U.S. Securities and Exchange Commission

Commission Action System (CAS)
PRIVACY IMPACT ASSESSMENT (PIA)

February 22, 2022

Office of the Secretary

Privacy Impact Assessment

Commission Action System (CAS)

Section 1: System Overview

1.1 Name of Project or System

Commission Action System (CAS)

1.2 Is the system internally or externally hosted?

☒ Internally Hosted (SEC) Office of the Secretary (OS)

☐ 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: 10/1/2014

Last updated: 4/14/2020

Description of update: Commission Action System (CAS) 4.7.0.1 system updated legacy CAS, Release Log (RELLOGG), and Comment Letter Log (CLL). The latest update, CAS 4.7.0.1, includes enhancements to Memo Request and Notification functionalities.

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

☒ 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

Office of the Secretary (OS) hosts CAS data. CAS version 4.0 replaced legacy CAS and integrated RELLOG and CLL. The CAS database stores memoranda, release log records and agendas for executive, open, and closed meetings. CAS allows OS to perform administrative functions including tracking of commission votes on action memoranda, monitoring and processing of seriatim memos, tracking of advice memoranda, and scheduling and management of SEC meetings. In addition, CAS allows OS to receive, store, manage, publish, and process public comments related to SEC releases received from various SEC.gov web forms. SEC web forms (or HTML forms) allow members of the public to submit comments for processing. The SEC publishes its views and interpretation of federal securities laws and SEC regulations via interpretive releases and issues concept releases to solicit the public's views on securities issues and to evaluate the need for future rulemaking.

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*

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 privacy risks related to the purpose of the collection include personal information is collected without a clear purpose or without clear legal authority. This risk is mitigated by collecting information as authorized and in accordance with the collection purpose identified in SORN SEC-26.

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: Commenting members of the public will occasionally provide information that is not solicited by the SEC. Examples of the types of information that have been provided include financial account numbers and Social Security numbers. This information is redacted from the published version of the comments.

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: Commenting members of the public will occasionally provide information that is not solicited by the SEC. Examples of the types of information that have been provided include home address and personal telephone number. This information is redacted from the published version of the comments.

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: In addition, commenting members of the public will occasionally provide information that is not solicited by the SEC. Examples of the types of information that have been provided include work address, work telephone number, and professional affiliation. These are not considered PII and are not redacted from the published comments.

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?

PII is collected in order to associate an individual submitting a comment with a particular comment received. Members of the public provide name and email address when providing comments via SEC.gov comment portals with the option to provide address and professional affiliation.

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

☐ SEC Employees
Purpose:

☐ SEC Federal Contractors
Purpose:

☐ Interns
Purpose:

☒ Members of the Public
Purpose: As part of the comment submission process.

☐ 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.

PII is not used for system testing, training, or research. Submitters are instructed on the web form itself to only submit information they wish to be made publicly available. OS Program Staff review all submissions and redact PII upon discovery.

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

☐

☒ Yes.
GRS 4.1 item 010 *Tracking and Control Records* applies, and the records are permanent.

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

Information in CAS is not purged due to the varied research requests OS receives.

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 minimal PII is collected, as provided directly by the individual, and only the name of the comment submitter is published. No other PII is published or shared.

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
SORN SEC-26
☐ Privacy Impact Assessment
Date of Last Update:
☒ Web Privacy Policy
SEC.gov website at https://www.sec.gov/cgi-bin/ruling-comments
For SEC internal users, the OFMW login banner at https://login.sec.gov/login/faces/login.jsp
☒ 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 privacy notice is provided via SORN SEC-26 and is posted on the web form comment submission pages that collect the information that appears in CAS.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

The CLL Web Operations Team (business users) manually reviews comments entered by individuals for inappropriate language only. The application does not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

5.2 Will internal organizations have access to the data?

☒ No
☐ Yes
Organizations:

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

The risk is inadvertent disclosure of personal information to unauthorized internal parties. This risk is minimized because individuals are required to provide only a minimal amount of PII (i.e., name, e-mail) in order to submit a comment. In addition, OS personnel reviewing CAS submissions are trained in the handling of PII and do not share CAS information internally to unauthorized personnel.

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 CAS does not share data 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.
☐ Other source(s):

6.2 What methods will be used to collect the data?

Data is collected via web forms, email, and paper copy as described in the comment submission guidelines on SEC.gov. Comments received on physical paper are converted to PDF prior to posting on the SEC website.

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

Submissions from SEC.gov web forms are accepted into CAS upon system validation. Information contained 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 for vulgarity, appropriateness, and PII and may be rejected or redacted as a result.

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?

The risk related to data quality and integrity is that inaccurate information may be collected in comments submitted by an individual via SEC.gov. This risk is minimized by manual review of comment submissions as described in section 6.3.

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.

Privacy notice posted on SEC web forms provides individuals the option to opt out from providing information to the SEC. Privacy notice is also posted on the CAS portal.

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

Individuals seeking notification of or access to any record contained in this system of records 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 CAS. 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. Standard FOIA/PA procedures also apply as previously discussed.

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

There are no identified privacy risks related to individual participation. No mitigation actions are recommended. SORN SEC-26 provides procedures to access and amend records in this system.

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 https://www.sec.gov/privacy.htm
In addition, each online comment form has a privacy notice.
☐ 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 is low because a minimal amount of information is collected on a voluntary basis and the information resides on a secure system with no external sharing.