FINANCIAL INFORMATION FORUM

5 Hanover Square
New York, New York 10004

212-422-8568

Via Electronic Delivery

August 3, 2018

Mr. Vas Rajan
Chief Information Security Officer
ThesysCAT, LLC
1740 Broadway
New York, NY, 10019

Re: FIF Comments on Cybersecurity and Data Protection

Dear Mr. Rajan,

The Financial Information Forum ("FIF")[1] Consolidated Audit Trail Cybersecurity Working Group appreciates the opportunity to provide comments on specific industry member concerns regarding security-focused elements contained in V0.2 (excerpt) of the Industry Member Technical Specification released on February 21, 2018. Following a targeted review of the security measures incorporated in V0.2 of the tech spec, FIF formed a subgroup focused on assessing and providing recommendations pursuant to the security-related requirements specified in the Technical Specification. The comments below compile the feedback received from 5 subgroup sessions comprising approximately 15-member firms specifically addressing data access and encryption. FIF respectfully requests that the recommendations below be considered along with FIF's previously submitted comments[2] on V0.3.1 of the Industry Member Technical Specification for incorporation into the September 5, 2018 release of the initial Industry Member Technical Specification.

Data Access

The CAT NMS Plan outlines a number of considerations related to 'Data Access' required by ThesysCAT to incorporate into the Industry Member Technical Specification.[3]

---

[1] FIF (www.fif.com) was formed in 1996 to provide a centralized source of information on the implementation issues that impact the securities industry across the order lifecycle. Our participants include trading and back office service bureaus, broker-dealers, market data vendors and exchanges. Through topic-oriented working groups, FIF participants focus on critical issues and productive solutions to technology developments, regulatory initiatives, and other industry changes.

[2] *See* letter from Christopher Bok, FIF to Mr. Shane Swanson, Chief Compliance Officer, ThesysCAT LLC, *RE: FIF Comments on V0.3.1 of the Industry Member Technical Specification (Dated June 6, 2018)* (July 16, 2018).

[3] *See* CAT NMS Plan, Appendix D, Section 4.1.2

As of July 25, 2018, ThesysCAT has provided Industry Members with limited information in the previously released technical specifications (Draft V0.1 and V0.2 (excerpt)) and V0.3.1 as it relates to Data Access / Password protection. Specifically, V0.2 of the technical specification specifies only that "Submission to CAT requires a valid user ID and password. Reporters must obtain a master user ID and password combination during the CAT registration process. Reporters will also be assigned a multi-factor authentication (MFA) token during the registration process. An MFA token is required for authentication when accessing SFTP and Reporter Web Portal." Further, because the proposed user ID and password requirement is limited to 'Reporters' only, coupled with the information that has been made available thus far, we wish to highlight additional areas for consideration and clarification.

Data Access and Password Protection Strategy

As the outline for Data Access and Password Protection as specified in Appendix D is fairly generic, FIF would like to explicitly state the following requirements:

Authentication (this control should be replicated in Far DMZ, Near DMZ, Internal Network):

- **Internal users**: Access for internal users to the application should be confined within network and use issued identities. If there is a need for users to access remotely (in their role as employees), should be via VPN.
- **External users – Federated Authentication:** Support for federated authentication (*e.g.* SAML) should be used for authentication.
- **External users – that do not support Federated Authentication, should follow below guidelines:**
    - ***User Registration***
        - The creation of username and password is part of a self-service flow and only possible after the user being registered undergoes pre-validation checks
        - The user should be able to pick from a list of pre-canned challenge questions and provide responses on first login. The questions / responses will be stored and used as part of all user management activities.
    - ***User Authentication***
    - There should be 2-factor authentication process via username + password and a one-time cryptographically generated token or other hardware approaches. For example:
        - USB dongle issued to a user that will be required to be inserted into the computer to get access to that system.
        - The Bloomberg BUnit system, where users are issued a 2fa card with fingerprint scanner incorporated that is used to log into the Bloomberg terminal.

            - Password requirement is as follows:
                - Minimum 8 characters
                - Combination of numbers, letters (uppercase and lowercase) and special character
                - Passwords are stored as secure one way hash
            - One time cryptographically generated pin:
                - 2 FA leveraged through U2F / UAF → preferred option
                - 2 FA leveraged through RSA → preferred option
                - 2 FA delivered over text / email / voice → not preferred, with associated risk

- User Lockout:
    - Should be locked out after 5 unsuccessful login attempts
    - Should be automatically unlocked after 30 minutes
    - Next login after first unlock should be done with CAPTCHA

- ***Forgot Password / Change Password:***
    - When users click Forgot Password link, they should be asked to answer challenge questions. If the user:
        - Successfully answers challenge, then send a one-time passcode to the user that can be used to authenticate and create a new password
        - If the user does not successfully answer the challenge, then request a call to the helpdesk and perform further validation. Only when validation is successful will the one-time passcode be sent for them to login and create new password.
    - To change password or perform other user activities, user must:
        - First be logged in
        - Successfully answer challenge questions
        - Be able to enter the correct one time passcode delivered to them

- **Logging**
    - All the security-control validation (authentication, authorization, IV etc.) events (success and failures) are logged.
    - Sensitive data including the authentication credentials, Client PII and other sensitive data are NOT logged in application log file.
    - Debug mode logging should not enabled for production.
    - Tainted (Invalidated) user input is not logged in the log file.
    - Logs are fed to centralized logging system.
    - There is anomaly detection, reporting and escalation for the application.

