U.S. Securities and Exchange Commission

General Support System (GSS)
PRIVACY IMPACT ASSESSMENT (PIA)

July 1, 2024

Office of Information Technology

Privacy Impact Assessment
General Support System (GSS)

Section 1: System Overview

1.1	**Name of Project or System**

General Support System (GSS)

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: 1/1/2005
Last updated: 2/9/2022
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
☐ 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 GSS, maintained by the SEC OIT, provides connectivity to SEC sites throughout the continental United States. In addition, the GSS includes internal systems and devices to support the processing of data on the SEC network.

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

The SEC collects the information pursuant to 5 U.S.C. 301; 5 U.S.C. 302; 15 U.S.C. 78d et seq.; 44 U.S.C. 3101; departmental regulations; and records management by agency heads.

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
The GSS is not considered a Privacy Act system of record. However, the systems and applications within the GSS have the appropriate SORNs, as necessary.

☐ Yes, a SORN is in progress
☐ Yes, there is an existing SORN

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 identified are unauthorized access or unauthorized disclosure of SEC non-public information contained in the GSS. To minimize these risks, secure authentication to the SEC network and access controls are employed to restrict user/system/services access to only information needed to perform system functions or assigned user 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.

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: Ticket number		

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: Division Office		

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: Device identifiers; serial number

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

Personally identifiable information (PII) is used and maintained in the GSS to perform system support functions.

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

☒ SEC Employees

Purpose: To determine who is accessing information contained within the GSS.

☒ SEC Federal Contractors

Purpose: To determine who is accessing information contained within the GSS.

☐ Interns

Purpose:

☐ Members of the Public

Purpose:

☐ 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 ingested from internal SEC systems is minimized at the source collection point and is not used for testing, training, or research efforts. The PIA for each source system describes PII minimizing mechanisms employed.

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

☐ No.

☒ Yes.

DAA-GRS-2013-0006-0002 Computer Security Incident Handling, Reporting and Follow-up Records

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

Procedures for identification and disposition are:

1. Destroy three years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded.

2. Longer retention is authorized, if required for business use.

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?

There is risk of users accessing information that falls outside of their work role and need to know. To mitigate this risk, access to information is restricted by employing role-based access control.

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
While the GSS does not require a Privacy Act Statement, one is provided in the source system prior to the collection of PII.

☒ System of Records Notice
The GSS is not a system of record as defined by the Privacy Act of 1974, as amended. However, the GSS supports Privacy Act systems of records. SORNs for source systems of records are available on the SEC privacy site.

☐ Privacy Impact Assessment
Date of Last Update:

☐ Web Privacy Policy

☐ Other notice:

☐ 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?

There is minimal risk to privacy regarding notice because notice is adequate as described in section 4.1.

Section 5: Limits on Uses and Sharing of Information

5.1   What methods are used to analyze the data?

The GSS does not analyze data. However, the PIA for each GSS source system discusses methods used to analyze data as applicable.

5.2	**Will internal organizations have access to the data?**

☐ No
☒ Yes
Organizations: All SEC divisions and offices have access to data in GSS applications.

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

The risk to privacy related to internal sharing in minimal because role-based access control is employed.

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 externally.

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):   The GSS is the underlying infrastructure in which SEC applications and services reside. Data is collected by the applications and services themselves, but not directly by the GSS.

6.2	**What methods will be used to collect the data?**

The PIA for source systems and applications, that reside within the GSS, describe the methods used to collect data as applicable.

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

Data ingested from source systems and applications supported by the GSS is assumed to be accurate and is not checked for accuracy and completeness by the GSS. The PIA for each source system describes how data is checked for accuracy and completeness.

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

☒ No
The GSS does not directly access PII from other SEC systems. However, PII obtained from other SEC systems may be processed by the GSS.
☐ 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 risk of inaccurate data ingested to the GSS. The risk is minimized by data integrity and quality control checks performed as described in the PIA for each source system of information ingested into the GSS. Only

authorized OIT personnel are allowed to access the GSS to minimize risk to data quality and integrity of information ingested and processed by the GSS.

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 opportunity for individuals to opt out or decline to provide their information for use by the GSS because information is not collected from individuals but ingested from source systems.

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

An individual may make a request under the Privacy Act for access to information maintained by the SEC about themselves by submitting a request in writing to the FOIA/PA Office, 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 may not directly amend information about themselves in the GSS. However, they may submit a request in writing 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?**

There is minimal risk related to individual participation and redress because individuals seeking to correct information about themselves in the GSS may submit a request in writing to the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-2736.

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

9.5   **Does the system employ audit logging or event logging?**

☐   No

☒   Yes