U.S. Securities and Exchange Commission

Rule 19d-1 Tracking System
PRIVACY IMPACT ASSESSMENT (PIA)

August 13, 2020

Office of Compliance Inspections and Examinations

Privacy Impact Assessment

Rule 19d-1 Tracking System

Section 1: System Overview

1.1 Name of Project or System

Rule 19d-1 Tracking System ("Rule 19d-1 Filing System")

1.2 Is the system internally or externally hosted?

☒ Internally Hosted (SEC) Office of Information Technology (OIT)

☐ Externally Hosted (Contractor or other agency/organization)

1.3 Reason for completing PIA

☐ New project or system

☒ This is an existing system undergoing an update

First developed: 4/22/2009

Last updated: 12/27/2019

Description of update: This PIA is being updated to identify privacy risks and mitigating controls of the Rule 19d-1 system.

1.4 Does the system or program employ any of the following technologies?

☐ Electronic Data Warehouse (EDW)

☐ Social Media

☐ Mobile Application (or GPS)

☐ Cloud Computing Services

☐ www.sec.gov Web Portal

☒ None of the Above

Section 2: Authority and Purpose of Collection

2.1 Describe the project and its purpose or function in the SEC's IT environment

The Rule 19d-1 Tracking System is a National Exam Program (NEP) system used by Self-Regulatory Organizations (SROs) to submit electronic filings pursuant to Rule 19d-1 under the Securities Exchange Act of 1934. Exchange Act Rule 19d-1 (Minor Rule Violations) requires SROs to promptly notify the SEC of final disciplinary actions against its members Many SROs submit these 19d-1 filings electronically, both through email and the 19d-1 Tracking System. Some SROs may submit filings as a hard copy.

Rule 19d-1 notices are collected and maintained as a repository by Office of Compliance Inspections and Examinations (OCIE). The system provides a standardized entry form through which the SROs can electronically submit the 19d-1 notice of final disciplinary action against a member as required by the Securities Exchange Act.

The system involves two applications: (1) External (public facing) 19d-1 application; (2) Internal 19d-1 application.

The external 19d-1 application, a contractor developed application to facilitate the collection of 19d-1 notices consists of a standardized secure web entry form that is used by SROs to electronically file 19d-1 notices. The system collects, through the secure form, the member's name, occupation, job title, work address, certificate/license number, work history, business associates, case ID, financial accounts, and financial transactions. External users cannot perform any administrative tasks since there is no administrative functionality on the external application. 19d-1 integrates with GSA (General Services Administration)'s

login.gov to authenticate external users. All external users are authenticated by login.gov using multi-factor authentication, which includes username (email address) and a combination of user-entered password and login.gov token sent through SMS (Short Messaging Service) or phone call. All these accounts go through proper approval process before being granted access to 19d-1. Login.gov is a service that offers secure and private online access to government programs, such as federal benefits, services and applications. With a login.gov account, you can sign into multiple government websites with the same email address and password.

The internal 19d-1 application collects data provided by SROs and enables internal review, search, and reporting of 19d-1 notice. Internal access accounts are processed by the Sybase database administrator once approval is received from the System Owner. The internal application is housed on a different server from the external application and is accessible only to SEC staff.

2.2 What specific legal authorities, arrangements, and/or agreements allow the information to be collected?

Rule 19d-1 of the Securities and Exchange Act. Securities Exchange Act Release No. 53428 (March 7, 2006), 71 FR 13645. Self-Regulatory Organizations; Order Approving Minor Rule Violations Plan The NASDAQ Stock Market LLC.

2.3 Does the project use, collect, or maintain Social Security numbers (SSNs)? *This includes truncated SSNs.*

☒ No
☐ Yes
If yes, provide the purpose of collection:
If yes, provide the legal authority:

2.4 Do you retrieve data in the system by using a personal identifier?

☐ No
☐ Yes, a SORN (System of Records Notices) is in progress
☒ Yes, there is an existing SORN
SEC-55 ("Information Pertaining or Relevant to SEC Regulated Entities and Their Activities")

2.5 Is the information covered by the Paperwork Reduction Act of 1995 (PRA)?

☐ No
☒ Yes
OMB Control Number:3235-0206 ; Expiration Date: 08/31/2022

2.6 Considering the purpose of the collection, what privacy risks were identified and how were those risks mitigated?

Potential privacy risks are that personal information may be collected without a clear purpose or without clear legal authority; information collected is either unnecessary or excessive; or the information provided for one purpose may be used inappropriately. These potential risks are mitigated by stating clearly the purpose for collecting the personal information in the applicable systems of records notices, privacy impact assessments and other notices, and limiting the information collected to what is truly necessary for intended purposes.

