U.S. Securities and Exchange Commission

EntryPoint
PRIVACY IMPACT ASSESSMENT (PIA)

March 29, 2023

Office of the Chief Operating Officer

Privacy Impact Assessment

EntryPoint

Section 1: System Overview

1.1 Name of Project or System

EntryPoint Version 5.8.3.8506

1.2 Is the system internally or externally hosted?

☒ Internally Hosted (SEC) Office of Support Operations (OSO)

☐ 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: 11/17/2017

Last updated: 7/20/2020

Description of update: The latest update include bug fixes, stylistic changes to the Pre-Registration Portal, improved application responsiveness, configuration and customization abilities for administrators, and a change to the security manager's role to include the ability to run reports..

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

EntryPoint Version 5.8.3.8506 is a commercial off-the-shelf (COTS) electronic management system hosted internally by the Office of Support Operations (OSO) and owned by the Office of the Chief Operating Officer, OSO, and the Physical Security & Emergency Management (PSEM) Operations Branch. Pre-reregistration, same-day visitor registration, entrance validation, tracking, and reporting are all done through the system. EntryPoint allows physical security personnel at the Securities and Exchange Commission (SEC) to register visitors and SEC staff (employees and contractors) to pre-register visitors and receive notification upon arrival. The solution enables SEC Headquarters security personnel to view real-time visitor activities in the eleven regional offices and reduces data re-entry at pre-registration for previous SEC visitors.

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

5 U.S.C. 301, Executive Order 13231, and Homeland Security Presidential Directive-12 (HSPD-12)

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
SORN SEC-23,Visitor Badge and Employee Day Pass System

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 primary privacy risk is that personal information collected to enable an individual to visit an SEC facility could be used inappropriately for another purpose. This risk is mitigated by limiting the information collected to what is necessary to document an individual's visit to an SEC facility and by clearly stating the purpose for collecting information in SORN SEC-23.

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: Country Representing		

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: Company Name, Visit Details (Time, Date, Location Of Visit, Event Name)		

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?

Visitors will be pre-registered in EntryPoint by SEC staff. A visitor sponsor (anyone in the SEC with network access) logs into the SEC network and navigates to the pre-registration webpage. The sponsor enters all required information, including non-sensitive PII, into the EntryPoint database to pre-register visitors, including the visitor's name and photograph, if available. When the visitor arrives, the guard staff will be able to look up the visit record. Furthermore, if an SEC employee or authorized on-site contractor requires a printed temporary badge, they must present ID (name, driver's license, and/or passport) and their identity will be verified against the SEC Active Directory (AD). EntryPoint, does not exchange data with any other system. Data will be stored on the SEC network in a SQL database. The EntryPoint 5.8 system will be accessible only within the SEC network through single sign-on authentication with AD authentication.

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

☒ SEC Employees
Purpose: Employee information is collected to validate that the user is permitted to pre-register visitors.

☒ SEC Federal Contractors
Purpose: Contractor information is collected to validate that the user is permitted to pre-register visitors or for in person registration as a visitor.

☒ Interns
Purpose: Intern information is collected to validate that the intern is permitted to pre-register visitors or for in person registration as a visitor.

☒ Members of the Public
Purpose: Information is collected for pre-registration or in person registration as a visitor.

☒ Employee Family Members
Purpose: Information is collected for pre-registration or for in person registration as a visitor.

☒ Former Employees
Purpose: Information is collected for pre-registration or in person registration as a visitor.

☒ Job Applicants
Purpose: Information is collected for pre-registration or for in person registration as a visitor.

☒ Vendors
Purpose: Information is collected for pre-registration or for in person registration as a visitor.

☐ 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.

Only the necessary PII (visitor name, company, and country represented) is collected in order to allow entry into SEC facilities. Required fields (first and last name) are indicated with an asterisk. Only non-sensitive PII is retained (visitor name, company, and country represented) in the system. PII is not used in or for testing, training, or research efforts.

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

☐ No.

☒ Yes.

GRS 5.6 Item 111, data retention period of two (2) years.

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

When a visitor leaves the SEC facility, all printed temporary badges are destroyed. All other records are stored electronically in the EntryPoint 5.8 system, which has a disposition feature that allows records to be automatically deleted after two years. Visitors will be photographed upon each new visit and given a temporary badge. EntryPoint 5.8 does not exchange data with any other system. Data will be stored on the SEC network in a SQL database. Within the SEC network, the EntryPoint 5.8 system will only be accessible via single sign on authentication with AD.

