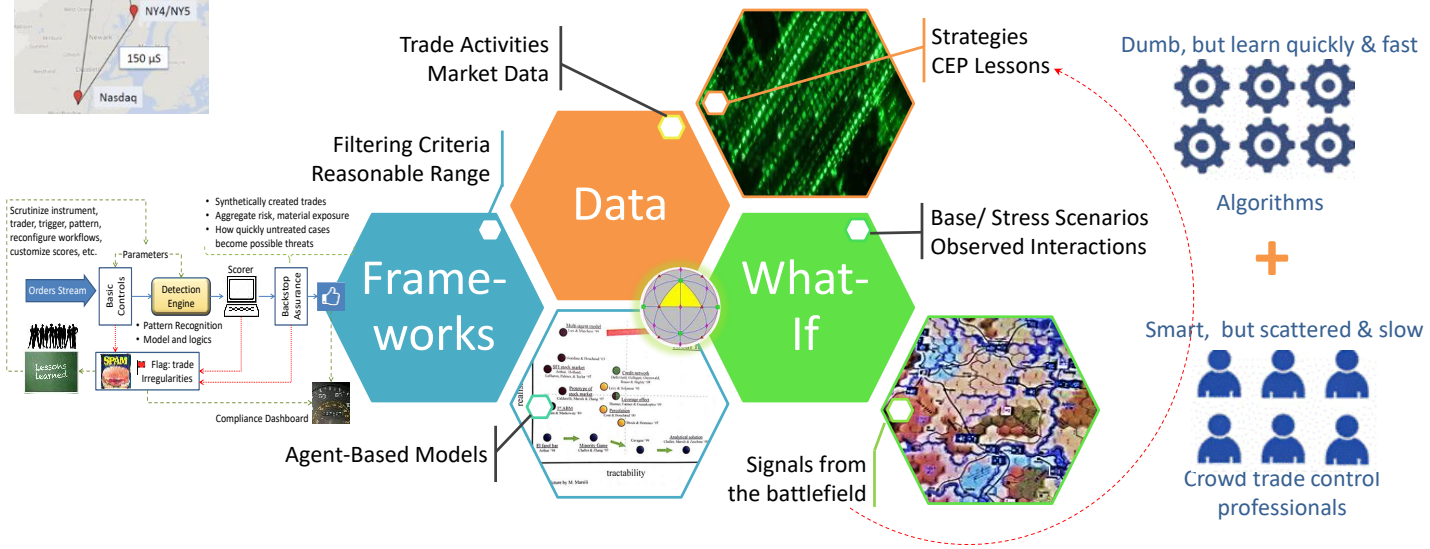
☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

#	Suggested Clauses (continue)	Rationale/ Justifications
K	All data trajectory must be mapped, assessed, and monitored;	Scrutinize any Repurpose or Reuse or Recycle of data.
L	All users' entitlement in accessing CAT or its data must be duly authorized and maintained without delay;	Share access is a common threat, and lapsed entitlement introduces opportunities for hackers.
M	No access to CAT before a 'defined purpose' is identified and a secured connection is established;	Access entitlement does not mean there is no usage limit on CAT. Gateway and proxies need appropriate inspection to deter unsecure connection to CAT.
N	All user activities must be logged timely in the system;	For scrutinization of any abnormal activities.
O	CAT functionalities and 'data-in-use' should be segregated based on 'defined purpose(s)' of specific user group(s);	Restrict the usage to specific range of data fields and/or records that fits the 'defined purpose(s)'.
P	Whenever possible, apply analytic techniques closest to the original source of data rather than making redundant copies of data;	Redundant copies of data affect data quality and expose the information to higher chance of unauthorized access.
Q	Use of 'predefined automated analytical steps' instead of ad-hoc data query wherever possible;	'Predefined automated analytical steps' require proper testing and authorization by Operating Committee.
R	Volume and frequency of ad-hoc data queries for 'specific case investigation' or 'rule enforcement' purpose is limited;	E.g. to < 0.001% of daily order volume of the targeted broker-dealer with suspicious activity per-query per-user per-day; < 0.01% in aggregate every two weeks.
S	No access to CAT for 'market surveillance' purpose prior to identifying symptoms of irregularity that are substantiated by data at SIPs and/or analytical procedures at SROs/ the SEC;	Again, the Civic concern as stated in "B". Suspicion of crime or anticipation of market turmoil should begin with some basis or require 'search warrant' before permissible surveillance on information that would otherwise be considered as private.
T	Bulk data extraction is generally prohibited, except during 'market crash' with special authorization from the SEC;	Where 'market crash' period may refer to Limit Up-Limit Down trigger or exchange halt scenarios.
U	Database server infrastructure and configuration should prioritize 'consistency' and 'partition tolerance' over 'availability', and CAT system should be in compliant with Atomicity, Consistency, Isolation, and Durability (ACID).	The controversy is that CAT as a surveillance tool is supposed to prioritize 'availability' over the two other attributes. Real-time or velocity of data serves to provide a higher values than veracity of data during a 'market crash'. The T+5 access defeats CAT purpose.
V	Data loss protection (DLP) infrastructure must include proper steps for effective and efficient data disposal;	Retaining more data than necessary is a liability. Record retention must be enforced diligently.
W	Audit logs (including user activities, network performance and other system gauges for automated threat detection) must be readily available for exam upon request;	The timelier the review, the higher the chance to salvage a loss situation.
X	Abnormality to CAT or its data or connectivity, or breach of control must be reported in timely manner;	Give the reviewers the authority to provide non-bias and timely report of problems to the upmost Seniors.
Y	Any control compromised must be diligently rectified; independent assessment to recommend interim actions;	Avoid 'bandage' or temporary fix, or a fix in one area may inadvertently cause vulnerability in other area(s).
Z	Must actively observe, adopt and pursuit relevant information security and privacy best practices.	Continuous improvement, ensure forward looking (e.g. today's encryption will be obsoleted upon quantum).

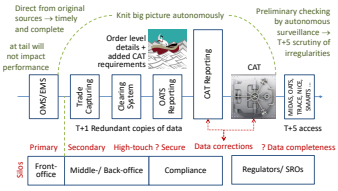
☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

To effectively mitigate privacy and security risks without creating bureaucracy, do keep in mind the following three management fundamentals: (i) segregation of duties[12], (ii) keep clean with high incentives (e.g. whistleblower award), and (iii) precognitive prevention by reducing the amount of unknown unknowns[13]. We envisage a crowd model to reduce unknown unknowns while enhance security of CAT, see ***Figure 2*** below:

1. If SIPs will expand core data to include depth-of-book, odd-lots, auction, etc. (i.e. 'order level' details), then there is no need to overlap this publicly available information at CAT.
2. Cross tabulate early warning signals from mining of SIP data with intelligence gathered from SROs' surveillance systems (i.e. onset signal detection from better data (captured data at SIPs and SROs are at nanoseconds rather than CAT data with 50± milliseconds tolerance).



3. Enabling the crowd with an open platform consists of: (a) a community library of basic trade patterns, similar to a music editor tool for the crowd to modify basic patterns into new trade strategies to discover alpha (or the unknown unknowns), a simulation tool where new strategies will be back tested, and a reward scheme if back-testing results shown useful insights into reducing unknown unknowns.
4. By leveraging crowd intelligence in step 3 (learn from the field that is closest to the market and in real time) and combining with surveillance findings gathered from steps 1 and 2, it would substantiate enough supporting arguments for identified 'symptoms' of market or trade irregularities.
5. Then, whatever residual data that are not otherwise available at SIPs or SROs would be collected through CAT, which substantially reduces CAT storage (avoid unnecessary regurgitation or repetitive copies of data) to only those data that are essential for law enforcement or prosecution investigation related to specific cases.
6. Through pre-defined automated pre-screening of data that broker-dealers are about to submit to CAT (i.e. targeted to look for specific 'red-flag(s)'), if no 'red-flag' is found relevant to previously identified symptom(s), then trade activities may be certified 'clean' and that batch of data is no longer required to be stored at CAT.
7. With substantiated 'symptoms' and identified 'red-flag(s)', retrieve or subpoena evidence by querying relevant data field/ records would be permissible.



The benefits of the suggested approach are: (a) dramatically reduce CAT footprint or data storage and traffic by avoiding unnecessary redundant copies of data and minimize 'data-in-motion'; (b) confine access to CAT data to 'targeted search' of relevant data that fits the 'defined purposes'; and (c) better intelligence for market monitoring by enabling and

[12] https://www.linkedin.com/pulse/big-data-privacy-security-control-kelvin-to/
[13] https://www.pmi.org/learning/library/characterizing-unknown-unknowns-6077

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

rewarding the crowd for identifying early warning signals to potential flash crash or other trade irregularities (see our comments[14] to the SEC regarding 'CT Plan'[15] for further details).