Section 3: Data Collection, Minimization, and Retention

3.1 What information is collected, maintained, used, or disseminated about individuals? *Check all that apply.*

☐ The system does not collect, maintain, use, or disseminate information about individuals.

Identifying Numbers

☐ Social Security Number ☐ Alien Registration ☒ Financial Accounts

☐ Taxpayer ID	☐ Driver's License Number	☒ Financial Transactions
☐ Employee ID	☐ Passport Information	☐ Vehicle Identifiers
☒ File/Case ID	☐ Credit Card Number	☐ Employer ID
☐ Other:		

General Personal Data

☒ Name	☐ Date of Birth	☐ Marriage Records
☐ Maiden Name	☐ Place of Birth	☐ Financial Information
☐ Alias	☐ Home Address	☐ Medical Information
☐ Gender	☐ Telephone Number	☐ Military Service
☐ Age	☐ Email Address	☐ Mother's Maiden Name
☐ Race/Ethnicity	☐ Education Records	☐ Health Plan Numbers
☐ Civil or Criminal History	☐ Zip Code	
☐ Other:		

Work-Related Data

☒ Occupation	☐ Telephone Number	☐ Salary
☒ Job Title	☒ Email Address	☒ Work History
☒ Work Address	☒ Certificate/License Number	☒ Business Associates
☐ PIV Card Information	☐ Fax Number	
☐ Other:		

Distinguishing Features/Biometrics

☐ Fingerprints	☐ Photographs	☐ Genetic Information
☐ Voice Recording	☐ Video Recordings	☐ Voice Signature
☐ Other:		

System Administration/Audit Data

☒ User ID	☐ Date/Time of Access	☐ ID Files Accessed
☒ IP Address	☐ Queries Ran	☐ Contents of Files
☐ Other:		

3.2 Why is the PII listed in Question 3.1 collected, used, shared, or maintained by the system or project?

The Commission uses the information provided in the Rule 19d-1 notices for its SRO oversight program, and the information helps ensure that SRO enforcement of the federal securities laws is performed diligently and fairly. For internal users of the system, Rule 19d-1 does maintain data necessary for establishing a user account for SEC employees that have been approved access to the system. For external users of the system, name, address, email address, and phone number are collected to confirm the identity of the individual requesting access to the system.

3.3 Whose information may be collected, used, shared, or maintained by the system?

☒ SEC Employees

Purpose: Rule 19d-1 does maintain data necessary for establishing a user account for SEC employees that have been approved access to the system.

☒ SEC Federal Contractors

Purpose: Rule 19d-1 does maintain data necessary for establishing a user account for SEC Federal Contractors that have been approved access to the system.

☐ Interns

Purpose:

☒ Members of the Public

Purpose: The data is being collected in compliance with Rule 19d-1 of the Exchange Act. SROs are required to submit notice of final disciplinary actions taken against its members to the SEC through a standardized entry form that SROs submit to Office of Compliance Inspections and Examinations (OCIE).

☐ Employee Family Members

Purpose:

☐ Former Employees

Purpose:

☐ Job Applicants

Purpose:

☐ Vendors

Purpose:

☐ Other:

Purpose:

3.4 Describe the PII minimizing mechanisms and if the PII from the system is being used for testing, training, and/or research efforts.

The external facing application in stage environment allows the SROs to submit test data. There is no PII in test data used for testing, training, or research.

3.5 Has a retention schedule been established by the National Archives and Records Administration (NARA)?

☐ No.

☒ Yes.

DAA-0266-2013-0004, Documents Related to OCIE Examinations, Monitoring or Other Inquiries of Regulated Entities

3.6 What are the procedures for identification and disposition at the end of the retention period?

Disposition of the data is in accordance with the SEC's NARA-approved record retention schedule and applicable SEC administrative regulations and Office of Records Management Services (ORMS) Directives. Records are cut off at the end of the calendar year in which either the underlying matter is closed or the document is received (whichever is later). The retention period allows for destruction 10 year(s) after cutoff. The ORMS' procedures, *OP7-1c Destruction of SEC Records* outlines procedures for destroying records at the SEC. This process is coordinated between ORMS and the records liaisons in the respective division and office.

