FINANCIAL INFORMATION FORUM

5 Hanover Square
New York, New York 10004
———————
212-422-8568

FIF CAT WG Review -CAT NMS Plan Security and Confidentiality Requirements

This document is divided into two sections:

1. A summary of the comments received from the FIF CAT Working Group, showing the general concerns that are persistent throughout the Amended CAT NMS Plan ("CAT NMS Plan") relating to security and confidentiality.
2. Following the outline provided by the DAG for the next few DAG meetings, specific comments/questions are provided with references from the CAT NMS Plan which are examples of and support the general concerns provided in the first section.

Summary of Comments

1. Although the CAT NMS Plan does mention that CAT is a Reg SCI system, and as such, will abide by the Reg SCI requirements, there is little mention of the Reg SCI security requirements imposed on the CAT System. There is no incorporation in the CAT NMS Plan of the risk-based approach inherent in Reg SCI. The CAT NMS Plan does not specify that a process, as mandated by Reg SCI, is required to determine the security risk levels of the CAT Systems and subsequently the appropriate security controls that will be implemented by the Plan Processor in its information security program.

2. Just referencing NIST industry standards is not prescriptive of which standards must be implemented, for these standards also adopt a risk-based approach. Depending on the risk level assigned to that system/function, different families of controls within the standards can be applied. So inclusion of a requirement for an (on-going) assessment of risks associated with the CAT System and data is also needed to meet the NIST Industry Standards referenced in the CAT NMS Plan.

3. The CAT NMS Plan contains good requirements on security and confidentiality controls for certain aspects of the Central Repository, specifically database controls; however, there is no mention of requirements for other data formats that are likely included in the Central Repository (e.g., CAT Reporter flat files received via FTP by the CAT).

4. There is little mention of requirements for controls on the overall CAT System, including network controls. There are many references in the CAT NMS Plan to security and confidentiality controls for the Central Repository; these points should be expanded to discuss similar controls on the CAT System.

5. There is no mention of requirements for security and confidentiality controls on CAT Reporter test systems in Appendix D.4 – Data Security. CAT Reporters will likely use production level data to test their CAT interfaces and repairs to their CAT reports. The same requirements for security and confidentiality applied to the CAT production system should also be applied to the CAT Reporter test systems.

6. The CAT NMS Plan includes a good focus on security reporting, but is lacking in requirements for follow-up actions that will bring closure to any identified problems. Some examples include: requirements for timely remediation plans, proposed actions to fix identified problems that include timeframes that can be monitored, methodologies for thorough investigations and future prevention; e.g., postmortems, etc.

7. There are a number of security requirements included in the CAT NMS Plan regarding commingled infrastructures and public cloud infrastructures. These requirements are

inconsistent and incomplete (e.g., singular focus on public cloud infrastructure). Further, the requirements stated for the public cloud infrastructure should apply equally to most compute and data infrastructures, not just public cloud infrastructures.

8. The security and confidentiality requirements contained in the CAT NMS Plan are inconsistent in their level of specificity. It difficult to determine why some requirements are discussed in the CAT NMS Plan, and other critical areas that require security controls are not mentioned at all. For example, monitoring of all Central Repository data accesses is included, but there is no mention of monitoring of system accesses or unsuccessful attempts to access data/system; an automated mechanism to monitor direct query usage is included, but there is no mention of an automated mechanism to monitor logs and alerts. The CAT NMS Plan should provide an overall security framework so that specific controls included in the CAT NMS Plan can be put in context.

9. Certification (not just review) of all Participants, SEC CAT employees and third party agents who have access to the system and/or CAT data, and the level of authorization rights assigned to each individual should be performed quarterly, not periodically or annually, as currently included in the CAT NMS Plan.

Central Repository Architectural Security Features (DAG meeting topics 2/24/16)

- Appendix D.1.2 states "The Plan Processor must provide an environment supporting industry testing (test environment) that is functionally equivalent to the production environment, including…Management with the same information security policies applicable to the production environment." Why is this requirement not included in both Appendix C.4 and Appendix D.4?
- There are references to security requirements of database controls for Central Repository. The Central Repository will likely be a mix of data formats, not just databases. For example, the CAT will receive flat files via FTP containing CAT reports from CAT Reporters. Those files must be protected with the same stringency as the CAT databases. (e.g., Article VI, 6.5.f.iv.C, Article VI.6.9.b.xi, Appendix D.4.1.1). References to database controls should be expanded to include all appropriate data formats.

