U.S. Securities and Exchange Commission

LEAP Extended (LEAP-EX)
PRIVACY IMPACT ASSESSMENT (PIA)

April 23, 2020

Office of Human Resources

Privacy Impact Assessment

LEAP-EX

Section I: System Overview

1.1 Name of Project or System

LEAP Extended (LEAP-EX)

1.2 Is the system internally or externally hosted?

☐ Internally Hosted (SEC)

☒ Externally hosted (Contractor or other agency/organization): Contractor: Cornerstone On Demand (CSOD)

1.3 Reason for completing PIA

☒ New project or system

☐ This is an existing system undergoing an update

First developed: 6/2/2017

Last updated:

Description of update:

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

☐ Electronic 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

LEAP-EX is a new external-facing portal of the internal LEAP system which enables new hires access to SEC training courses through the Extended Enterprise module prior to their onboarding at the SEC. This means that contractors and other SEC workers can complete relevant and mandatory training before beginning their period of performance with the SEC and prior to obtaining access to SEC information and information systems.

New SEC employees will be registered for the PISA training with their LEAP-EX account in advance of their onboarding date. During New Employee Orientation the new employees log into LEAP-EX and complete the training during the session.

Other worker types (contractors, detailees, student volunteers, etc.) upon receipt of Interim Suitability from Personnel Security, the Contracting Officer or Program Coordinator will distribute an email with instructions for an individual to self-register through LEAP-EX.

LEAP-EX creates a daily transcript via outbound data feed which auto loads into the existing LEAP internal system.

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

5 U.S.C. § 4103, Establishment of Training Programs

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-39 "Personnel Management Employment and Staffing Files"

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 risks are that personal information may be collected without a clear purpose or without sufficient legal authority; information collected may be either unnecessary or excessive; or the information provided for one purpose may be used inappropriately. These potential risks are mitigated by clearly stating the purpose for collecting the personal information in the applicable SORNs, PIAs, and other notices, and limiting the information collected to what is truly necessary for the 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:		

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:		

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 document the SEC workforce's completion of privacy and information security (PISA) training prior to start date and to support recruiting and onboarding processes.

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

☒ SEC Employees
Purpose: Basic account information containing names and SEC email addresses is required for the purpose of supporting the extended enterprise module.

☒ SEC Federal Contractors
Purpose: Basic account information containing names and SEC email addresses is required for the purpose of supporting the extended enterprise module and maintaining auditing information related to completion of mandatory training.

☒ Interns
Purpose: Basic account information containing names and personal and/or SEC/contractor email addresses is required for the purpose of supporting the extended enterprise module and maintaining auditing information related to completion of mandatory training.

☒ Members of the Public
Purpose: Basic account information containing names and personal email addresses is required for the purpose of self-registering for creating an account to complete mandatory training during the onboarding process prior to the employee's first day at SEC.

☐ Employee Family Members
Purpose:

☒ Former Employees
Purpose: After an employee has departed, the user record is deactivated. The user record includes basic account and organizational data, which contains names and SEC/contractor/personal email addresses, for the purposes of maintaining the auditing information related to actions taken by the user.

☐ Job Applicants
Purpose:

☐ Vendors
Purpose:

☐ Other:
Purpose:

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

If live PII is used, an authorization to test is required from the CIO/SAOP.

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

☒ No.
OHR is working with the Office of Records Management Services to schedule the official records.
☐ Yes.

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

At this time, there is no records schedule number. The OHR is working with the Office of Records Management Services to schedule the official records. Records will be maintained until they become inactive, at which time they will be destroyed or retired in accordance with the SEC's published records disposition schedules, as approved by the National Archives and Records Administration (NARA).

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 primary privacy risk is unnecessary collection of PII, which increases risks of unwarranted use or access. This risk is mitigated by importing into each module only PII that is directly relevant and necessary to accomplish the authorized purpose of each module, and also, implementing role-based access controls. System Administrators' access permissions are restricted to the organizations for which they are responsible. Other SEC users' access is limited to review only their data, or, if the user supervises employees, to review data of their subordinates.

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-39 "Personnel Management Employment and Staffing Files"
☒ Privacy Impact Assessment
Date of Last Update: Current PIA
☐ 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 these risks mitigated?

The primary risk is inadequate notice. Individuals may not be aware of the use of their information in the LEAP-EX system. This risk is mitigated by ensuring that applicable SORNs are current and adequately describe the uses and disclosures of information contained in LEAP-EX. The risk is also mitigated by ensuring that PIAs for LEAP-EX and interconnected systems are published and adequately describe how personal information is protected and managed in each system.

