

U.S. Securities and Exchange Commission

**Comment Letter Log (CLL)
PRIVACY IMPACT ASSESSMENT (PIA)**



March 27, 2024

Office of the Secretary

Privacy Impact Assessment

Comment Letter Log (CLL)

Section 1: System Overview

1.1 Name of Project or System

Comment Letter Log (CLL)

1.2 Is the system internally or externally hosted?

- Internally Hosted (SEC) Office of the Secretary
- 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:
Last updated:
Description of update:

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

- Enterprise 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

Comment Letter Log (CLL), owned by the Office of the Secretary (OS) and operated by the Office of Information Technology (OIT). CLL allows the OS Information and Publishing branch to receive, process, and approve comments received from the public and SEC employees for rulemaking proposals.

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

5 U.S.C. 77a *et seq.*, 78a *et seq.*, 80a-1 *et seq.*, and 80b-1 *et seq.*

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 and Other Lists, 85 FR 85440 \(January 27, 2021\)](#)

Privacy Impact Assessment

Comment Letter Log (CLL)

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

- No
 Yes

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

The risk to privacy for the purpose of collection is that individuals may submit more personal information than required. This risk is mitigated by using a web form on SEC.gov to collect information (clearly stating on each form that information collected will be made publicly available on the SEC website) and through the comment review process where excess PII is redacted before publishing.

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

- | | | |
|---|--|---|
| <input type="checkbox"/> Social Security Number | <input type="checkbox"/> Alien Registration | <input type="checkbox"/> Financial Accounts |
| <input type="checkbox"/> Taxpayer ID | <input type="checkbox"/> Driver's License Number | <input type="checkbox"/> Financial Transactions |
| <input type="checkbox"/> Employee ID | <input type="checkbox"/> Passport Information | <input type="checkbox"/> Vehicle Identifiers |
| <input type="checkbox"/> File/Case ID | <input type="checkbox"/> Credit Card Number | <input type="checkbox"/> Employer ID |
- Other: Members of the public may occasionally provide identifying numbers via SEC.gov that are not solicited by the SEC. Examples of such numbers are financial account number and Social Security number. Such information is redacted from the published version of a comment.

General Personal Data

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Date of Birth | <input type="checkbox"/> Marriage Records |
| <input type="checkbox"/> Maiden Name | <input type="checkbox"/> Place of Birth | <input type="checkbox"/> Financial Information |
| <input type="checkbox"/> Alias | <input type="checkbox"/> Home Address | <input type="checkbox"/> Medical Information |
| <input type="checkbox"/> Gender | <input type="checkbox"/> Telephone Number | <input type="checkbox"/> Military Service |
| <input type="checkbox"/> Age | <input checked="" type="checkbox"/> Email Address | <input type="checkbox"/> Mother's Maiden Name |
| <input type="checkbox"/> Race/Ethnicity | <input type="checkbox"/> Education Records | <input type="checkbox"/> Health Plan Numbers |
| <input type="checkbox"/> Civil or Criminal History | <input type="checkbox"/> Zip Code | |
- Other: Members of the public may occasionally provide general personal data via SEC.gov that is not solicited by the SEC. Examples of such personal data are home address and personal telephone number. This information is redacted from the published version of a comment. In addition, file attachments submitted by the public may include any of the data elements listed above but are not required to submit a comment to the SEC.

Work-Related Data

- | | | |
|---|---|--|
| <input type="checkbox"/> Occupation | <input type="checkbox"/> Telephone Number | <input type="checkbox"/> Salary |
| <input type="checkbox"/> Job Title | <input type="checkbox"/> Email Address | <input type="checkbox"/> Work History |
| <input type="checkbox"/> Work Address | <input type="checkbox"/> Certificate/License Number | <input type="checkbox"/> Business Associates |
| <input type="checkbox"/> PIV Card Information | <input type="checkbox"/> Fax Number | |
- Other: In addition, commenting members of the public will occasionally provide information via SEC.gov that is not solicited by the SEC. Examples of the types of information are work address, work telephone number, and professional affiliation. File attachments submitted by the public may include any of the data elements listed above but are not required by the system.

Distinguishing Features/Biometrics

- | | | |
|---------------------------------------|--------------------------------------|--|
| <input type="checkbox"/> Fingerprints | <input type="checkbox"/> Photographs | <input type="checkbox"/> Genetic Information |
|---------------------------------------|--------------------------------------|--|

Privacy Impact Assessment

Comment Letter Log (CLL)

- | | | |
|--|---|--|
| <input type="checkbox"/> Voice Recording | <input type="checkbox"/> Video Recordings | <input type="checkbox"/> Voice Signature |
| <input type="checkbox"/> Other: | | |

System Administration/Audit Data

- | | | |
|---|--|--|
| <input checked="" type="checkbox"/> User ID | <input type="checkbox"/> Date/Time of Access | <input type="checkbox"/> ID Files Accessed |
| <input type="checkbox"/> IP Address | <input type="checkbox"/> Queries Ran | <input type="checkbox"/> Contents of Files |
| <input type="checkbox"/> Other: | | |

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

PII is collected to associate an individual with a particular comment submitted to the SEC.

