U.S. Securities and Exchange Commission

EntryPoint System
PRIVACY IMPACT ASSESSMENT (PIA)

12/4/2018

Office of the Chief Operating Officer
Office of Support Operations

Section I: System Overview

1.1 Name of Project or System

EntryPoint 5.8

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:
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

The EntryPoint 5.8 system is an electronic management Commercial Off-the-Shelf (COTS) system internally hosted and used by the Office of Support Operations (OSO) to identify, register, badge, and track visitors to the SEC Headquarters and its eleven regional offices. The system consists of hardware and software components. The system is owned by the Office of the Chief Operating Officer, Office of Support Operations, and the Physical Security & Emergency Operations Branch. The system is needed to protect the physical safety of SEC information, staff, and contractors. The information stored on the system includes a visitor's name, company, citizenship status, and details regarding the visit, such as arrival/departure times, and the name of person visited. EntryPoint scans the barcodes of driver's licenses and/or passports and reads the person's name from the code and fills in the name fields on the application screen.

Two basic transactions will be made on the system:

(1) Individuals will be photographed, identified, and provided temporary badges at an SEC front desk with data retained for future reference. Upon an individual's visit onsite, the visitor will supply a security guard with ID information (name, driver's license and/or passport) in a visitor record at the Guard workstation. A name check is conducted against the OSO's list of individuals who are not authorized to access the SEC. Typically these individuals are employees or contractors

that have been separated from the SEC or have been deemed to represent a security concern. The Office of Security Services, in collaboration with other SEC offices and divisions, as needed, makes this determination and maintains this list in EntryPoint. If the name is not on the list, the visitor registration continues. If the visitor's name appears on the list, an email notification is sent from the EntryPoint server to the EntryPoint administrators and the guard views a notice on the workstation screen that prohibits the visitor from entering the premises.

The name of the person that the individual is visiting is verified against the Active Directory (AD). Once the visitor is checked in, a temporary visitor badge is printed. The visitor sponsor is notified to come an escort the visitor inside the building. When the visitor leaves for the day, the badge is scanned at the guard workstation, collected back, and the visit record is closed out in the database.

(2) SEC staff will pre-register visitors in EntryPoint. A visitor sponsor (any person in the SEC with network access) logs into the SEC network and goes to the pre-registration webpage inside the SEC network. The sponsor enters in the EntryPoint database all the required information with non-sensitive PII to pre-register visitors to include the visitor's name, and photograph, if available. The visit record will be available to the guard staff to look up when the visitor arrives. Upon an individual's visit on-site at SEC Headquarters or a Regional Office the same process as described in (1) above is followed to issue a temporary badge to the visitor.

Additionally, if an SEC employee or authorized on-site contractor needs a printed temporary badge, they will present ID information (name, driver's license and/or passport) and their identity will be verified against the AD. If they are authorized for a temporary badge, a temporary badge record will be entered and submitted to the EntryPoint 5.8 database. When the employee or contractor leaves for the day, the temporary badge will be checked back in at the guard workstation and then the temporary badge will be closed out in the EntryPoint 5.8 database.

All printed temporary badges are destroyed when the visitor leaves the SEC facility. All other records are stored electronically within the EntryPoint 5.8 system, which has a disposition feature to facilitate automatic deletion of records after two years. Upon each new visit, visitors will be photographed when issued a temporary badge.

EntryPoint 5.8 does not share information with any other system. Data will be stored on an SQL database on the SEC network. The EntryPoint 5.8 system will only be accessible within the SEC network via single sign on authentication with AD authentication. There is no public access to the system.

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 or collect 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-52, "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 identified is that personal information provided for one purpose may be used inappropriately for another purpose. This potential risk is mitigated by clearly stating the purpose for collecting the personal information in the applicable SORNs, privacy impact assessments, and other notices, and limiting the information collected to what is truly necessary for intended purposes.

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: Click here to enter text.

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 , SEC Point of Contact (name, phone number from Active Directory)

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 and date of visit)		

Distinguishing Features/Biometrics

☐ Fingerprints	☒ Photographs	☐ Genetic Information
☐ Voice Recording/Signature	☐ Video Recordings	
☐ Other:		

System Administration/Audit Data

☐ User ID	☐ Date/Time of Access	☐ ID Files Accessed
☐ IP Address	☐ Queries Run	☐ 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?