- ***Encryption and key management***
    - Appendix D.4.1.1 – "CAT Reporters must connect to the CAT infrastructure using secure methods….".The connection requirements for Participants, SEC, Plan Processor employees and third party agents should be included in the CAT NMS Plan and be, at a minimum, as restrictive as CAT Reporter requirements.

- ***Architectural segregation (e.g., firewalls, DMZs)***
    - Appendix D.4.1.3 – "CAT compute infrastructure may not be commingled with other non-regulatory systems (or tenets, in the case of public cloud infrastructure)." If commingling is allowed with other regulatory systems, there should also be a requirement that these "other" regulatory systems must also abide by the same security controls imposed on the CAT systems. Is the CAT data infrastructure (not just the compute infrastructure) also required to be separated in cloud and non-cloud implementations?
    - Appendix D.4.1.1 – "If public cloud infrastructures are used, virtual private networking and firewalls/access control lists or equivalent controls … must be used to isolate CAT data from unauthenticated public access". These security controls should be included in the CAT NMS Plan as examples of security controls expected in any CAT infrastructure, not just public cloud infrastructures.
    - Appendix D.4.1.2 – Are any of the bidders proposing either a shared private environment implementation or an implementation using public computing

infrastructures? If yes, what are the special security requirements to protect the CAT data in these environments?
    - Appendix D.4.1.2 – "Auditing and real-time monitoring of the service for when cloud provider personnel are able to access/decrypt CAT data must be documented …" This requirement should be included in the CAT NMS Plan as applicable to any CAT infrastructure implementation, not just cloud providers.

- ***Threat monitoring***
    - There is no mention in the list of security requirements about follow-up management of results of various data security and penetration test reviews (e.g., Article VI.6.2.b.v.H). It is insufficient to conduct a penetration test review if there is not a remediation plan and monitoring following the review including a schedule of planned fixes, post mortems to identify and correct processes that contributed to the deficiency, etc.
    - The certification of CAT system and Central Repository access and authorization levels by the Plan Processor to the Operating Committee should be required of all CAT users and Plan Processor employees quarterly, not annually (e.g., Article VI.6.5.c.iii)

Plan Processor Governance, Policies, and Procedures (DAG meeting topics 2/24/16)

- ***Data management and destruction***

- ***CCO and CISO roles and responsibilities***
    - Many references to CCO and CISO roles/responsibilities only mention Central Repository security requirements; many of these references should be generalized to also include the CAT System. (e.g., Article VI,6.1.o.ii, Article VI, 6.2.b.v, Article VI,6.5.f.i.B).
    - The annual audit plan should include an audit of the Plan Processor and CAT System, not just Central Repository. The audit should also include a comparison of the implementation of security controls against the Plan Processor approved policies and procedures (Article VI.6.2.a.v.C, Appendix C.A.4.a)
    - What is the CISO's responsibility relative to the information security program referenced in Article VI.6.2.a.v.H and Article VI.6.12 other than review? Shouldn't the CISO be responsible for the development of this program, as well as ensuring that it remains current?
    - The CISO should be responsible for creating and enforcing security policies, etc. for the CAT System, not just the Central Repository (Article VI.6.2.b.v).

- ***Plan Processor responsibilities:***
    - Many references to Plan Processor responsibilities only mention the Central Repository security requirements; these references should be generalized to also include the CAT System. Without thorough protection and monitoring of overall CAT System and network access, including definition and implementation of policies/procedures governing entire CAT System and reporting to OC, Central Repository security is meaningless (e.g., Article, Article VI,6.5.f.i.B, Appendix C.A.4.a)

- ***Participant and SEC responsibilities:***
    - Articles VI.6.5.f.i.A and B – Exclusion of the SEC from agreement to use appropriate safeguards and execution of a personal "Safeguard of Information Affidavit" is inappropriate without a compensating statement about safeguards that will be executed by SEC.

- Article VI.6.5.g – The SEC is not included in the requirement to establish and enforce written policies and procedures designed to ensure CAT data confidentiality. This appears contradictory to the overall security policy included in this CAT NMS Plan.

