Investor Response Information System and Relational Junction Software (IRIS-RJS)

PRIVACY IMPACT ASSESSMENT (PIA)

September 14, 2021

Office of Investor Education and Advocacy
Privacy Impact Assessment
Investor Response Information System and Relational Junction Software (IRIS-RJS)

Section 1: System Overview

1.1 Name of Project or System

Investor Response Information System and Relational Junction Software (IRIS-RJS)

1.2 Is the system internally or externally hosted?

☐ Internally Hosted (Securities and Exchange Commission (SEC))
☒ 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: 1/20/2010
Last updated:
Description of update: An update to the cloud platform.

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
☒ 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

Investor Response Information System and Relational Junction Software (IRIS-RJS), an externally hosted system hereafter referred to as IRIS is used by the Office of Investor Education and Advocacy (OIEA) to manage investor contacts (including complaints) and requests for information from the public, Congress, and other government agencies. IRIS allows OIEA to track staff replies to investor and related activity. Relational Junction Software (RJS) is an internally hosted data integration and warehousing tool that allows the SEC to copy IRIS data to the SEC where it can be shared with the Tips, Complaints, and Referrals (TCR) system and Palantir Electronic Data Analytics Platform (EDAP). Only system administrators use RJS.

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

15 U.S.C. 77s, 77sss, 78d, 78d-1, 78d-2, 78w, 78ll(d), 79t, 80a-37, and 80b-11

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 is in progress
  - ☒ Yes, there is an existing SORN
    - SEC-26 Mailing, Contact, Other List
    - SEC-31 Investor Response Information Systems (IRIS)
    - SEC-33 General Information Technology Records

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

- ☐ No
  - ☒ Yes

OMB Control Number 3235-0547

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

The purpose of this collection is to accept complaints from individual investors about firms and individuals regulated by the SEC. The privacy risk is that individuals who submit complaints could provide information that is either unnecessary or excessive. To mitigate this risk, the Investor Complaint Form is designed as a web form that only requests information from individuals that is necessary to resolve or refer their complaint to the appropriate SEC office, regulated entity, or external Government agency.

Another privacy risk is that information collected for the intended purpose could be used inappropriately. To mitigate this risk, role-based access controls are used to ensure that users only have access to the information necessary to perform their job duties.

---

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.

<table>
<thead>
<tr>
<th>Identifying Numbers</th>
<th>Alien Registration</th>
<th>Financial Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Social Security Number</td>
<td>☐ Driver’s License Number</td>
<td>☐ Financial Transactions</td>
</tr>
<tr>
<td>☐ Taxpayer ID</td>
<td>☐ Passport Information</td>
<td>☐ Vehicle Identifiers</td>
</tr>
<tr>
<td>☐ Employee ID</td>
<td>☐ Credit Card Number</td>
<td>☐ Employer ID</td>
</tr>
<tr>
<td>☐ File/Case ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>☐ Other:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

General Personal Data
Privacy Impact Assessment
Investor Response Information System and Relational Junction Software (IRIS-RJS)

☒ 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:
☐ Other:

<table>
<thead>
<tr>
<th>Work-Related Data</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Occupation</td>
<td>☒</td>
<td>☒</td>
<td>☐</td>
</tr>
<tr>
<td>Job Title</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Work Address</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>PIV Card Information</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Other:</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Distinguishing Features/Biometrics</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprints</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Voice Recording</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Other:</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Administration/Audit Data</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>☒</td>
<td>☒</td>
<td>☐</td>
</tr>
<tr>
<td>IP Address</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Other:</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

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

PII is collected, used, shared, and maintained to provide OIEA the capability to manage investor correspondence, including complaints and requests for information from the public, Congress, and other government agencies. Within IRIS, the personally identifiable information (PII) associated with an individual is used to correspond with the individual to answer a question or correspond with a financial service provider regarding the individual’s complaint.

Generally, PII about individuals associated with regulated entities is used:
- To identify individuals;
- To communicate with transfer agents, broker-dealers, investment advisers, municipal advisors, or their associated personnel, regarding the a complaint;
- By the SEC and other enforcement agencies in any enforcement or disciplinary proceedings or complaint-related inquiries concerning Transfer Agents, Broker Dealers, Investment Advisers, Municipal Advisors, or individuals associated with regulated entities in other capacities; and
- By the SEC or SEC-regulated institutions that employ Transfer Agents, Broker Dealers, Investment Advisers, Municipal Advisors, or individuals associated with regulated entities in other capacities, for taking disciplinary actions or making employment decisions.