Section 5: Limits on Uses and Sharing of Information

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

Data is analyzed via search and reporting capabilities, which may present existing information in the form of reports, graphs, charts, and related management metrics. The system does not otherwise analyze or derive new information.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes

Organizations: Limited Office of Human Resources (OHR) users have access for the purposes of approving access requests and administering the system. Users are authenticated via single sign on (SSO), and therefore, must have an active directory (AD) account to access the system. In addition, a limitation of a single user also has access as an approver from the following offices: Office of Acquisition (OA), Office of Financial Management (OFM), and Office of International Affairs (OIA).

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

Privacy risks associated with internal sharing are inadvertent or unauthorized disclosure of information to individuals without authorization; and use or disclosure of personal information for reasons not directly related to the primary purpose of the collection. These risks are mitigated by implementing role-based access controls. Access permissions to System Administrators are limited to a few users.

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.

PII is not shared with external organizations in LEAP-EX.

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): Internal Leap System

6.2 What methods will be used to collect the data?

The data about new hires, such as basic account and organizational data, will be transmitted daily from the Internal Leap System via a flat file through a Secure File Transfer Protocol (SFTP) connection to LEAP-EX for

single sign on capabilities. New Hires input their first name, last name, and email address through the front-end self-registration page.

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

The SEC Self-Registration Approvers will check to ensure the data is accurate or sufficient in order to approve the self-registered accounts.

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

☐ No
☒ Yes.
System(s): The internal LEAP system

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 primary risk is that incorrect or inaccurate information may lead to inappropriate use or unwarranted disclosure. To help mitigate this risk, as appropriate, data is exchanged in a secure automated fashion from the original source and/or collected directly from the user.

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.

Necessary PII (name and work email address) is required for SEC users to access LEAP-EX in order for SSO to function. Most accounts for Student Volunteers will be created by a file load process. External users, including some Student Volunteers, will self-register to create accounts. Non-SEC employees will not have access to the system if they do not provide the required information (name and personal email address) in order to create their account.

7.2 What procedures will allow individuals to access their information?

None. Users can see some account information, which includes name, email address, and training transcript, but cannot edit their data once a self-registration account is approved. Accounts for self-registered users will be deactivated once PISA training is complete. Once training is complete, there's a daily outbound transcript data feed into the internal LEAP system which updates the corresponding user's account transcript in LEAP.

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

Self-registered users will not be able to access their information and make amendments to it.

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

Since individuals cannot amend their own information, a very slight risk exists. This risk is mitigated by allowing users to contact OHR system administrators in order to amend their information.

Section 8: Security

8.1 Has the system been authorized to process information?

☒ Yes

8.2 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

8.3 Does the site have a posted privacy notice?

☐ No
☒ Yes
☐ N/A

8.4 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
Data is analyzed via search and reporting capabilities, which may present existing information in the form of reports, graphs, charts, and related management metrics. These outputs could potentially contain information on individuals.

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

There is a risk that other clients of CSOD will be able to gain access to SEC data over the CSOD database. This privacy risk is mitigated by the fact that at CSOD, databases are never shared across tenants. Each client's database is fully segregated from other clients as each client's portal is only accessible to the client's users and authorized CSOD support personnel. Authorized CSOD support personnel are required to take the SEC's privacy and information security awareness training.

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.

The SEC provides the required privacy and security awareness training to all employees and job applicants, which equips them with information on safeguarding personally identifiable information (PII). SEC personnel who do not safeguard information contained in this system are subject to the appropriate disciplinary action.

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

☐ No
☒ Yes
Data is analyzed via search and reporting capabilities, which may present existing information in the form of reports, graphs, charts, and related management metrics. These outputs could potentially contain information on individuals.

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

OHR has the option to download daily application level audit records via SFTP. Also, all firewalls and routers log critical events such as

authentication attempts and configuration changes to a centralized syslog server for alerting and forensic analysis. LEAP-EX has an internal logging system which indexes and pulls various types of logs, including system logs and windows event logs, to a centralized server/system which Cornerstone personnel can access. Cornerstone can query the logging system and generate a report based on the defined criteria require and make it available.

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 SEC has built in adequate security and privacy controls to minimize the residual risk. Any residual risks are mitigated by the controls discussed in Section 8.4 above.