3.7 Will the system monitor members of the public, employees, and/or contractors?

☐ N/A

☐ Members of the Public

Purpose:

☒ Employees

Purpose: Surveillance cameras are used to monitor the data centers that house 19d-1 system components.

☐ Contractors

Purpose:

3.8 Considering the type of information collected, what privacy risks were identified and how were those risks mitigated?

The main privacy risk is inadvertent disclosure of the information. This risk is mitigated by (1) limiting access to the external application to only users with approved login credentials. (2) login.gov is for authentication. (3) 19d-1 integrates with GSA's login.gov to authenticate external users once access is approved User registers with login.gov. (4) All external users are authenticated by login.gov using multi-factor authentication, which includes username (email address) and a combination of user-entered password and login.gov token sent through SMS or phone call; (5) using a standardized form with minimal information being sought; (6) using a secure HTTPS web-based platform to retrieve data; and (7) compiling data from SROs transmitted to an internal database housed on a different server and accessible only to authorized SEC employees.

Section 4: Openness and Transparency

4.1 What forms of privacy notice were provided to the individuals prior to collection of data? *Check all that apply.*

☒ Privacy Act Statement
https://www.login.gov/policy/

☒ System of Records Notice
SEC-55 ("Information Pertaining or Relevant to SEC Regulated Entities and Their Activities") and SEC-70 ("SEC's Division of Trading and Markets Records")

☒ Privacy Impact Assessment
Date of Last Update: 8/26/2009

☒ Web Privacy Policy
https://www.sec.gov/privacy

☒ Other notice: External User Guide for Rule 19d-1 filing system
The external users receive notice of accessing a U.S. Government Computer System. This is shown on Page 5 of the External User Guide for Rule 19d-1 filing system. Page 6 of the External User Guide indicates that there is a warning on the user access request form: "Any information you submit here and usage of this website is subject to the terms of our privacy policy."

☐ Notice was not provided.

4.2 Considering the method(s) of notice provided, what privacy risks were identified regarding adequate notice and how were those risks mitigated?

The primary privacy risk is that individuals may not be aware that their information is being collected in the Rule 19d-1 Tracking System without an opportunity for them to consent. To mitigate this risk, the SEC has published SORN SEC-55 that provides notice of the nature and types of PII that may be collected on the individuals and the routine uses of the information by OCIE. External users are provided with a warning on the User Access Request form and receive a notification message or banner before being granted access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Internal users receive a notification upon initial login to the GSS (local LAN). Additionally, this PIA serves as notice of the nature and uses of PII collected and the privacy controls implemented to protect the information.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

None. The system has no mechanism in place to process and/or aggregate any data to derive new data.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes
Organizations: OCIE is the primary user. Also, Office of the General Counsel (OGC), Office of the Secretary (OS) or other divisions in the SEC may use the system to investigate disciplinary actions by SROs.

5.3 Describe the risk to privacy from internal sharing and describe how the risks are mitigated.

The primary risk is unauthorized access. This risk is mitigated by limiting use of the system to OCIE staff and a limited number of users (i.e., six) in other divisions with read-only access to the internal application.

5.4 Will external organizations have access to the data?

☒ No
☐ Yes
Organizations:

5.5 Describe the risk to privacy from external sharing and describe how the risks are mitigated.

The primary privacy risk associated with external sharing is that information could be erroneously disclosed to unauthorized parties or for an unauthorized purpose. This risk is mitigated by ensuring that the external sharing of PII is compatible with SORN SEC-55.

Section 6: Data Quality and Integrity

6.1 Is the information collected directly from the individual or from another source?

☐ Directly from the individual.
☒ Other source(s): Self-Regulatory Organizations (SROs) such as FINRA (Financial Industry Regulatory Authority, Inc.) and New York Stock Exchange (NYSE) notify the SEC if they are taking any of the following actions against its members: final disciplinary actions, denials, bars, limitations regarding membership, association, participation, or access to services or summary suspensions. The data is submitted using the Rule 19d-1 application system that provides a standardized entry form that SROs have been directed to submit to OCIE.