- ***Plan Processor employee controls***
  - Article VI, 6.1.d - "The Plan Process shall have hiring standards and shall conduct and enforce background checks for all of its employees and contractors to ensure the protection, safeguarding and security of the facilities, systems, networks, equipment and data of the CAT System, and shall have an insider and external threat policy to detect, monitor and remedy cyber and other threats". Very few requirements are included in the CAT NMS Plan of security and confidentiality controls for Plan Processor employees, especially administrative personnel, systems and database maintenance personnel, and especially persons with high levels of system authority. Shouldn't this requirement statement from Article VI, at a minimum, be included in the security related sections Appendices C.4 and D.4?

- ***Breach detection and management***
  - Appendix D.4.1.5 – Breach management does not include any requirements for action plans following the breach – actions that will create closure following the breach. For example, the documentation expected on a breach does not include any remediation actions, and a timeline for implementation of these actions.
  - What is the process for notifying CAT Reporters when an incident (not necessarily a breach) has been identified?

- ***Training***
  - Article VI, 6.1.m – This specifies that security training must be made available to the CAT Reporters. Please clarify if this training is mandatory for CAT Reporters.
  - Article VI, 6.1.m – Shouldn't there be a requirement in the CAT NMS Plan that this security training material be reviewed and updated periodically to consider the changing risk landscape?

- ***Testing***
  - Appendix D.4.1.3 – Penetration testing and an application security code audit should be completed, with implementation of the most serious fixes in place prior to start of CAT Reporter testing (prior to "go-live" is too late!). CAT Reporter production data will be committed to the CAT Reporter test environment and could be exposed if the CAT environment is not secure.
  - Appendix D.4.1.3 – All security reports should include remediation plans with specified or expected timeframes for action. All security issues identified should require a post-mortem report (how it happened, why it wasn't identified before, how similar incidents will be prevented from re-occurring)

Data Usage & SRO Controls (DAG meeting topics 3/9/16)

- ***Data query and usage***
  - Appendix D.2.2.1 – What security policies are required for the CAT Reporter GUI interface and CAT Reporter web site?
  - Appendix D.4.1.4 –"Periodic reports detailing current list of authorized users…provided to Participants and SEC". These periodic reports should be required quarterly.
  - Appendix D.4.1.4 – The certification process for Participant/SEC authorized CAT access list should include a reasonable timeframe for the expected response.

- Appendix D.4.1.4 – The CAT NMS Plan should require that role-based controls include the capability to limit regulators to specified sections of the CAT data, and not just all data from all CAT Reporters, with the exception of PII data. The role-based controls should be defined to support CAT Reporter extraction of CAT data, whenever permitted within the CAT NMS Plan.

- ***PII retrieval and usage***
  - Article VI.6.10.c.ii – Clarification is needed on what "masked" means? Appendix D.8.2 says that "Direct queries must not return or display PII data. Instead, they will return existing non-PII unique identifiers (e.g., Customer ID or Firm Designated ID). Is that what "masked" means?
  - Appendix D.4.1.6 - "Annual review by chief regulatory officer at each Participant and SEC to review/certify PII access list". A quarterly review would be more consistent with current administrative practices for authorization reviews.

- ***Audit trail functionality***
  - Appendix D.7.3 - "The Plan Processor must maintain a detailed audit trail capturing corrections to and replacement of records". Assuming PII data will be included in the CAT data written to audit logs, what are the security and confidentiality controls on the CAT data in the audit logs?

- ***SRO policies and procedures for CAT data usage***
  - Appendix D.4.1.4 – "The Plan Processor must develop and maintain policies … to prevent, detect and mitigate the impact of unauthorized access or usage of data in Central Repository". Is this policy aimed at Plan Processor employees?
  - Article VI.6.5.g - "The Participants shall establish, maintain and enforce written policies and procedures reasonably designed to (1) ensure the confidentiality of the CAT Data obtained from the Central Repository; and (2) limit the use of CAT Data obtained from the Central Repository solely for surveillance and regulatory purposes. Each Participant shall periodically review the effectiveness of the policies and procedures required by this paragraph, and take prompt action to remedy deficiencies in such policies and procedures". This requirement should be extended to the SEC, and these Participant/SEC systems that process/store CAT data should be classified as Reg SCI systems.