After all, the purpose and challenge of CAT (or IOSCO – CR12/2012[16]) cannot be solved by a gigantic data vault. Big data is about fit-for-purpose. Again, **a timely early warning to facilitate analysis and good decisions is substantially superior than perfecting whatever 'golden-source' of data**. Velocity (real-time) is more important than Veracity (too late by the time data achieves perfect accuracy).[17] We argue that Variety of data (i.e. inclusion of CFTC's Futures data) is more important than solely having high Volume of equity and option data. For that, we urge the SEC and CFTC to work together in considering our suggested approach in ***Figure 2***. We hope the above comments and the detailed responds to the Commission's specific questions below will be helpful to the SEC and benefiting to the broader industry. Feel free to contact us with any questions. Thank you and we look forward to engage in any opportunities where our expertise might be required.

Sincerely,

Kelvin To

Founder and President

Data Boiler Technologies, LLC

Former member of Financial Services Roundtable – BITS (Banking Policy Institute) information security committee

CC: The Honorable Jay Clayton, Chairman
The Honorable Hester M. Peirce, Commissioner
The Honorable Elad L. Roisman, Commissioner
The Honorable Allison Herren Lee, Commissioner
The Honorable Caroline A. Crenshaw, Commissioner
Mr. Brett Redfearn, Director, Division of Trading and Markets
Ms. Andrea Orr, Counsel to the Director of Trading and Markets

This letter is also available at:
https://www.DataBoiler.com/index_htm_files/DataBoiler%20SEC%20CAT%20Enhanced%20Security.pdf

[14] https://www.sec.gov/comments/4-757/4757-8011765-225416.pdf
[15] https://www.sec.gov/comments/4-757/4757-8038490-225613.pdf
[16] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD389.pdf
[17] https://www.amazon.com/Big-Data-Revolution-Transform-Think/dp/0544227751/

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Table of Contents

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Answers to Specific Questions

II. Description of Proposed Amendments

A. Comprehensive Information Security Program

Question 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?

The Commission should not attempt to prescribe any particular form of security control measures or best practices. Instead, there should be high-level principles to guide the CAT project to embed essential security, privacy, and analytical frameworks in its design. It is better than reference to an outdated revision 4 of NIST's SP800-53. Please see footnote 9 and ***Table 1***.

Question 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.

CISP should be modified per our 'A through Z' suggested clauses in ***Table 1***.

Question 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.

In our opinion, civic concern about massive government surveillance is the biggest issue aside from the lack of funding or money problem for CAT. The related information security and privacy problems for CAT are rooted from the fundamental design of CAT as a gigantic data-vault being flawed.[2] CISP as currently proposed in §6.12, §4 of Appendix D and §6.13 is incomplete. Before implementing surveillance, policy makers should evaluate the proposed methods and develop appropriate respond to the following questions raised by M.I.T. professor Gary Marx in this Stanford University study.[8]

*"**A. The Means***

***Harm:** does the technique cause unwarranted physical or psychological harm?*

***Boundary:** does the technique cross a personal boundary without permission (whether involving coercion or deception or a body, relational or spatial border)?*

***Trust:** does the technique violate assumptions that are made about how personal information will be treated such as no secret recordings?*

***Personal relationships:** is the tactic applied in a personal or impersonal setting?*

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Invalidity: *does the technique produce invalid results?*

B. The Data Collection Context

Awareness: *are individuals aware that personal information is being collected, who seeks it and why?*

Consent: *do individuals consent to the data collection?*

Golden rule: *would those responsible for the surveillance (both the decision to apply it and its actual application) agree to be its subjects under the conditions in which they apply it to others?*

Minimization: *does a principle of minimization apply?*

Public decision-making: *was the decision to use a tactic arrived at through some public discussion and decision making process?*

Human review: *is there human review of machine generated results?*

Right of inspection: *are people aware of the findings and how they were created?*

Right to challenge and express a grievance: *are there procedures for challenging the results, or for entering alternative data or interpretations into the record?*

Redress and sanctions: *if the individual has been treated unfairly and procedures violated, are there appropriate means of redress? Are there means for discovering violations and penalties to encourage responsible surveillant behavior?*

Adequate data stewardship and protection: *can the security of the data be adequately protected?*

Equality-inequality regarding availability and application:

a) *is the means widely available or restricted to only the most wealthy, powerful or technologically sophisticated?*
b) *within a setting is the tactic broadly applied to all people or only to those less powerful or unable to resist*
c) *if there are means of resisting the provision of personal information are these equally available, or restricted to the most privileged?*

The symbolic meaning of a method: *what does the use of a method communicate more generally?*

The creation of unwanted precedents: *is it likely to create precedents that will lead to its application in undesirable ways?*

Negative effects on surveillors and third parties: *are there negative effects on those beyond the subject?*

C. Uses

Beneficiary: *does application of the tactic serve broad community goals, the goals of the object of surveillance or the personal goals of the data collector?*

Proportionality: *is there an appropriate balance between the importance of the goal and the cost of the means?*

Alternative means: *are other less costly means available?*

Consequences of inaction: *where the means are very costly, what are the consequences of taking no surveillance action?*

Protections: *are adequate steps taken to minimize costs and risk?*

Appropriate vs. inappropriate goals: *are the goals of the data collection legitimate?*

The goodness of fit between the means and the goal: *is there a clear link between the information collected and the goal sought?*

Information used for original vs. other unrelated purposes: *is the personal information used for the reasons offered for its collection and for which consent may have been given and does the data stay with the original collector, or does it migrate elsewhere?*

Failure to share secondary gains from the information: *is the personal data collected used for profit without permission from, or benefit to, the person who provided it?*

Unfair disadvantage: *is the information used in such a way as to cause unwarranted harm or disadvantage to its subject?"*

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

B. Security Working Group

Question 4

Should a Security Working Group be formally established and maintained?

We think establishing and maintaining a Security Working Group (SWG) would be beneficial to provide the Operating Committee (OC) with expert knowledge on the information security and privacy subject. We also envisage the SWG to take a 'check-and-balance' role alongside the CISO from CAT Processor. The diversified mix of SWG and OC should consist of not only participants or stakeholders that currently required submission of data to CAT, but also include non-contracting parties, such as academia and 'other' civic communities. SWG and OC should not be a private party among elites, SWG and OC should welcome tier 2 and 3 firms to join, as well as observe international best practices. The purpose of SWG and OC is to prevent massive government surveillance from inflicting damage[18] on anyone alongside the industry' value chain smile curve[19] as well as the general public. It would be our honor if given the opportunity to serve in SWG or OC.

Question 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.

No. It is not just about expertise in information security and privacy, but also ethical/ civic concerns that this SWG and OC ought to address. Please see our respond to Question 4.

Question 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?

Not sufficient, please refer to ***Table 1*** and our respond to Question 3.

[18] https://iea.org.uk/wp-content/uploads/2016/07/THE%20MYTH%20OF%20SOCIAL%20COST.pdf
[19] https://www.linkedin.com/pulse/smile-curve-changes-securities-value-chain-evolves-kelvin-to/

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Question 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?

It is interesting that the Commission allows themselves to attend all meetings of the SWG as observers, when there is likelihood that SWG may review system log records to assess if there might be potential abusive usage of CAT by allegedly a Commission staff. Yet, the Commission limits the SWG access to CAT data per footnote 33 of the SEC's proposal. To earn public trust on CAT, the first priority is to allow the public to scrutinize of government agencies and SROs' actions, not the other way around. Please refer to our respond to Question 3 regarding civic concerns of massive government surveillance.

Question 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?

If SWG and OC are representative of public interests rather than just 'participants' from the Exchanges, they should have rights to challenge anything that deems inflicting damage on 'others' as a result of inappropriate use or negligence in design of CAT. We are against limiting SWG or OC's scope to any list of specific issues.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

C. Secure Analytical Workspaces

The proposed definition of SAW is problematic. For civic concern of massive government surveillance[8], the defined purposes of accessing CAT should be much narrower than the broadly defined "regulatory purposes". 'Online targeted query' seems reasonable under certain conditions, while UDDQ and bulk extraction should be avoided whenever and wherever possible. Please refer to our 'A through Z' suggested clauses in ***Table 1***, points D, H, I, J, M and O in particular.

1. Provision of SAW Accounts

Question 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?

Regarding the proposed amendment for provision of SAW accounts, we are not sure what constitute as "implements all common technical security controls required by the CISP" and how it would be enforced. The nine groups of participants may each have their own SAW(s). Also, security and privacy controls would always be a race against hackers, setting a minimum standard rather than pursuing the best defense would introduce opportunities for the hackers. By the time the participants agreed to a "common" SAW, the techniques may have been obsoleted.

Modern surveillance is able to discover intelligence through deploying "agents", in-memory forensic, and/or uses other techniques across decentralized or distributed networks to pick up 'bits-and-pieces' to knit the big picture. Going to a central vault via a centralized SAW is not only outdated but it is also a target attracting hackers to treasure hunt.