Authorization:

- Access to objects must be governed by Access Control List (ACL) rules, which largely define a list of permissions related to a given object. (*i.e*. which users / systems are granted access / what operations are permitted).
- Defined roles should be scoped to what is required for that role. The Plan Processor should ensure that entitlements are defined within a given application / role.
- There should be no vertical (ability to obtain a higher level of access than an administrator or system developer intended, seeing above intended level) or horizontal (ability to obtain same level of access, for material / data not intended for a given user) access escalation.

Session Management (this control should be replicated in Far DMZ, Near DMZ, Internal Network):

- IP address filtering - allow users to access the system from only the system IP address that is registered for that user.
- Randomly generated and secure sessionIDs should be assigned to each session

- Session tokens should be transmitted securely
- Sessions should time out after 5 minutes of inactivity
    - Longer session may be required for Reporters, to fulfill daily uploads
- Absolute timeout for sessions should be 24 hours
- Sessions should terminate after logout
- Sessions must have protections in place to prevent token capture by malicious actors
- There is no simultaneous login

Governance

FIF requests that the policies, procedures, and protocols be established to support the data access strategy as described above. These may include:

- A data access management policy, defining the objectives, roles, responsibilities, and requirements for executing the data access management strategy.
- Develop and maintain policies and procedures reasonably designed to prevent, detect, and mitigate the impact of unauthorized access or usage of data in the Central Repository.
    - Information barriers governing access to and usage of data in the Central Repository;
    - Monitoring processes to detect unauthorized access to or usage of data in the Central Repository; and
    - Escalation procedures if unauthorized access to or usage of data is detected.
- CAT must support a defined number of roles with access to different types of CAT Data, down to the attribute level. Roles must be documented with periodic reports with the current list of authorized users, on a quarterly basis.
    - Immediate review must follow in instances where change of access is warranted. (*e.g.* Termination, role coverage changes, etc…)
- An incident response plan that includes coverage for data compromise incidents, with plans for timely notifications to Participants.
- Auditing and testing of data access policies and procedures as part of third party reviews of the Plan Processor.

Encryption Key Management

A number of considerations related to encryption key management have been put forth so far for the Plan Processor as specified in Appendix D – of the CAT NMS Plan. These considerations are outlined in Section 4.1.2 - Data Encryption and Section 4.1.3 - Data Storage and Environment.

FIF notes that there has been some information provided thus far in the Draft CAT NMS Technical Specification(s) related to encryption:

- PGP will be used to encrypt, sign, and securely hash data. The CAT public encryption key must be used to encrypt data and will be made available to reporters. Submitters may also sign files with their private key. (11.3.1 File Size, Encryption, and Compression)
- Public / private key pairs should be RSA with a bit length of at least 2048 and up to 4096. The cipher algorithm must be AES-256 or higher. The digest algorithm used to sign the file must be SHA256. (11.3.1 File Size, Encryption, and Compression)

Based on the requirements proposed, and what information has been made available thus far, we wish to highlight additional areas for consideration and clarification.

Encryption Key Management Strategy

To date, ThesysCAT has not provided the industry with sufficient detail related to the Plan Processor's encryption key management strategy. We would expect such a strategy to include security requirements for each phase of the key management lifecycle.

- **Selection of key algorithms and protocols**
  - Definition of required encryption algorithm and key strength
    - Asymmetric key encryption (*e.g.,* PGP) for exchanging data between Data Submitters and the Central Repository is desirable.
  - Use of Key Encryption Keys (KEKs) and Data Encryption Keys (DEKs) for storage of information on cloud infrastructure
- **Generation and Distribution**
  - Key generation should be fully automated to mitigate risks of accidental exposure by a protocol operators
  - Multiple personnel are required to generate and update keys
  - Generate keys with purpose-build hardware, such as a Hardware Security Module (HSM)
  - Keys are distributed via secure channel
- **Access Control**
  - Access to keys requires an identifier and at least 2 other factors
  - Access to keys is logged and monitored
  - Key access is restricted to the fewest number of employees necessary
  - Segregation of duties taken into account when determining access
- **Storage**
  - Keys are never stored in plaintext format
  - Store keys on purpose-built hardware (HSM)
  - Implement methods to validate key integrity while in storage
- **Backup**
  - Key backups are stored securely in separate location from keys themselves
  - Key backups are validated, tested on a periodic basis
- **Rotation**
  - Keys are rotated periodically
  - Keys are rotated as needed based on an event (e.g., security breach)
- **Compromise and Recovery**
  - Use integrity checking to validate keys and encrypted materials
  - A key compromise recovery procedure is established, documented, and regularly trained with plan participants

Governance

FIF requests that policies, procedures, and protocols be established to support the key management strategy described above. These may include:

- An encryption key management policy, defining the objectives, roles, responsibilities, and requirements for executing the key management strategy

- Documented procedures supporting each component of the lifecycle above – key generation and distribution, key rotation, key compromise and recovery
- An incident response plan that includes coverage for key compromise incidents, with plans for timely notifications to Participants
- Auditing and testing of key management policies and procedures as part of third party reviews of the Plan Processor

Summary

FIF wishes to thank ThesysCAT for considering the aforementioned recommendations related specifically to data access and key encryption/management. FIF members view the security of the Consolidated Audit Trail to be among the highest priority items to be assessed and fully incorporated into the technical specifications. While Industry Members understand that certain security measures will not be publicized to better protect the CAT security infrastructure, FIF will continue to assess the security features of the CAT repository and provide best practice recommendations to be considered by ThesyCAT as you develop the security controls around the CAT. FIF offers our assistance to ThesysCAT as you continue to build out and refine the CAT security protocols.

Regards,

Christopher Bok, Esq.
Financial Information Forum

CC Mr. Andre Frank, President, ThesysCAT, LLC
Mr. Shane Swanson, Chief Compliance Officer, ThesysCAT, LLC
Mr. Todd Golub, Head of Product Management, ThesysCAT, LLC