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

☐ N/A

☒ Members of the Public

Purpose: Members of the Public who visit SEC facilities are monitored while in the building and checked in and out of the facility. A record of visit is retained.

☐ Employees

Purpose:

☐ Contractors

Purpose:

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

The primary privacy risk is the collection of excessive PII. This risk is mitigated by the business decision to not collect sensitive PII (such as a social security number (SSN)) and to collect only the minimally required PII to facilitate access to SEC facilities. The system retains only the visitor name, company, and photograph. In addition, the country for which visitor represents and visit date/time is retained. All printed temporary badges are destroyed when the visitor leaves the SEC facility.

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

A Privacy Act Statement is posted or provided at all guard stations that process visitors in SEC Headquarters and regional offices.

☒ System of Records Notice

SEC 23 "Visitor Badge and Employee Day Pass System" is not provided to individuals prior to collection, but is published in the Federal Register and is available on the SEC's website www.sec.gov.
85 FR 85440 (January 27, 2021)

☒ Privacy Impact Assessment

The EntryPoint PIA is not provided to individuals prior to collection, but is available on the SEC's website.
Date of Last Update: 12/4/2018

☐ Web Privacy Policy

☒ Other notice:
Visitors are verbally informed they will not be allowed entry to SEC facilities if PII is not provided.
☐ 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 risk is that visitors will not be able to make an informed decision on whether to provide the information requested and may be unaware of what information is collected to fulfill the requests. This risk is mitigated by clearly stating the purpose for collecting and sharing the personal information in the SORN, PIA, and at guard stations.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

EntryPoint does not analyze data.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes
Organizations: Office of Inspector General (OIG), Office of the General Counsel (OGC), and other SEC divisions and offices may receive reports from the system when there is a business need or investigatory purpose.

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

The risk to privacy from internal sharing is inadvertent disclosure. This risk is minimized because information is shared internally to the SEC offices listed above only when there is a business need or for internal investigation.

5.4 Will external organizations have access to the data?

☐ No
☒ Yes
Organizations: Data may be disclosed to external organizations for law enforcement purposes upon request.

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

The risk to privacy from external sharing is minimal to none because visitor information is only shared, upon request, to law enforcement organizations.

Section 6: Data Quality and Integrity

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

☒ Directly from the individual.
An individual may provide their information directly at the guard station in SEC buildings.
☒ Other source(s): An individual may give their information to an SEC employee or contractor for pre-registration in the system.

6.2 What methods will be used to collect the data?

The data is collected in-person at the guard station or via pre-registration through an SEC employee or contractor.

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

Data collected from individuals such as name and country represented may be verified against the information provided on the visitor's valid identification. Data such as company name, phone number, and email address may be verbally verified with the visitor.

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

☐ No

☒ Yes.

Outlook Global Access List (GAL) to verify SEC employee or contractor being visited. AD for user authentication.

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 data quality and integrity as visitors are the primary source of PII collected. Visitors provide the data directly to the SEC guard or to SEC staff for pre-registration. Visitors must present a valid ID (i.e., state or federal government issued photo identification) upon arrival to the SEC that can be used to verify collected information.

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 decline to provide the information requested, though failure to do so would result in denial of access to SEC facilities. They do not have the opportunity to consent to the uses of the information provided.

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

At the time of visit, individuals can note corrections or changes to their PII by contacting the security concierge staff or the Office of Security Services.

In addition, persons wishing to obtain information on the procedures for gaining access to or contesting the contents of these records may contact the FOIA/PA Officer Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549 or foiapa@sec.gov.

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

Individuals can note corrections or changes to their PII by contacting the security concierge staff or the Office of Security Services at the time of visit.

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

There is a privacy risk that information in EntryPoint may be inaccurate. However, because the individual has the opportunity to verify the information at the time of visit and correct errors, the risk is minimal.

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
Reports are generated only when requested by the host of a meeting, OIG, or OGC.

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.

There is minimal residual risk related to access to the non-sensitive personal information residing in the system. Access to the EntryPoint system is limited to all SEC authorized users connecting from within the SEC network only. In addition, the EntryPoint workstation located at the guard station in SEC buildings are under direct oversight of SEC PSEM Operations at all times.