Question 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.

It is highly possible. Once a hacker is inside SAW, it is up to the other controls to make it sufficient hard or not enough time for the hacker to inflict any damage, as well as pessimistically, minimize loss when all else failed. Thus, even inside SAW, we recommend protocols to address security risks for data-in-motion, in-use, at-rest, disposal, and restrict the volume and frequency of data queries for 'specific case investigation' or 'rule enforcement' purpose, etc. Please refer to our 'A through Z' suggested clauses in ***Table 1***.

Question 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,

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

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?

As long as CAT remains a gigantic vault, access to the vault would always be a complicated question. One can set up the best structural controls, multi-layers of defenses and what not. Yet, hackers are equally familiar with these structural parameters, if not smarter. A well-organized and standardized approach to privacy and security control is NOT better than data obfuscation through random. So, an alternate approach to security control is called "chaos" (i.e. without a known structure). As an analogy, port cities would make their streets like a maze to deter pirates and other adversaries. The more organized things are, the easier it is for hackers to crack down patterns in breaching controls. Chaos or "unknown unknowns" would significantly heighten the difficulty of access. Remember, hackers steal what is easy and "common".

Question 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?

Share SAW account?! Share access is a common threat that introduces opportunities for hackers. Participants better discuss among themselves how do they plan on using or not using CAT. Asking this question at this time is like the plane already taken flight while the engineers are still trying to figure out how to assemble the parts in the air.

Question 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.

Not necessary, see our respond to Question 11.

Question 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.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

This is a moot point depends on case-by-case how the participants and the processor may permit different access techniques to SAW. There are pros and cons to different access techniques. Be mercy to the CISO of CAT Processor.

Question 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?

There is no free lunch. Yet, who is bearing the cost of CAT ultimately? Before moving forward on any initiative that will add any additional cost to the CAT project, policy makers should access the related impacts or potential adverse consequences to the industry value chain smile curve.[19]

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

2. Data Access and Extraction Policies and Procedures

Question 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.

It is understandable to have privacy and security concerns with Big Data. However a complete lock down from extracting any Big Data intelligence would affect the effectiveness of CAT for market surveillance purpose. On the other hand, continuous building of data controls and governance policies and procedures may unintentionally create big bureaucracy overtime. It affects operations efficiency while the privacy and security controls are not necessarily any more effective than a little chain.

Question 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?

It is either 'end-to-end' protection of every data-in-motion in-and-out and within CAT, or else do not border to create bureaucratic policies and procedures. Hackers are known to exploit any unclosed backdoor(s) that invites them in. SAW permitting bulk extraction or redundant copies of data or recycle of data are examples of wide open backdoors. Rather than relying on a static written policy and procedures, CISO of CAT should consider dynamic approaches to winning the race against hackers. If CISP is mandated to establish formal policies and procedures, then please refer to footnote 9 and our 'A through Z' suggested clauses in ***Table 1***.

Question 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

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

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?

We favor RTAP to help conduct automated surveillance at high "velocity" efficiency rather than "subjective" to user defined queries or bulk data extraction. UDDQ and bulk extraction increase the vulnerability of data being misused for impermissible purposes. Automated checking of trade irregularities according to certain "defined purposes" would improves "objectiveness" of the surveillance scan. See ***Table 1*** points Q, R, and T in particular.

Question 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.

See ***Table 1*** point R in particular.

Question 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?

Bulk data extraction should generally be prohibited, except during 'market crash' with special authorization from the SEC. See ***Table 1*** point T in particular.

Question 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

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

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.

CAT should minimize 'data-in-motion' whenever and wherever possible. File sharing should generally be prohibited. Whenever and wherever the data is consumed or 'in-use', it has to serve 'defined purpose(s)' and be at a 'secured environment'. See ***Table 1*** points A and B in particular.

Question 22

The proposed amendments require the CCO, in collaboration with 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.

See our respond to Question 7.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

3. Security Controls, Policies, and Procedures for SAWs

Question 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.

Please refer to footnote 9 and our 'A through Z' suggested clauses in ***Table 1***.

Question 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.

Please refer to footnote 9 and our 'A through Z' suggested clauses in ***Table 1***.

Question 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?

Please refer to footnote 9 and our 'A through Z' suggested clauses in ***Table 1***.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

4. Implementation and Operational Requirements for SAWs

a. Implementation Requirements for SAWs

Question 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?

Development and maintenance of detailed design specifications sounded good. Yet, 'secure' may sometimes be in conflict with 'consistent', and often observed to be 'inefficient' in real-life practices. According to the CAP theorem,[20] one can only achieve two of the three attributes concurrently but not all three at the same time. See ***Table 1*** point U in particular.

Question 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.

The more parties having access to the full design specifications, the more vulnerability CAT will be. Secrets must be well kept. No single party would have the full design specifications. For checks-and-balance, the design should be broken into partial pieces that no single developer or any trusted party would be able to know the other portions of the CAT design.

Question 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.

Automated monitoring is generally better in efficiency and effectiveness than relying on human. Yet, hackers might be able to decipher and identify patterns of these "standardized" automated monitoring protocols overtime. Irrational behaviors of human being might be hard for hackers to predict or by-pass certain random or ad-hoc scrutiny initiated by human. In short, we recommend both manual and automated processes to augment weakness of each other. Regarding NIST SP800-53, please refer to footnote 9 and our 'A through Z' suggested clauses in ***Table 1***.

Question 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

[20] https://www.ibm.com/cloud/learn/cap-theorem

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

should be used, please identify the format that the detailed design specifications should be provided in and explain why that format is appropriate.

There are pros and cons with unified format. "Non-compatible" format is indeed a way to enhance security.

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

It is not appropriate for the Plan Processor to make a determination of whether Participant's SAW has achieved compliance standards. If CAT system and Stock Exchange's systems are on equal footing to be considered as national critical infrastructures under NIPP,[21] then the SEC and the Plan Processor should partner with CISA to put in place appropriate defense measures instead of setting its own cybersecurity rules.

"Evaluation (or not) before SAW connects with Central Repository" depends on many factors. The detailed design specifications required by Section 6.13(b)(ii) is not an appropriate benchmark, please refer to footnote 9 and our 'A through Z' suggested clauses in ***Table 1*** for explanations.

The diversified represented OC should be notified if their role is served as civil rights monitoring to ensure massive government surveillance would not be inflicting damage[18] on anyone alongside the industry' value chain smile curve.[19]

b. Operation of the SAWs

Question 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?

[21] https://www.cisa.gov/national-infrastructure-protection-plan

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Participant's SAW ought to be monitored, but the Plan Processor might not be the best party to perform the monitoring function. It should be an independent party commissioned by the OC to carry out appropriate reviews and assessments. Regarding NIST SP 800-53, please refer to footnote 9 and our 'A through Z' suggested clauses in ***Table 1***.

Question 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?

See our respond to Question 31 and please refer to our 'A through Z' suggested clauses in ***Table 1***.

Question 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 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.

See our respond to Question 31 and please refer to footnote 9 and our 'A through Z' suggested clauses in ***Table 1***.

Question 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.

Both the monitoring and notification should be performed by an independent third party commissioned by the OC. See our respond to Question 31.

Question 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.

Please refer to footnote 9 and our 'A through Z' suggested clauses in ***Table 1***.

Question 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

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

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?

Again, both the monitoring and notification should be performed by an independent third party commissioned by the OC instead of the Plan Processor. In case of a dispute, the OC may seek second opinion from another independent third party to perform another review.

Question 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.

'Prompt' remediate is the wrong security concept. Non-compliance ought to cut-off immediately rather than allowing tolerance. It is better to thoroughly review and make permanent fix rather than rush through remediation. To ensure other areas would not be affected due to a particular non-compliance, the end-to-end system ought to be tested as soon as discovery of non-compliance, as well as after every attempt to apply fix. No access is allowed before satisfactory testing is completed. See ***Table 1*** point Y.

Question 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?

This is a moot point depends on case-by-case how the participants and the processor may permit different access techniques to SAW. There are pros and cons to different access techniques. Be mercy to the CISO of CAT Processor.

Question 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.

Please refer to ***Table 1*** points Q, R, S, and T in particular.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

5. Exceptions to the SAW Usage Requirements

a. Exception Process for Non-SAW Environments

Question 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?

No exception in general, except during market crash with special authorization from the SEC. Please refer to ***Table 1*** point T in particular.

Question 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.

It is better than before, but CAT should consider additional privacy and security protections to enable surveillance intelligence without crossing the line of privacy hazard. Please refer to ***Table 1*** point G in particular.

Question 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?

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

No. Please see our respond to Question 30 and Question 31.

b. Is it appropriate to require that the proposed security assessment 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 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.

   No. Please refer to footnote 9 and our 'A through Z' suggested clauses in ***Table 1***.

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?