The PII listed is collected to verify and document the visitor's identity in order to allow access to SEC's facilities. The security guard can verify the visitor's identity and check that identity against the Banned list of individuals barred from SEC property. The Banned list is a list of people that the OSO group maintains. OSO owns the rules and procedures for this list outside of the EntryPoint 5.8 system. The SEC point of contact information (name and phone number from Active Directory) is collected in order to contact the visitor's escort and for future verification of identity. The nationality is collected for reporting purposes and to display on badge for selected conferences.

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

☒ SEC Employees
Purpose: To validate that the user is permitted to pre-register visitors or to obtain a temporary badge.

☒ SEC Federal Contractors
Purpose: To validate that the user is permitted to pre-register visitors or, if not an SEC badge holder, to register as a visitor.

☒ Interns
Purpose: To validate that the user is permitted to pre-register visitors or, if not an SEC badge holder, to register as a visitor.

☒ Members of the Public
Purpose: To register as a visitor

☒ Employee Family Members
Purpose: To register as a visitor

☒ Former Employees
Purpose: To register as a visitor

☒ Job Applicants
Purpose: To register as a visitor

☒ Vendors

Purpose: To register as a visitor

☐ Other:
Purpose:

3.4 What mechanisms are in place to minimize the use of PII for testing, training, and research efforts?

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?

All printed temporary badges are destroyed after the visit. All other records are stored electronically within the EntryPoint 5.8 system, which has a disposition feature to facilitate automatic deletion of records after two years.

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

☐ N/A

☒ Members of the Public
Purpose: Visitors will be checked into and out of the SEC facility.

☒ Employees
Purpose: If the employee is sponsoring a visitor, a record of the visit will be retained.

☒ Contractors
Purpose: Visitors will be checked into and out of the SEC facility; if the contractor is sponsoring a visitor, a record of the visit will be retained.

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 unnecessary collection of PII, which increases risks of unwarranted use or access. This risk is mitigated with the decision not to collect sensitive personally identifiable information, e.g. social security numbers and to collect only the minimally required PII to facilitate access to SEC facilities. The system retains only the name, company, visitor's photograph for badge, visitor's nationality, and details of the visit (time and date). In effort to mitigate risks from collection of non-sensitive PII, all printed temporary badges are destroyed when the visitor leaves the SEC facility. All other records are stored electronically within the EntryPoint 5.8 system, which has a disposition feature to facilitate automatic deletion of records after two years.

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 52 "Visitor Badge and Employee Day Pass System"

☒ Privacy Impact Assessment
Date of Last Update: In progress

☐ 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 these 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 applicable SORN(s), privacy impact assessments, and other applicable notices. **.** Also, visitors have access to written notice before visiting and verbally notified upon their visit to verify their identity. All visitors have the option of not providing this information at the risk of not being allowed access to SEC facilities.

Section 5: Limits on Uses and Sharing of Information

5.1 What types of methods are used to analyze the data?

The system does not analyze the data that is collected. The data is used only for display on a visitor's badge and reports of an individual's visit history to the SEC. The system does not otherwise analyze or derive new information from the information collected.

5.2 Will internal organizations have access to the data?

☐ No

☒ Yes

Organizations: OIG, OGC, and other offices may receive reports from the system when there is a business need or investigatory purposes.

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

Privacy risks associated with internal sharing are that individuals may feel a loss of control over what information is collected and may be surprised or upset by an unanticipated secondary use that may involve fulfilling requests from OIG for information on an individual's visits to an SEC facility. This risk is mitigated by clearly stating the purpose for collecting and sharing the personal

information in the applicable SORNs, privacy impact assessments, and other notices.

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 are no potential privacy risks from external sharing as personal information will not be accessed by external 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.
☒ Other source(s): Visitors may give their information directly to guards at the lobby desk or they may give their information to an SEC employee/contractor who will pre-register the visitor in the system.

6.2 What methods will be used to collect the data?

The data is collected via in-person visitor registration or pre-registration by SEC staff. The record is created in person at the time of visit.

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

Data on individuals is immediately verified by the individual examining the issued badge. Details on individual visits (time and date of visit) are recorded automatically.

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

☐ No
☒ Yes.
System(s): Global Access List to verify SEC person being visited.
Active Directory 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 the individual's privacy as only non-sensitive PII (name, company, and nationality) are retained. Photograph(s) are not retained. Visitors are the primary source of PII related to them. Visitors provide the data directly to the SEC guards or to SEC staff to pre-register them. Additionally, all individuals requesting access to SEC facilities must present a valid ID upon arrival to the SEC.