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

☒ SEC Employees
  Purpose: Contact information required in order to create an IRIS file.
☐ SEC Federal Contractors
  Purpose:
☐ Interns
Purpose:
☒ Members of the Public
  Purpose: To facilitate the processing of investor complaints and requests for information.
☐ Employee Family Members
  Purpose: 
☐ Former Employees
  Purpose: 
☐ Job Applicants
  Purpose: 
☐ Vendors
  Purpose: 
☒ Other:
  Purpose: To facilitate the processing of investor complaints and requests for information from Congressional offices on behalf of constituents and other government agencies.

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 web-based Investor Complaint Form only requests information from individuals that is necessary to resolve or refer their complaint to the appropriate SEC office, regulated entity, or external Government agency. PII collected in IRIS is not used for testing, training or research.

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

☒ Yes

N1-266-95-1 - Complaint Correspondence Files

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

Records are maintained until they become inactive, at which time they are destroyed in accordance with records schedules of the SEC and as approved by the National Archives and Records Administration (NARA).

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

☒ Yes

☐ Members of the Public
  Purpose: 
☐ Employees
  Purpose: All internal IRIS users expressly consent to monitoring by a system administrator purpose detecting evidence of criminal activity, misuse, or other misconduct. See login page notice below.
3.8 Considering the type of information collected, what privacy risks were identified and how were those risks mitigated?

Investors who file complaints against regulated entities provide their name, address, and a description of the complaint. The privacy risk is unauthorized disclosure of information that could compromise investigations. This risk is mitigated by informing complainants by email how the information collected from the Investor Complaint Form will be shared with the individual or entity against whom the complaint is filed. Individuals who do not wish to have this information shared may submit complaints anonymously or select an option to withhold the complaint from the registered entity. Both the anonymous option and the withhold option enable individuals filing a complaint to have their information shielded if they so choose.

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
- System of Records Notice
  - SEC-26 Mailing, Contact, Other List
  - SEC-31 Investor Response Information Systems (IRIS)
  - SEC-33 General Information Technology Records
- Privacy Impact Assessment
- Date of Last Update:
- Web Privacy Policy
  - The SEC Web Site Privacy and Security Policy is located on the form at the following link: https://www.sec.gov/oiea/Complaint.html
- Other notice:
  - Bulletin on www.investor.gov entitled “Investor Bulletin: Investor Complaints” which provides an overview of complaint types, the process for handling complaints, the use of complaint information, and other options for resolving a complaint.
- 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 inadequate notice to individuals. This risk is mitigated through the use of the SORNs listed in 4.1, this PIA, and a link to the SEC Web Site Privacy and Security Policy on the Investor Complaint web form.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

Data submitted to IRIS by individual investors is not analyzed for the purpose of creating new information on the individual.

5.2 Will internal organizations have access to the data?

- No
Privacy Impact Assessment
Investor Response Information System and Relational Junction Software (IRIS-RJS)

☐ Yes
Organizations: Users share information within IRIS with authorized SEC recipients, including SEC’s Division of Enforcement (ENF) and other SEC offices or divisions with a business need-to-know the information in IRIS, to assist in the agency response to investor complaints and requests for information.

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

The primary risk is unauthorized access or disclosure of information stored in files on the SEC shared drive. The risk is mitigated through the use of two-factor authentication and role-based access controls, to ensure that users only have access to information on the shared drive that is required to perform their job function.

5.4 Will external organizations have access to the data?
☐ No
☒ Yes
Organizations: No external parties have access to IRIS; however, data may be shared with Federal law enforcement agencies as a part of the investigative process.

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

The primary risk is disclosure to unauthorized recipients during the transmission of information to external parties. Communication with external entities is handled by ENF, Office of Market Intelligence. Encrypted email or Kiteworks (a secure file transfer tool), are the only acceptable methods to share information.

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): Complaints may be forwarded to OIEA from the White House, Congressional offices, or other government agencies.

6.2 What methods will be used to collect the data?

Data is collected from an individual or other sources as follows:
1. Call OIEA directly using the number listed on https://www.investor.gov/contact-us and speak with an investor specialist. An investor specialist will manually enter the information into IRIS.
3. Submit email to help@sec.gov or oiea@sec.gov.
4. Send fax to OIEA using the number provided on https://www.investor.gov/contact-us.