   No, CAT data should not be exported in general. Export, UDDQ, and bulk extraction are indeed 'data-in-motion' which should be minimized whenever and wherever possible. Allowing CAT data be in-use at possible non-secure environment and/or for non-defined purposes is dangerous and would also trigger 'function creep' and civic concerns. Redundant copies of data increases possibility of 'function creep'. Please refer to ***Table 1*** points A, B, C, D, H, I, J, M, and O in particular.

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?

   If it is not 'end-to-end' protected and tested to ensure every data-in-motion, in-use, at-rest, and proper disposal in-and-out and within CAT, CAT should not be up in operations. Hackers are known to exploit any unclosed backdoor(s) that invites them in. So, there should only be one milestone in theory – i.e. CAT is secured. In case of any dispute, the OC may seek second opinion from another independent third party to perform another review.

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.

   How one behaves when no one is watching often reveal the most of the person's character. Same goes with assessing security of a system, we recommend surprise checks and ethical hacking.

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?

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Reference to our respond to Question 27, the more parties having access to the full design specifications, the more vulnerability CAT will be. Secrets must be well kept. No single party would have the full design specifications. For checks-and-balance, the design should be broken into partial pieces that no single developer or any trusted party would be able to know the other portions of the CAT design. Makers of privacy and security controls should preserve their secrets. Checkers should independently conduct their testing, include ethical hacking. That being said, Control Makers should share some high level infrastructure setup (without unveiling critical secrets) with the Checkers to allow the checkers to apply analytical procedures and plan for relevant tests.

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.

A general rule of thumb is no exception. Requiring a Participant seeking an exception from the proposed Secure Analytical Workspace usage requirements to provide the SWG with specified application materials may indeed encourage exceptions. The only exception allows should be during market crash with special authorization by the SEC. Last but not least, the fewer parties having access to the application materials or design specifications the better, the current list of recipients is too much.

Question 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.

No. Please see our respond to Question 30 and Question 31.

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

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

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?

No. We recommend using independent third party as reviewer and directly accountable to OC. So, OC would be the first to be notified. Please see our respond to Question 30 and Question 31.

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.

The Plan Processor's CISO is assumed to be the Chief Maker of Privacy and Security Controls embedded in CAT design and the related connections. So, it is inappropriate for him/her to also be the Checker. Given the CCO is also a staff member of the Plan Processor, the independence to make a determination may be questionable. Again, an independent third party should be commissioned by the OC. OC would making a reasonable determination within reasonable time on a case-by-case basis, but not necessarily set at 60 days duration.

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?

Again, it is inappropriate for the Plan Processor's CISO or CCO to take up the Checker's role when they are the Maker whom designed the CAT.

Question 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.

No, the burden of proof should be on the Checker. See our respond to Question 42 part f.

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.

Exception should be discouraged. Giving leeway to permit exception under conditions introduces opportunities for hackers. The only authority that can grant an exception is the SEC during market crash, and we think such authority cannot be transferred or assigned.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

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.

   The Plan Processor's CISO and CCO may change job causing an "I'll be gone or you'll be gone" situation. Also, we have seen the previous Plan Processor being replaced by FINRA. With that in mind, it is inappropriate to entrust any individual staff at the Plan Processor to make determination to accept or tolerate risk for and on-behalf of the entire industry when everyone's trade data is at stake. We think it would require a unanimous recommendation for exception by the OC, and then a formal vote by the SEC to properly authorize any exception. Besides, exception should only be permissible during 'market crash' and for 'market surveillance' purpose (see ***Table 1*** points S and T).

Question 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?

Again, this should be the job of an independent checker commissioned by the OC, not the Plan Processor's CISO or CCO. OC should be the first to be notified.

Question 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

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

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?

We have make it clear that no exception in general. Any exception would have to overcome the barriers as set out in our respond to Question 44 part c.

Question 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.

We have make it clear that no exception in general. Any exception would have to overcome the barriers as set out in our respond to Question 44 part c.

Question 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.

Considering a 'revoking process' indeed implies a weak security control sense to permit exception during normal course of business. We have make it clear that no exception in general. Any exception would have to overcome the barriers as set out in our respond to Question 44 part c. Make determination based on a well-articulated self-assessment may be a false sense of security. Checker ought to perform his/her own independent review (include ethical hacking) rather than rely on a Participant to submit a security assessment.

Question 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?

The Plan Processor's CISO and CCO roles as proposed are inappropriate. The idea of considering possible exceptions and a revoke process indeed reflects a weak sense of security. See our respond to Question 48.

Question 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?

We think any exception would have to overcome the barriers as set out in our respond to Question 44 part c.

Question 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

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

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.

Regardless of new application for exception or renewal request, make determination based on a well-articulated self-assessment may be a false sense of security. Checker ought to perform his/her own independent review (include ethical hacking) rather than rely on a Participant to submit a security assessment or additional materials. Nevertheless, exception should only be permissible during the brief period of 'market crash'. Once the period is over, the exception should automatically be lapsed and the data must be automatically eradicated per ***Table 1*** point C.

Question 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.

Again, the Plan Processor's CISO and CCO roles as proposed are inappropriate. The idea of considering possible exceptions for a continuous period other than during a 'market crash' indeed reflects a weak sense of security. See our respond to Question 48.

b. Operation of Non-SAW Environments

Question 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.

The proposed definition of SAW is problematic. For civic concern of massive government surveillance[8], the defined purposes of accessing CAT should be much narrower than the broadly defined "regulatory purposes". Regardless of SAW or non-SAW, UDDQ and bulk extraction should be avoided whenever and wherever possible. Please refer to our suggestions in ***Table 1***, points D, H, I, J, M and O in particular.

Question 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 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.

SAW and non-SAW ought to be monitored, but the Plan Processor might not be the best party to perform the monitoring function. It should be an independent party commissioned by the OC to carry out appropriate reviews and assessments. Please see our respond to Question 30, Question 31, and part c of Question 43 and Question 44.

Question 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.

Please see our respond to Question 30, Question 31, Question 43 part c, Question 44 part c, and Question 54.

Question 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.

The diversified represented OC should be notified if their role is served as civil rights monitoring to ensure massive government surveillance would not be inflicting damage[18] on anyone alongside the industry' value chain smile curve.[19] See ***Table 1*** point D.

Question 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.

Principle based rather than over prescriptive reference to NIST revision 4 of SP800-53 is better. See footnote 9 and ***Table 1***.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Question 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.

'Prompt' remediate is the wrong security concept. Non-compliance ought to cut-off immediately rather than allowing tolerance. It is better to thoroughly review and make permanent fix rather than rush through remediation. To ensure other areas would not be affected due to a particular non-compliance, the end-to-end system ought to be tested as soon as discovery of non-compliance, as well as after every attempt to apply fix. No access is allowed before satisfactory testing is completed. See ***Table 1*** point Y.

Question 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.

It should be the independent party commissioned by the OC to send out simultaneous notifications.

Question 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.

For civic concerns, no access to CAT for 'market surveillance' purpose prior to identifying symptoms of irregularity that are substantiated by data at SIPs and/or analytical procedures at SROs/ the SEC. See ***Table 1*** points M and S, and ***Figure 2***.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

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

Question 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?

200,000 records would never be enough to scrutinize the larger firms, causing a 'too big to exam' scenario. It would be discriminative to smaller firms or non-HFTs. See ***Table 1*** point R for our counter suggestion.

Question 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?

We are okay with this definition as long as there are some ways to capture or timely logged audit trails of all users' activities in CAT systematically. See ***Table 1*** point N.

Question 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?

Literally everything, include every keystroke should be logged using keylogging techniques.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

E. CAT Customer and Account Attributes

1. Adopt Revised Industry Member Reporting Requirements

Question 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?

Customer and Account Attributes are considered 'sensitive'. It must be obfuscated at all time ('at-rest or 'in-motion') except when it is 'in-use'. Therefore, whenever alternate surveillance method is available, CAT should refrain from collecting or querying sensitive data. See ***Table 1*** point G.

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

Question 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.

CAIS or PII or any data similar to that nature are deemed sensitive. If there is a way(s) to enable surveillance intelligence[10] without crossing the line of privacy[11] hazard, CAT must adopt.

Question 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.

In general, CAT should not be collecting, accessing or querying CAIS or other sensitive data except for gathering evidence for prosecution of alleged rule violation only.

Question 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?

CCID subsystem should ideally be shut completely when alternate method is available to subpoena evidence for prosecution of alleged rule violation. For CCID subsystem to be considered secured, it needs to satisfy all 'A through Z' criteria set out in ***Table 1***.

Question 68

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

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Mathematical logic to scramble data and partial masking of SSN are ways to do obfuscation. We recommend applying a mix of other security control techniques where applicable, such as introduce random, roll-up aggregation, segregate sensitive data with other data, etc. Besides, maze or chaos is somehow more effective than structural controls. Indeed, our proposed ***Figure 2*** encompasses abilities to pick up bits-and-pieces of intelligence in real-time from chaotic or widely distributed sources of data and knitting them together. It is more resilient than a gigantic data vault.