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.
Prospective visitors do not have the opportunity to consent to the uses of the information provided. They are provided notice of the uses of the information via this PIA and SORN SEC-52. Visitors may decline to provide the information requested though failure to do so would result in denial of access to SEC facilities.

7.2 What procedures will allow individuals to access their information?
The individual's PII is accessed and visually validated on credentials at time of visit. The individual's PII is recorded in EntryPoint 5.8. 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.

7.3 Can individuals amend information about themselves in the system? If so, how?
Individuals can correct errors in their record (e.g. name spelling) by contacting the security concierge staff or the Office of Security Services.

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 Has the system been authorized to process information?

☒ No

SA&A Completion Date: Click here to enter a date.

Date of Authority to Operate (ATO) Expected or Granted: **Pending the Authorization to Operate**

8.2 Identify individuals who will have access to the data in the project and state their respective roles.

☒ Users

Roles: Register visitors, search database for information on previous visits, pre-register individuals.

☐ Contractors

Roles: Register visitors, search database for information on previous visits, pre-register individuals.

☒ Managers

Roles: Create user accounts, generate reports, and update the Banned list.

☒ Program Staff

Roles: Check in visitors and issue visitor badges; issue temp badges to employees and contractors when PIV cards forgotten; manage conference registration; reporting; manage Watch List; and manage staff access to the EntryPoint guard workstation application

☐ Developers

Roles:

☒ System Administrators

Roles: Configure the system, back up the system, record disposal.

☐ Other

s:

Roles:

8.3 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

8.4 How will the system be secured?

The SQL database is encrypted internally. Security staff workstations will be under direct oversight of SEC security personnel at all times. The entire system is within the SEC network with no external connections. Access is controlled via Single Sign On and group access permissions on the application server.

8.5 Does the project or system involve online collection of personal data?

☒ No

☐ Yes

Public URL:

8.6 Does the site have a posted privacy notice?

☐ No

☐ Yes

☒ N/A

8.7 Does the project or system use web measurement and/or customization technologies?

☒ No

☐ Yes but they do not collect PII

☐ Yes and they collect PII

8.8 Describe any privacy risks for this system that relate to the technology and security of the system and how those risks are mitigated.

Privacy risks associated with this technology include unauthorized disclosure of PII or unauthorized access to the badge issuance capability which could impact the security operations within the agency. These risks are mitigated by installing EntryPoint 5.8 only on one security guard workstation thereby limiting the authorized user access to the security staff located at Station Place and the Operations Center. Also, risks are mitigated by hosting the database physically

within the confines of a secured SEC facility, protecting the server behind SEC firewalls, and restricting database access using standard SEC security policies limited to database administrators.

Moreover, EntryPoint 5.8 uses an internally, hosted COTS solution that does not share PII collected with other SEC organizations as the system is not connected to any other systems outside the SEC network. Privacy risk is minimal as only non-sensitive PII is retained (e.g. name), access to personal information is restricted to concierge staff and administration staff, data is not shared with other SEC organizations, and the entire system is within the SEC network.

Section 9: Accountability and Auditing

9.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system or project.

All users receive standard SEC annual privacy training via LEAP. In addition, the standard security guard training includes a module on protection of individual privacy in the performance of all security guard duties.

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

☐ No
☒ Yes

A PIV card and password is needed in order to access the system. Reports are not automatically generated so there is no retention schedule. Reports are only pulled based on a request from a host of a meeting, the Office of Inspector General or General Counsel. The reports are disposed of based on the need of no longer needing the information.

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

The EntryPoint 5.8 tool provides audit logs tracking check-in and check-out of all visitors and the identity of staff executing these transactions. Access to these logs is restricted to Administrative personnel in the Security Office.

9.5 What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of the data? What mechanisms are in place to identify security breaches?

SEC Security Policy is in place in order to access workstations. Access to personal information is restricted to the concierge staff and administrative personnel.

9.6 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. Security staff workstations will be under direct oversight of SEC security personnel at all times. All users who have access to the data have had background checks, signed non-disclosure agreements and will have attended Privacy Awareness Training prior to using EntryPoint 5.8. The entire system is within the SEC network with no external connections. Access is controlled via Single Sign On and group access permissions on the application server.