6.3 How will the data collected from individuals, or derived by the system, be checked for accuracy and completeness?
It is not possible to ensure the accuracy of some of the information submitted by members of the public. However, an Investor Specialist may directly follow up with individuals who provide contact information, depending on the nature of the issue. As data is input into the Investor Complaint Form, input validation is performed to ensure that the data is consistent with the type expected. Data collected from individuals, as discussed in Section 6.2 above, is manually reviewed for accuracy and completeness by an OIEA Investor Specialist. If additional information is required to process the IRIS file, the Investor Specialist corresponds with the individual and enters the additional information into IRIS.

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

<table>
<thead>
<tr>
<th></th>
<th>No</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☒</td>
<td></td>
</tr>
</tbody>
</table>

**System(s):** IRIS interfaces with other SEC systems as follows:

- TCR has read-only access to a limited amount of IRIS data related to the correspondent, underlying question or complaint and how the matter was disposed. The data shared includes the correspondent’s contact information, the question or complaint, the categorization of the question or complaint, work notes, and electronic communications related to the disposition of the complaint or question.
- Palantir has read-only access to a limited amount of IRIS data. The data shared includes the correspondent’s contact information, the question or complaint, the categorization of the question or complaint, work notes, and electronic communications related to the disposition of the question or complaint.

### 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?

The risk to data quality and integrity is minimized by collecting PII directly from the individual and reviewing that information for accuracy and completeness. All data transmitted between the application and the cloud service provider and metadata stored on externally hosted servers, is encrypted so there is minimal risk to the modification of its content by an unauthorized individual.

### 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.

There is no obligation for individuals to submit correspondence to the SEC and individuals may submit information anonymously. The information provided by an individual is not disclosed beyond OIEA or authorized SEC staff with a valid need to know, unless the individual affirmatively checked “Yes - send the form to the firm or company” on the Investor Complain Form located at [https://www.sec.gov/oiea/Complaint.html](https://www.sec.gov/oiea/Complaint.html).

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

Individuals may request access to and correction of their information in accordance with the SEC Privacy Act/Freedom of Information Act (FOIA) procedures.

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

Investors cannot directly amend information about themselves in IRIS. However, individuals may contact OIEA at help@sec.gov to update or correct their information.
7.4 Discuss the privacy risks related to individual participation and redress. How were these risks mitigated?

The risk to individual participation and redress is minimal because individuals voluntarily submit their information, may provide information anonymously, and also may specify information to be withheld from disclosure.

### Section 8: Security

#### 8.1 Can the system be accessed outside of a connected SEC network?

- ☒ No
- ☐ Yes

  If yes, is secured authentication required?  
  - ☐ No  
  - ☐ Yes  
  - ☐ Not Applicable

  Is the session encrypted?  
  - ☐ No  
  - ☐ Yes  
  - ☐ Not Applicable

#### 8.2 Does the project or system involve an online collection of personal data?

- ☐ No
- ☒ Yes

  Public URL:  
  - [https://www.sec.gov/oiea/Complaint.html](https://www.sec.gov/oiea/Complaint.html)

#### 8.3 Does the site have a posted privacy notice?

- ☐ No
- ☒ Yes, Public URL [https://www.sec.gov/oiea/Complaint.html](https://www.sec.gov/oiea/Complaint.html) is posted on the Complaint form within the page footer.
- ☐ N/A

### Section 9: Accountability and Auditing

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

All SEC staff and contractors receive initial and annual privacy awareness training, which outlines roles and responsibilities for proper handling and protection of PII. SEC Rules of the Road ensure that employees and contractors are aware of their security responsibilities and how to fulfill them.

#### 9.2 Does the system generate reports that contain information on individuals?

- ☐ No
- ☒ Yes

  IRIS has preconfigured reports that allow SEC users from Regional Offices, Division of Examinations (EXAMS), Office of Internal Affairs (OIA), and OIEA to view complaint types at the aggregate level and allow users to identify trending questions or complaints.

#### 9.3 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

#### 9.4 Does the system employ audit logging or event logging?

- ☐ No
9.5 Given the sensitivity of the PII in the system, manner of use, and established safeguards, describe the expected residual risk related to access.

Residual risk related to access is minimal because access to IRIS-RJS is limited to SEC-approved users who are assigned roles based on least privilege required to perform job responsibilities. Access is also restricted to specific SEC IP addresses.