Question 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?

No, the more details to disclose how the obfuscation is done, the weaker the form of control it is. To best kept a secret is to not tell anybody and "silent" the secret creator via high incentives (☺ hopefully no one would use threat or harm the person physically). How the Transformed Value would be used should comply with our suggested clauses in ***Table 1***.

Question 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.

It should not be made available to Regulatory Staff for "queries". Law enforcers may only subpoena sensitive private information as evidence when there is reasonable ground to substantiate a prosecutable alleged crime. If the use of CAT data is for general market surveillance purpose, roll-up aggregated data is more than sufficient to fulfill regulatory purpose. Do not forget, there are the revolving doors that regulatory staffs may join the industry, and elite firms are also sponsors to Stock Exchanges. When CAT appears to have no effective way to avoid 'function creep', if granting access to these sensitive information may implicitly be given the elite firms a potential unfair advantage.

Question 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.

Why should industry members bear any cost or effort to CCID subsystem? Obfuscation serves no value to them. Ultimately such cost would cascade down to investors and creating barriers of entry. We argue that privacy information should not even be collected in the first place unless there is reasonable ground to substantiate a prosecutable alleged crime.

Question 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.

The more details to disclose the process of machine-to-machine processing, the weaker the form of control it is. It will invite opportunities for the hackers.

Question 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.

Segregation of duties is good, but 'partitioning' alone would never be effective mechanism for security control. See our 'A through Z' suggestions in ***Table 1***.

Question 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.

No, standards are 'recognizable patterns' that hackers like and capable to by-pass related controls. 'Completeness' rather than 'omission' or 'random' may be a sign of security weakness. Besides, with regards to Big Data, we prioritize timeliness over veracity.[17] Perfect accuracy or golden-source of data is merely well-articulated "promotes" to sell data-vault storage products, rather than a true pursuit of big data.

Question 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.

Annual assessment should be done by an independent third party commissioned by the OC. Participants as Users of CCID subsystem should refrain from being the Checkers at the same time.

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

Question 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

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

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.

Based on what are being provided in these sections, the OC should reject and call for a halt of CAT.

Question 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 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.

With respect to CCID subsystem's functionalities, see our respond to Question 67 and Question 68.

4. Reporting Transformed Value

Question 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.

Customers have rights to object sharing of privacy information with other parties other than their service providers, unless being subpoena by court.

5. Data Availability Requirements

Per ***Table 1*** point Q, use of 'predefined automated analytical steps' instead of ad-hoc data query wherever possible. 'Predefined automated analytical steps' require proper testing and authorization by Operating Committee.

6. Customer and Account Attributes in CAIS and Transformed Values

Question 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.)?

Prosecutors may ask for these details in subpoena, but it should not be made available for "query" as we foresee privacy objection from the civic communities. Given all working population would likely have a retirement or investment account, CAT is essential a massive government surveillance without obtaining the proper consents by ordinary citizens.

Question 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,

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

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?

See our respond to Question 79.

Question 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.

See our respond to Question 79.

Question 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?

Whatever refresh update or other ways to enable surveillance intelligence should not cross the line of privacy hazard.

7. Customer-ID Tracking

Question 83

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

Learn to work with messiness of data and be respectful of privacy ordinance is the beginning of wisdom for ethical surveillance of big data intelligence.

8. Error Resolution for Customer Data

Question 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.

See our respond to Question 79 and Question 83.

Question 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?

See our respond to Question 79 and Question 83.

Question 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?

See our respond to Question 79 and Question 83.

Question 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.

Do not correct. Perfect accuracy or golden-source of data is merely well-articulated "promotes" to sell data-vault storage products, rather than a true pursuit of big data. Big Data prioritizes velocity (real-time) over veracity.[17] See our respond to Question 79 and Question 83.

9. CAT Reporter Support and CAT Help Desk

Question 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.

Instead of asking the Plan Processor to provide helpdesk support to CAT reporters, broker-dealers would much rather want reliefs to their compliance burdens. See ***Figure 1*** for our counter suggestions (using RTAP at original data sources and the analogy from IRS - 'My Free Taxes' initiative).[5] Our suggested 'predefined automated analytical steps' (see ***Table 1*** point Q) enhance security and allows regulators to focus on those high-risk candidates for scrutinized exams while majority of good citizens get their reliefs.

Question 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?

Understand, acknowledge and respect the civic concerns regarding massive government surveillance[8] should be the priority "help" that the SEC and the Plan Processor can offer.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

F. Customer Identifying Systems Workflow

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

Question 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.

'Partitioning' alone would never be effective mechanism for security control. See our 'A through Z' suggestions in ***Table 1***. Besides, PII should not be captured in the first place. See our respond to Question 79 and Question 83.

Question 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?

CAIS must not be included anywhere in CAT. The obfuscated CCID must follow the 'A through Z' protocols as suggested in ***Table 1*** whether it is 'in-motion', 'at-rest', 'in-use', or 'in disposal'.

Question 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.

There should not even be a Customer Identifying System. It invites opportunities for hackers. See our respond to Question 79 and Question 83.

Question 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

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

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.

Participants self-assessing information security has nothing to do with CAT. They are Users of CAT, and therefore they should not be Checkers at the same time. The job should be done by independent third party commissioned by the OC.

Question 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.

Literally everything, include every keystroke should be logged using keylogging techniques.

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

Question 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.

There should not even be a Customer Identifying System. It invites opportunities for hackers. See our respond to Question 79 and Question 83.

Question 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.

See our respond to Question 79 and Question 83.

Question 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.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

'Least privileged' is not the same as 'no privilege'. Prosecutors may ask for these details via subpoena, but never "query" or share privacy information without individual's consent. See our respond to Question 79 and Question 83.

Question 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.

Role Based Access Model or whatever other security measures would likely not be in compliance with privacy ordinance. Learn to deal with messiness of data[10] is the only way out to ethically enable surveillance intelligence without crossing the line of privacy hazard. We look forward to engage in any opportunities where our expertise might be required.

Question 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.

Instead of the proposed "need to know" basis, the proper standard should be to go through a court subpoena process to obtain privacy information if CAT is unwilling to learn the ethical way to deal with messiness of data.

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

Anything could be for 'regulatory purpose', the permissible 'purposes' need to be confined, see ***Table 1*** points H, I, J, M, and S.

Question 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?

There should not even be a Customer Identifying System. It invites opportunities for hackers. See our respond to Question 79 and Question 83.

Question 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.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

No, absolutely not. Both methods are intrusive and allegedly are not in compliance with the privacy ordinance. See our respond to Question 79 and Question 83.

Question 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?

Customers have rights to object sharing of privacy information with other parties other than their service providers, unless being subpoena by court. Neither the Commission nor the Plan Processor has right to access privacy information without consent or proper subpoena. If SWG and OC are representative of public interests rather than just 'participants' from the Exchanges, they should have rights to challenge anything that deems inflicting damage on 'others' as a result of inappropriate use or negligence in design of CAT.

4. Manual CAIS Access

Question 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.

Manual CAIS Access might be appropriate only when there is proper subpoena with valid 'defined purposes' (not any regulatory purpose).

Question 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.

No, CAIS may not be access or collect anytime other than law enforcers obtained proper subpoena.

Question 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.

See our respond to Question 104 and Question 105.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Question 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.

No, there should not be manual CAIS access at all. Use alternate means to subpoena privacy information as fit, or learn to deal with messy and incomplete data.

Question 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.

See our respond to Question 104 and Question 105.

Question 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.

See our respond to Question 104 and Question 105.

5. Manual CCID Subsystem Access

Question 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.

A possible permissible way to scrutinized suspicious activities conducted by rogue traders is by using recognized trade patterns to approximate who the rogue traders might be. Transforming CAIS to CCID would not be sufficient to overcome civic objection to unauthorized collection or possession of privacy information.

Question 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.

Neither the Commission nor the Plan Processor has right to access any ITIN(s)/SSN(s)/EIN(s) without consent or proper subpoena. See our respond to Question 79, Question 83, and Question 103.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Question 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.

See our respond to Question 79, Question 83, and Question 103.

Question 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?

Why should industry members bear any cost or effort to CCID subsystem or allow Transformation Logic be embedded in the client-side code? Obfuscation serves no value to them. Ultimately such cost would cascade down to investors and creating barriers of entry. We argue that privacy information should not even be collected in the first place unless there is reasonable ground to substantiate a prosecutable alleged crime. Besides, there is no reason to capture privacy information in CAT when other mean is available to subpoena the privacy related 'evidence' for suspicious activities or alleged crime.

Question 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.

See our respond to Question 79, Question 83, and Question 103.

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

Question 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?

Regardless of programmatic access or manual access, CAIS and CCID as proposed are inappropriate. See our respond to Question 79, Question 83, and Question 103.

Question 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?