6.2 What methods will be used to collect the data?

The Rule 19d-1 application under the SEC Standard Application Architecture automates the collection of Rule 19d-1 filing from SROs through a secured Web site, and processes them through an internal database used to facilitate the review of the filings. The Rule 19d-1 application is comprised of internal and external applications that work together. The internal application is used by SEC employees and is only accessible to them. The external application is used by SROs. The internal application securely pulls the information from the external application while keeping the SEC's internal network secure. Only authorized users who have been granted access are authorized to submit filings. HTTPS protocol is used to submit the data files. This practice is

standard throughout the external filing systems within SEC. FINRA uses a web service to submit multiple filings in batch mode instead of filing it individually via the 19D1 external application. The web service is secure through the same security controls as the website. External (FINRA) web service requests are identified by 19d-1-supplied "username" and authenticated using 19d-1 generated tokens provided to login.gov authenticated and 19d-1 authorized FINRA users.

6.3 How will the data collected from individuals, or derived by the system, be checked for accuracy and completeness?

The information collected by the system is submitted directly from the SROs. Errors in the information, such as obvious erroneous sanction amounts, will result in an inquiry from OCIE to the SRO that sent the information requesting confirmation and clarification of the data. Additionally, the system compares the number of filings sent by Financial Industry Regulatory Authority, Inc. (FINRA) automatically through a feed with the number of filings received by the internal system to ensure that all filings sent were, in fact, received.

6.4 Does the project or system process, or access, PII in any other SEC system?

☒ No
☐ Yes.
System(s):

6.5 Consider the sources of the data and methods of collection and discuss the privacy risk for this system related to data quality and integrity? How are these risks mitigated? N/A

The SRO that is submitting the notice electronically provides the data that is collected by OCIE using a secure web application. The data that is collected includes the member's name, occupation, job title, work address, certificate/license number, work history, business associates, case ID, financial accounts, and financial transactions. The risk to data quality and integrity is mitigated by the fact that the information is obtained directly from the SRO whose member is responsible for keeping their records updated with the SRO. SROs must in turn provide this data to the SEC under Rule 19d-1 of the Securities and Exchange Act.

Section 7: Individual Participation

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

Individuals do not have an opportunity to consent, decline, or opt out of sharing with OCIE because SROs are required under Rule 19d-1 to provide this information. SROs registered with the SEC provide notice to members of their obligations to the SEC.

7.2 What procedures are in place to allow individuals to access their information?

Although SRO entities that submit information for 19d-1 notice may access their information through logging into the external website, members who are the subject of the notice do not have access the information submitted to OCIE. Members are responsible for keeping their records updated with the SRO.

7.3 Can individuals amend information about themselves in the system? If so, how?

Individuals would have to amend information with entities, who would then have to submit the updated information into the 19d-1 system. Only SROs can request SEC on behalf of members to delete information.

7.4 Discuss the privacy risks related to individual participation and redress? How were these risks mitigated?

Individual participation and redress with the system is limited. However, this is mitigated by SROs being required to file accurate information to the SEC. Accordingly, individuals should correct information with the submitting entity who would then update the SEC.

Section 8: Accountability and Auditing

8.1 Describe what privacy training is provided to users, either general or specific to the system or project.

All SEC users complete the Privacy and Information Security Awareness training prior to being granted access to SEC information and information systems. Also, users are trained on SEC Rules of the Road governing their activities related to safeguarding SEC information. Privacy and Information Security Awareness is provided on a continuous basis to keep users alert to the privacy and security requirements and safeguards." Additionally, the SEC attorneys using the system have been trained on the system.

8.2 Does the system generate reports that contain information on individuals?

☒ No
☐ Yes

8.3 Do contracts for the system include Federal Acquisition Regulation (FAR) and other applicable clauses ensuring adherence to the privacy provisions and practices?

☐ No
☐ Yes
☒ This is not a contractor operated system

8.4 Does the system employ audit logging or event logging?

☐ No
☒ Yes

8.5 Given the sensitivity of the PII in the system, manner of use, and established safeguards, describe the expected residual risk related to access.

The information in this database consists of information maintained by the SRO. Access is limited externally to SROs accessing the system to send data and internally the system is limited to OCIE staff and a limited number of users (i.e., six) in other divisions with read-only access.