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

- SEC Employees
Purpose: SEC employees may submit or process comments.
- SEC Federal Contractors
Purpose: SEC contractors may submit or process comments.
- Interns
Purpose:
- Members of the Public
Purpose: Members of the Public may submit comments for proposed rules to the SEC.
- 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.

Individuals are instructed on the web form used for comment collection to only submit information they wish to be made publicly available. OS Program Staff review comment submissions and redact PII not required as discussed in section 3.1. PII is not used for system testing, training, or research.

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

- No.
- Yes.
 1. Rulemaking comments; DAU: DAA-0266-2020-0002-0001
 2. Rulemaking petitions; DAU: DAA-0266-2020-0002-0005
 3. Self-regulatory organizations (SROs); DAU: NC1-266-82-1, item 8 **Note:** This DAU instruction may change in the near future.
 4. Commissioner solicited comments; DAU: DAA-0266-2020-0002-0001

Privacy Impact Assessment

Comment Letter Log (CLL)

5. Draft strategic plan: DAU: DAA-0266-2014-0002-0001
6. Distribution plan comments: DAU: DAA-2017-0009-0001

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

1. Rulemaking comments
 - a. Disposition: Permanent
 - b. Disposition instructions: Accession to NARA 15 years after case file closed.
2. Rulemaking petitions
 - a. Disposition: Temporary
 - b. Disposition instructions: Destroy 30 years after case file closed.
3. Self-regulatory organizations (SROs)
 - a. Disposition: Temporary **Note:** This disposition instruction may change in the near future
 - b. Disposition instructions: Destroy 6 years after case file closed.
4. Commissioner solicited comments
 - a. Disposition: Permanent
 - b. Disposition instructions: Accession to NARA 15 years after case file closed.
5. Draft strategic plan
 - a. Disposition: Permanent
 - b. Disposition instructions: Accession to NARA 15 years after case file closed.
6. Distribution plan comments
 - a. Disposition: Temporary
 - b. Disposition instructions: Destroy 10 years after case file closed.

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

- N/A
- Members of the Public
Purpose:
- Employees
Purpose:
- Contractors
Purpose:

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

The privacy risk is inadvertent disclosure of PII to the public. This risk is minimized because only minimal PII, identified in section 3.1, is required for collection. In addition, authorized OS Information and Publishing branch staff review information collected and redact PII submitted that is not required by the SEC to submit a comment for a proposed rule. Only the name of the commenter is published with the reviewed comment.

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

Privacy Impact Assessment

Comment Letter Log (CLL)

SORN SEC-26, Mailing, Contact and Other Lists is not provided to individuals prior to collection but is published in the Federal Register and available on the SEC's website, www.sec.gov.

- Privacy Impact Assessment

The CLL PIA is not provided to individuals prior to collection, but is available on the SEC's website, www.sec.gov.

Date of Last Update:

- Web Privacy Policy

- Other notice:

SEC Web Site Privacy and Security Policy at <https://www.sec.gov/privacy.htm>

- 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 risk of insufficient notice to individuals is minimal because adequate notice is provided as identified in section 4.1.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

Comment Letter Log does not analyze data.

5.2 Will internal organizations have access to the data?

- No
 Yes

Organizations: All SEC Divisions and Offices who have access to EDW.

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

The risk to privacy from internal sharing via EDW is inadvertent or unauthorized disclosure of PII. This risk is minimized because access to EDW is only permitted to users who have authenticated to the SEC network.

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.

There is no risk to privacy from external sharing because data is not shared with external entities.

Section 6: Data Quality and Integrity

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

- Directly from the individual.

Privacy Impact Assessment

Comment Letter Log (CLL)

- Other source(s): Comments are submitted (collected) via SEC.gov comment portals from members of the public.

6.2 What methods will be used to collect the data?

CLL uses data collected via web forms on the SEC.gov website, email, and paper copy.

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

Information provided in comment submissions is not checked for accuracy or completeness. However, each comment submission is manually reviewed upon receipt by the CLL Web Operations Team within the OS Information and Publishing Branch.

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?

There is minimal risk to privacy from related to data quality and integrity. Comments are manually reviewed upon receipt by the CLL Web Operations Team and excessive PII and vulgarity is redacted before publishing comments for public viewing.

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 may voluntarily provide comments to the SEC via SEC.gov.

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

Individuals who wish to access their information may submit a request in writing to the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-2736.

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

Individuals do not have the ability to directly amend information about themselves in CLL. However, if individuals submit public comments containing incorrect information about themselves (e.g., contact information), they may submit a subsequent public comment with amended information. In addition, individuals may submit a written request to the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-2736.

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

Privacy risk related to participation and redress is minimal because participation is voluntary, and individuals may submit a subsequent public comment with amended information or submit a written request to the SEC as identified in section 7.3.

Privacy Impact Assessment

Comment Letter Log (CLL)

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:

8.3 Does the site have a posted privacy notice?

- No
- Yes

- 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

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
- Yes

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.

The expected residual risk related to access is minimal because authentication, access control, and encryption are employed as described in section 8.4. In addition, CLL is not accessible outside of the SEC network.