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

A possible permissible way to scrutinized suspicious activities conducted by rogue traders is by using recognized trade patterns to approximate who the rogue traders might be. Transforming CAIS to CCID would not be sufficient to overcome civic objection to unauthorized collection or possession of privacy information.

Question 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.

The only valid explanation is a subpoena; all other request for privacy information should be rejected.

Question 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.

Market surveillance should not be discriminative against any single entity or individual person. Anything could be for 'regulatory purpose', the permissible 'purposes' need to be confined, see ***Table 1*** points H, I, J, M, and S.

Question 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.

This is a flawed standard because CAIS and CCID as proposed crossed the line of privacy hazard.

Question 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.

Please refer to ***Table 1*** points C and D about 'Function Creep'.

Question 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.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Reference to our respond to Question 27, the more parties having access to the full design specifications, the more vulnerability CAT will be. Secrets must be well kept. No single party would have the full design specifications. For checks-and-balance, the design should be broken into partial pieces that no single developer or any trusted party would be able to know the other portions of the CAT design. Makers of privacy and security controls should preserve their secrets. Checkers should independently conduct their testing, include ethical hacking. That being said, Control Makers should share some high level infrastructure setup (without unveiling critical secrets) with the Checkers to allow the checkers to apply analytical procedures and plan for relevant tests. Last but not least, the Commission is a User of CAT, hence should not be the Checker at the same time.

Question 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.

It is unacceptable to allow anyone to access privacy information without proper consent or subpoena. See our respond to Question 79, Question 83, and Question 103.

Question 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.

It is inappropriate to entrust any individual staff at the Commission to make determination to accept or tolerate risk for and on-behalf of the entire industry when everyone's trade data is at stake. We think it would require a formal vote by the SEC to properly authorize access during 'market crash' only (see ***Table 1*** points S and T).

Question 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 believe 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.

45 days is too wide a window, it should limited to the hours during a 'market crash' and at most the day after, as well as having the data purged or disposed properly and immediately after used.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

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

This is unacceptable, and it opens the floodgate to 'function creep' and impairment of ordinary citizen's privacy rights. See our respond to Question 79, Question 83, Question 103, Question 123, and Question 124.

7. Programmatic CAIS Access

Question 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.

For civic concerns, no access to CAT for non-defined purposes prior to identifying symptoms of irregularity that are substantiated by data at SIPs and/or analytical procedures at SROs/ the SEC. See ***Table 1*** points M and S, and ***Figure 2***. It is unacceptable to allow anyone to access privacy information without proper consent or subpoena. See our respond to Question 79, Question 83, and Question 103.

Question 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.

Learn to deal with messiness of data[10] is the only way out to ethically enable surveillance intelligence without crossing the line of privacy hazard. We look forward to engage in any opportunities where our expertise might be required.

Question 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.

See our respond to Question 126 and Question 127.

8. Programmatic CCID Subsystem Access

Question 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.

A possible permissible way to scrutinized suspicious activities conducted by rogue traders is by using recognized trade patterns to approximate who the rogue traders might be. Transforming CAIS to CCID would not be sufficient to overcome civic objection to unauthorized collection or possession of privacy information.

Question 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?

For civic concerns, no access to CAT for non-defined purposes prior to identifying symptoms of irregularity that are substantiated by data at SIPs and/or analytical procedures at SROs/ the SEC. See ***Table 1*** points M and S, and ***Figure 2***. It is unacceptable to allow anyone to access privacy information without proper consent or subpoena. See our respond to Question 79, Question 83, and Question 103.

Question 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.

See our respond to Question 129 and Question 130.

G. Participants' Data Confidentiality Policies

1. Data Confidentiality Policies

Question 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?

No, it is definitely insufficient, see earlier sections for explanations.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Question 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?

No, it is definitely insufficient, see earlier sections for explanations.

Question 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?

See the 'A through Z' suggested clauses in ***Table 1***.

Question 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?

Security and privacy controls are much broader than data loss protection, encryption, and availability restriction, etc. See the 'A through Z' suggestions in ***Table 1***.

Literally everything, include every keystroke should be logged using keylogging techniques.

Question 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?

Participants as free enterprises should have freedom to adopt whatever security and privacy policies. That being said, regulators can rebuke its effectiveness and impose fines. Besides, if CAT system and Stock Exchange's systems are on equal footing to be considered as national critical infrastructures under NIPP,[21] then the SEC and the Plan Processor should partner with CISA to put in place appropriate defense measures instead of setting its own cybersecurity rules.

Question 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?

No. See ***Figure 2*** for our suggestions to drastically reduce CAT data to the "true" minimum amount of data necessary to achieve essential 'defined purposes'. The benefits of our suggested approach are:

(a) dramatically reduce CAT footprint or data storage and traffic by avoiding unnecessary redundant copies of data and minimize 'data-in-motion';
(b) confine access to CAT data to 'targeted search' of relevant data that fits the 'defined purposes'; and

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

(c) better intelligence for market monitoring by enabling and rewarding the crowd for identifying early warning signals to potential flash crash or other trade irregularities (see our comments[14] to the SEC regarding 'CT Plan'[15] for further details).

Question 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?

Literally everything, include every keystroke should be logged using keylogging techniques.

Question 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?

See our respond to Question 140.

2. Access to CAT Data and Information Barriers

a. Regulatory Staff and Access to CAT Data

Question 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?

The definition of Regulatory Staff is too board. Staff may change job causing an "I'll be gone or you'll be gone" phenomenon. With that in mind, it is inappropriate to entrust any individual staff to make determination to accept or tolerate risk for and on-behalf of the entire industry when everyone's trade data is at stake. Rely on security and privacy control processes and/or "chaos" is better than entrusting a particular person with too much power.

To effectively mitigate privacy and security risks without creating bureaucracy, do keep in mind the following three management fundamentals: (i) segregation of duties[12], (ii) keep clean with high incentives (e.g. whistleblower award), and (iii) precognitive prevention by reducing the amount of unknown unknowns[13]. We envisage a crowd model to reduce unknown unknowns while enhance security of CAT, see ***Figure 2***.

b. Information Barriers

"Implement effective information barriers between such Participants' Regulatory Staff and non-Regulatory Staff with regard to access and use of CAT Data" will not enhance security of CAT. The distinction should not be drawn between the person being a regulatory staff or not. Segregation of duties is about segregating the function of Maker (designer of CAT security and privacy controls) with the Checker (independent assessor commissioned by the OC). Regulatory staffs are indeed Users of CAT, which should be a subject for scrutiny on potential 'function creep' or other breach of security and privacy controls.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

c. Access by Non-Regulatory Staff

Question 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?

Independent third party commissioned by the OC to conduct security and privacy may be the only exception to non-Regulatory Staff access to CAT, the independent assessor may perform ethical hacking in attempt to access mocked or oldest archives but not the live CAT data in production. These so called "specific regulatory need for access" other than what we suggested in ***Table 1*** as 'defined purposes' should be impermissible. The more exceptions grant, the higher vulnerability of CAT.

d. Training and Affidavit Requirements

Question 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?

Signing an affidavit means nothing when individual lack the ability to shoulder the liabilities of possible compromise of security and privacy risks. "All staffs are 100% trained on company's security policy" may appear nice on the paper, but it is common for many seniors to designate their secretaries to attend the training on their behalf. Training is a minor control; you want to major in the major, not major in the minor. Therefore, take a step back and consider your organization as a chain of capabilities. Who has the knowledge across most of these capabilities? Who are in control over most of the resources? Who can easily steal using their authorities, knowledge, and controlled resources? Help these middle and senior management resist the temptations of wrong doing with three effective methods: (i) segregation of duties[12], (ii) keep clean with high incentives (e.g. whistleblower award), and (iii) precognitive prevention by reducing the amount of unknown unknowns.[13]

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

a. Limitations on Extraction and Usage of CAT Data

Question 136

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

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

For civic concern of massive government surveillance[8], the defined purposes of accessing CAT should be much narrower than the broadly defined "regulatory purposes". No access to CAT for non-defined purposes prior to identifying symptoms of irregularity that are substantiated by data at SIPs and/or analytical procedures at SROs/ the SEC. Please refer to our suggestions in ***Table 1***, points D, H, I, J, M, O, and S and ***Figure 2***. It is unacceptable to allow anyone to access privacy information without proper consent or subpoena. See our respond to Question 79, Question 83, and Question 103.

b. Individual Roles and Usage Restrictions

Question 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?

The Plan Processor's CISO is assumed to be the Chief Maker of Privacy and Security Controls embedded in CAT design and the related connections. So, it is inappropriate for him/her to also be the Checker. Given the CCO is also a staff member of the Plan Processor, the independence to make a determination may be questionable. Again, an independent third party should be commissioned by the OC.

c. Policies Relating to Customer and Account Attributes

Question 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?

No, it is inappropriate and unreasonable. Customer and Account Attributes are considered 'sensitive'. It must be obfuscated at all time ('at-rest or 'in-motion') except when it is 'in-use'. Therefore, whenever alternate surveillance method is available, CAT should refrain from collecting or querying sensitive data. See ***Table 1*** point G. CAIS or PII or any data similar to that nature are deemed sensitive. If there is a way(s) to enable surveillance intelligence[10] without crossing the line of privacy[11] hazard, CAT must adopt. In general, CAT should not be collecting, accessing or querying CAIS or other sensitive data except for gathering evidence for prosecution of alleged rule violation only. CCID subsystem should ideally be shut completely when alternate method is available to subpoena evidence for prosecution of alleged rule violation.

For civic concerns, no access to CAT for non-defined purposes prior to identifying symptoms of irregularity that are substantiated by data at SIPs and/or analytical procedures at SROs/ the SEC. See ***Table 1*** points M and S, and ***Figure 2***. It is unacceptable to allow anyone to access privacy information without proper consent or subpoena. See our respond to Question 79, Question 83, and Question 103.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

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

Question 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?

Accountants are not necessary security expert. We are sure that the Commission would not allow favoritism or conflicts of interest situation to happen. Independent assessor should be commissioned by the OC. The assessor's main duty is to ethically break CAT related security and privacy controls (i.e. not to validate any well-articulated written documents against whatever compliance standards).

Question 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 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?

Security and privacy controls are much broader than data loss protection, encryption, and availability restriction, etc. See the 'A through Z' suggestions in ***Table 1***. Again, periodic review should be conducted by independent third party commissioned by the OC. Responsible government should subject itself to scrutiny by the public, therefore regulatory staff access should be part of the subject and scope to be assessed.

Question 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?

Confidentiality policies should be made public. The independent assessor's findings should also be public to allow civic scrutiny of massive government surveillance project, such as CAT would not directly or inadvertently inflicting damage and/or impairing anyone's privacy and other rights.

H. Regulator & Plan Processor Access

1. Regulatory Use of CAT Data

Question 149

There is existing CAT NMS Plan language stating that CAT Data may be used solely for surveillance and regulatory purposes. 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?

Anything could be for 'regulatory purpose', the permissible 'purposes' need to be confined, see ***Table 1*** points H, I, J, M, and S.

Question 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?

Convolution between serving commercial interests and performing designated regulatory purposes pose significant conflicts of interest concern. Besides, "revolving door" is a common civic concern for "I'll be gone or you'll be gone" phenomenon. It is inappropriate to entrust any individual staff to make determination to accept or tolerate risk for and on-behalf of the entire industry when everyone's trade data is at stake.

CAT data should not be used for policy making or SRO rule filing purpose regardless of any conditions or circumstances. There is the danger of discriminatory rule-making if one being tempted to peek at CAT data to pick winners or losers during market reform. Policy making or justice system should be "blind-folded" to who may be gaining or losing in the future, but focus on: (1) the righteousness to uphold the fair, reasonable, and non-discriminatory (FRAND) principles; (2) curb potential conflicts or abuses; (3) effectively and efficiently delineate rights; and (4) ensure seamless operation of the market and lower the overall transaction cost where possible to benefit the general public.

Question 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?

'Least privileged' is not the same as 'no privilege'. Role Based Access Control (RBAC) model is not wrong, but based on our review of the Commission's proposal, the Maker, Checker, and User's roles have been mixed up. "Implement effective information barriers between such Participants' Regulatory Staff and non-Regulatory Staff with regard to access and use of CAT Data" will not enhance security of CAT. The distinction should not be drawn between the person being a regulatory staff or not. Segregation of duties is about segregating the function of Maker (designer of CAT security and privacy controls) with the Checker (independent assessor commissioned by the OC). Regulatory staffs are indeed Users of CAT, which should be a subject for scrutiny on potential 'function creep' or other breach of security and privacy controls. Besides, Prosecutors may ask for privacy information via subpoena, but never "query" or share privacy information without individual's consent. See our respond to Question 79 and Question 83.

2. Access to CAT Data

Question 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?

Independent third party commissioned by the OC to conduct security and privacy may be the only exception to non-Regulatory Staff access to CAT, the independent assessor may perform ethical hacking in attempt to access mocked or oldest archives but not the live CAT data in production. These so called "specific regulatory need for access" other than

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

what we suggested in ***Table 1*** as 'defined purposes' should be impermissible. The more exceptions grant, the higher vulnerability of CAT.

Question 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?

If CAT system is being considered as national critical infrastructures under NIPP,[21] then the SEC and the Plan Processor should partner with CISA to put in place appropriate defense measures, including but not limited to, requiring appropriate security clearance for its contractors.

Question 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.

We agree that in general, 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. We however disagree with the whole proposal about CAIS/ CCID system because of civic concerns with massive government surveillance. It is unacceptable to allow anyone to access privacy information without proper consent or subpoena. See our respond to Question 79, Question 83, and Question 103.

Question 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?

Developers should not use production data, whereas testers would be allowed to conduct tests in both pilot and production environments. Developers should be able to create their own mock up data to replicate data set similar in format but not in any way be indicative of actual production data contents.

Question 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?

Yes for testing, no for development.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Question 157

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

Yes, imposing U.S. citizenship requirements on all administrators or other staff with access to the CAT System and/or the Central Repository is reasonable. If CAT system is being considered as national critical infrastructures under NIPP,[21] then the SEC and the Plan Processor should partner with CISA to put in place appropriate defense measures, including but not limited to, requiring appropriate security clearance as fit for their roles.

I. Secure Connectivity & Data Storage

Question 158

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

Using only private lines alone does not mean secured connectivity. Other security control measures include but not limited to, in-memory forensic.

Question 159

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

The Commission should not attempt to prescribe any particular form of security control measures or best practices. Instead, there should be high-level principles to guide the CAT project to embed essential security, privacy, and analytical frameworks in its design. Hackers would find way to circumvent control measures, such as private line and VPN. After all, security is about winning the race against hackers. Continuous learning and forward looking to reduce the amount of unknown unknowns would be helpful to avoid vulnerability. Please refer to ***Table 1*** point Z.

Question 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?

Do not attempt to be CISA when the SEC is not the country's designated government agency for security.

Question 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?

See our respond to Question 159 and Question 160.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Question 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?

See our respond to Question 159 and Question 160.

Question 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?

Yes, it should be physically located, developed, tested, and maintained within the United States.

Question 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.

See our respond to Question 159 and Question 160.

Question 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.

See our respond to Question 159 and Question 160.

J. Breach Management Policies and Procedures

Question 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?

No, the proposed modification is not appropriate. 'Prompt' remediate is the wrong security concept. Non-compliance ought to cut-off immediately rather than allowing tolerance. It is better to thoroughly review and make permanent fix rather than rush through remediation. To ensure other areas would not be affected due to a particular non-compliance, the end-to-end system ought to be tested as soon as discovery of non-compliance, as well as after every attempt to apply fix. No access is allowed before satisfactory testing is completed. See ***Table 1*** point Y.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Question 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?

Public, including the CAT Reporters have right to know as soon as a breach incident is detected.

Question 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?

See our respond to Question 166.

Question 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?

See footnote 9 and ***Table 1***.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

K. Firm Designated ID and Allocation Reports

Question 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?

There are civic concerns with massive government surveillance.[8] It is unacceptable to allow anyone to access privacy information without proper consent or subpoena. See our respond to Question 79, Question 83, and Question 103.

L. Appendix C of the CAT NMS Plan

We urge the Commission to carefully revisit our comments submitted in 2016[2] regarding Appendix C.

M. Proposed Implementation

1. Proposed 90-Day Implementation Period

Question 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?

CAT should go back to the drawing board and consider our suggestions per ***Figure 1*** and ***Figure 2***.

Question 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?

No, it fails to strike appropriate balance between the regulator's interest to tap into CAT data and addressing the industry's concerns about security and the civic concerns about massive government surveillance. The proposed SAW is problematic. Modern surveillance is able to discover intelligence through deploying "agents", in-memory forensic, and/or uses other techniques across decentralized or distributed networks to pick up 'bits-and-pieces' to knit the big picture. Going to a central vault via a centralized SAW is not only outdated but it is also a target attracting hackers to treasure hunt. Please refer to our comments in C. Secure Analytical Workspaces. CAT should go back to the drawing board and consider our suggestions per ***Figure 1*** and ***Figure 2***.

2. Proposed 120-Day Implementation Period

Question 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?

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

CAT should go back to the drawing board and consider our suggestions per ***Figure 1*** and ***Figure 2***.

3. Proposed 180-Day Implementation Period

Question 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?

See our respond to Question 172. If problems about SAW are not addressed satisfactorily, it should not be implemented. Instead, CAT should go back to the drawing board and consider adopting our suggestions per ***Figure 1*** and ***Figure 2*** in the next 90 to 180 days.

No exception should not be allowed in general, it is inappropriate to entrust any individual staff at the Plan Processor to make determination to accept or tolerate risk for and on-behalf of the entire industry when everyone's trade data is at stake. We think it would require a unanimous recommendation for exception by the OC, and then a formal vote by the SEC to properly authorize any exception.

III. Paperwork Reduction Act

Question 175-178

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.

The proposed collections of information by CAT are NOT necessary for the proper performance of the functions of the agency. The Commission significantly undermined the burden of the proposed collection of information by CAT. Our suggestions per ***Figure 1*** and ***Figure 2*** will enhance the quality, utility, and clarity of the information to be collected. Our suggested approach would also 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. Most importantly, our suggested approach would address any civic concerns about massive government surveillance.[8]

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

IV. Economic Analysis

Question 179-219

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 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?

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

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.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

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?

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

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 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?

The Commission's analysis of the potential effects of the proposed amendments to the CAT NMS Plan is not reasonable. The proposed amendments or the CISP would not improve the effectively and efficiency of CAT implementation, but added unnecessary bureaucracy and burden to all stakeholders. Do not attempt to be CISA when the SEC is not the country's designated government agency for security. The Commission should not prescribe any particular form of security control measures or best practices. Instead, there should be high-level principles to guide the CAT project to embed essential security, privacy, and analytical frameworks in its design. The proposal amendment is backward instead of

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

forward looking (e.g. it referenced to an outdated revision 4 of NIST's SP800-53) or at least not be able to stand the test of time during this brief commenting period. Please see footnote 9 and ***Table 1***.

Convolution between serving commercial interests and performing designated regulatory purposes pose significant conflicts of interest concern. Besides, "revolving door" is a common civic concern for "I'll be gone or you'll be gone" phenomenon. It is inappropriate to entrust any individual staff to make determination to accept or tolerate risk for and on-behalf of the entire industry when everyone's trade data is at stake. The Commission should duly consider the related economic effects of defining the scope of SAW, CAIS, CCID, and overall the information security program – CISP. We disagree with the Commission's assessment of the benefits of the proposed amendments. The Commission's cost estimates are not reasonable because it omitted to account civic concerns about massive government surveillance.[8]

We think SWG would be beneficial to provide the OC with expert knowledge on the information security and privacy subject. We also envisage the SWG to take a 'check-and-balance' role alongside the CISO from CAT Processor. The diversified mix of SWG and OC should consist of not only participants or stakeholders that currently required submission of data to CAT, but also include non-contracting parties, such as academia and 'other' civic communities. SWG and OC should not be a private party among elites, SWG and OC should welcome tier 2 and 3 firms to join, as well as observe international best practices. The purpose of SWG and OC is to prevent massive government surveillance from inflicting damage[18] on anyone alongside the industry' value chain smile curve[19] as well as the general public. It would be our honor if given the opportunity to serve in SWG or OC.

The Commission assumes hourly labor rate for the CISO should at least be triple if not quadruple in today's market. Given CAT is the largest financial database ever containing critical market information with extremely high monetary values, the benchmark rate should be against the CISO of Facebook, Amazon, or Google. The assumptions for Chief Regulatory Officer and Chief Compliance Officer are also underestimated. We envisage the Operating Committee members are diversified representatives from the industry as well as civic communities, which many of them would be Executive or Managing Director grade if not C-Suite.

Providing for exceptions for the SAW usage requirements is a moot point depends on case-by-case how the participants and the processor may permit different access techniques to SAW. FINRA and large exchange groups have well-established surveillance systems that they would prefer tapping to CAT data to augment their systems rather than migrate to a newly develop and untested CAT's SAW environment. Participant Group indeed should be encouraged to frequently change and update their SAW in pursuit of relevant information security and privacy best practices whenever and wherever they see opportunities for improvement or face security and privacy challenges as emerging technologies evolves every month or quarter. Every update or periodic review requires end-to-end testing which is more or less equal to the initial benchmarking effort. Although the Commission believes that test data are available for development purpose, but the proposal permits exception to allow "development and testing" to access production data if approved by the CISO.

The Commission accounted for only the efficiency gain with regards to the proposed exception to grant non-regulatory staffs the convenience to access CAT data but omitted the corresponding social cost about exposing the entire industry and investment communities to undue risks. The Commission failed to mitigate risk or avoid 'function creep'. We have illustrated multiple scenarios where CAT related tech or data might be able to exploit or controls be circumvented by Regulatory Staffs, Plan Processor, Participants, Contractors, and Hackers. Neither the Commission nor the Plan Processor has right to jeopardize valuable market information and privacy data. Urgency to respond to a market event is no excuse for not diligently addressing civic concerns. The proposal failed to satisfy or to some extents against the public's interest.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Security and privacy controls would always be a race against hackers, setting a minimum standard rather than pursuing the best defense would introduce opportunities for the hackers. By the time the participants agreed to a "common" SAW, the techniques may have been obsoleted. Modern surveillance is able to discover intelligence through deploying "agents", in-memory forensic, and/or uses other techniques across decentralized or distributed networks to pick up 'bits-and-pieces' to knit the big picture. Going to a central vault via a centralized SAW is not only outdated but it is also a target attracting hackers to treasure hunt.

We suggest using keylogging techniques to literally capture every keystroke to ensure maximum scrutiny of all users' activities, while we believe the Plan Processor's processes that produce log files for monitoring is different. So, it is like comparing apple to orange. Regarding limiting the number of records, the proposed 200,000 records would never be enough to scrutinize the larger firms, causing a 'too big to exam' scenario. It would be discriminative to smaller firms or non-HFTs (see ***Table 1*** point R), yet it will not reduce the regulatory use of CAT data.

The more parties having access to the full design specifications, the more vulnerability CAT will be. The design should be broken into partial pieces that no single developer or any trusted party would be able to know the other portions of the CAT design. Makers of privacy and security controls (i.e. the Plan Processor) should preserve their secrets. Checkers (independent assessor commissioned by the OC) should independently conduct their testing, include ethical hacking. That being said, Control Makers should share some high level infrastructure setup (without unveiling critical secrets) with the Checkers to allow the checkers to apply analytical procedures and plan for relevant tests.

Customers have rights to object sharing of privacy information with other parties other than their service providers, unless being subpoena. There should not even be a Customer Identifying System. It invites opportunities for hackers. We think neither the Commission nor the Plan Processor has the right to access privacy information without consent or proper subpoena. If SWG and OC are representative of public interests rather than just 'participants' from the Exchanges, they should have rights to challenge anything that deems inflicting damage on 'others' as a result of inappropriate use or negligence in design of CAT. The proposal reflects the egos of massive government surveillance while did not account for the corresponding social cost on the society. As of today, there is no mentioning of where the billions would come from to fund the CAT project. We argue that CAT cost burden would be added as part of the intermediary cost causing further "frowning" of the smile curve[19] and ultimately cascade down to every investors and the main street.

'Uniformly', 'reduce variability', or 'standardizing implementation of security protocols', and 'common detailed design specifications', etc. could be negatives in contexts of security. Saving a few dollars here may end up costing more down the road. Maze or chaos is somehow more effective and cheaper than structural controls. Perfect accuracy or golden-source of data is extremely expensive and unaffordable. It is merely well-articulated "promotes" to sell data-vault storage products, rather than a true pursuit of big data. Big Data prioritizes velocity (real-time) over veracity.[17]

Our proposed ***Figure 2*** encompasses abilities to pick up bits-and-pieces of intelligence in real-time from chaotic or widely distributed sources of data and knitting them together. It is more resilient than a gigantic data vault. It has the benefits of: (a) dramatically reduce CAT footprint or data storage and traffic by avoiding unnecessary redundant copies of data and minimize 'data-in-motion'; (b) confine access to CAT data to 'targeted search' of relevant data that fits the 'defined purposes'; and (c) better intelligence for market monitoring by enabling and rewarding the crowd for identifying early warning signals to potential flash crash or other trade irregularities.

The Commission's proposal has adverse effect on competition and detrimental to capital formation. It would shrink the number of small and diversified players, while market would be fragmented and dominated by elite players. It failed to allow participants feel safe and secure to freely engage in permissible trading activities with this massive government

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

surveillance knife overhanging above their heads. The negative economic impact is not "De Minimis"; it contrasted significantly with our positive and non-invasive way to knit surveillance intelligence together. The proposal ought to be rejected and go back to the drawing board to consider our suggestions in ***Figure 1*** and ***Figure 2***.

VI. Regulatory Flexibility Act Certification

Question 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.

We think the proposed amendments would not have a significant economic impact on a substantial number of small entities and favor the elites. For example, the proposed 200,000 records would never be enough to scrutinize the larger firms, causing a 'too big to exam' scenario. It would be discriminative to smaller firms or non-HFTs (see ***Table 1*** point R).

We however believe that the reference to "Independent Accountant" instead of "Independent Security Expert" in Question 146 may be an honest mistake.