U.S. Securities and Exchange Commission

Enterprise Human Capital Repository (EHCR)
PRIVACY IMPACT ASSESSMENT (PIA)

March 22, 2023

Office of Human Resources

Privacy Impact Assessment

Enterprise Human Capital Repository (EHCR)

Section 1: System Overview

1.1 Name of Project or System

Enterprise Human Capital Repository (EHCR)

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: 4/22/2015

Last updated: 4/15/2020

Description of update: Added SEC Learn Engage Achieve Perform (LEAP) platform as new source system and created Golden record table. This is an update to the existing PIA from 8/22/2017.

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

EHCR is a single centralized repository for personnel data for the SEC workforce (employees, contractors, interns, Intergovernmental Personnel Act employees, and fellows) and other individuals that may support the Commission. EHCR provides structured information and associated data schemata. Updates to data elements in the primary location propagate to the EHCR system, eliminating the possibility of missing a duplicate value. Links to the data elements in EHCR are by reference only. For example, EHCR is used as a reference repository of all personnel records and maintains a copy of information that resides in the source Office of Human Resources (OHR) systems and applications.

Data is ingested from source systems using SEC's enterprise ETL tool, Infosphere Information Server (IIS). Source Systems and data include the following:

- US Access: Employee and contractor information including enrollment ID and status. US Access sends data to EHCR.
- Workforce Tracking and Transformation System (WTTS): Worker Information including pay position, grade, salary, clearances, and department. Data is retrieved from Department of Interior (DOI) data-mart. WTTS sends data to EHCR.
- DOI, Federal Personnel/Payroll System (FPPS): Worker Information including work schedule, security clearances, position information and work schedule. FPPS sends data to EHCR.
- LEAP learning platform: Contains information about training courses taken and completed by workers and contractors. LEAP sends data to EHCR and receives data from EHCR.

- Active Directory (AD): Contains additional worker related information such as the username AD ID, which is used for system authentication. AD supplies data to EHCR and receives data from EHCR.
- Contractor Personnel (CP) List: Repository for Contractor related information. Data includes name, email, office location, and phone number for CP and contractor project manager or point of contact (POC). CP List sends data to EHCR and receives data from EHCR.
- Archibus: Contains employee and contractor workplace location information. Data includes name, building, office/cube assignment, and other related fields. Archibus sends data to EHCR and receives data from EHCR.
- HR4ME: Employee information for various SEC benefits programs and information on employee certifications, including Certified Public Accountants (CPAs) and Bar memberships. Also includes telework agreement details: employee name, work schedule, telework agreement status, and organization name, etc. HR4ME sends data to EHCR and receives data from EHCR.
- WebTA: Employee supervisor name and division/office.

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

All legal authorities and agreements associated with the data maintained in the source system follows the data collected, used, maintained, retrieved, and disseminated within EHCR, to include the following:
5 U.S.C. 1302, 2951, 3301, 3372, 4103, 4113, and 4118; and 5 CFR part 410; 5 CFR parts 213, 293, 302, and 335 and Office of Personnel Management Regulations promulgated thereunder; and 5 CFR, parts 213, 293, 302, and 335; 5 U.S.C. 3109 and Civil Service Regulations promulgated thereunder.

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:	The primary identifier to create a record is the Enrollment ID from US Access System. The US Access System includes the SSN. OHR uses the SSN to match employees with their DOI records. In addition, the SSN is used to complete the employee record in EHCR and to match employee information from multiple ingested from source systems.
If yes, provide the legal authority:	The legal authority to collect the SSN is outlined in the specific System of records notice, including Executive Orders 9397, as amended by 13478, 9830, and 12107.

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

Since EHCR does not collect information directly from individuals and no new information is created through the system about individuals, the information contained in the source systems performing the original collection is covered by the individual SORNs for those systems as listed below:
1. US Access: GSA/GOVT-7, Federal Personal Identity Verification Identity Management System
2. WTTS: OPM/GOVT-1, General Personnel Records; and OPM/GOVT-5, Recruiting, examining and placement records
3. FPPS: OPM/GOVT-1, General Personnel Records; and OPM/GOVT-5, Recruiting, examining and placement records
4. Active Directory: SEC-26, Mailing, Contact and Other Lists

5. LEAP: SEC-10, Personnel Management Employment and Staffing and Training Files
6. CP List: SEC-33 General Information Technology Records
7. Archibus: SEC-20 Facilities Access Badge System
8. HR4ME: SEC-10, Personnel Management Employment and Staffing and Training Files
9. WebTA: SEC-07: Payroll, Attendance, Retirement and Leave Records

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?

Business Intelligence (BI) system reads specific PII data from EHCR and provides dashboards and reports to senior management personnel within OHR. The primary privacy risks are: collecting information that is either unnecessary or excessive, information provided for one purpose may be used inappropriately, and information risking future exposure if the proper processes are not followed. These risks are mitigated by restricting access to specific service accounts which are granted permissions to view EHCR data within dashboards and reports in the BI system based on approval from the business solution owner. Also, EHCR restricts data through business need specific database views to minimize the exposure of PII.

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	☐ 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 ingested from source systems and maintained in ECHR for use in internal OHR reporting and BI reports.

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

☒ SEC Employees
Purpose: For truth verification of SEC workers HR information.

☒ SEC Federal Contractors
Purpose: For verifying truth about SEC workers

☒ Interns
Purpose: For truth verification of SEC workers HR information.

☐ Members of the Public
Purpose:

☐ Employee Family Members
Purpose:

☒ Former Employees
Purpose: For truth verification of SEC workers HR information.

☐ 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.

EHCR does not collect PII, but ingests PII collected by source systems. However, EHCR uses database views to minimize the exposure of PII to that which is required for use in the system. PII is not used for testing, training, and/or research efforts.

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

☒ No.
EHCR is a system of reference, not a system of record.

☐ Yes.

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

N/A

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?

EHCR does not directly collect information but ingests information collected from source systems. Any privacy risk to the type of information collected is mitigated by source system processes and procedures.

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

SORNs for the source systems are following. However, the SORNs are not provided to individuals prior to collection, but are published in the Federal Register and available on the SEC's website, www.sec.gov.

• US Access: GSA/GOVT-7, Federal Personal Identity Verification Identity Management System
• WTTS: OPM/GOVT-1, General Personnel Records; and OPM/GOVT-5, Recruiting, examining and placement records
• FPPS: OPM/GOVT-1, General Personnel Records; and OPM/GOVT-5, Recruiting, examining and placement records
• Active Directory: SEC -26, Mailing, Contact and Other Lists
• LEAP: SEC-10, Personnel Management Employment and Staffing and Training Files
• CP List: SEC-33 General Information Technology Records
• Archibus: SEC-20 Facilities Access Badge System
• HR4ME: SEC-10, Personnel Management Employment and Staffing and Training Files
• WebTA: SEC-07: Payroll, Attendance, Retirement and Leave Records

☒ Privacy Impact Assessment

Date of Last Update: 8/22/2017 The PIA is not provided to individuals prior to collection but is available on the SEC's website, www.sec.gov.

☐ 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 no risk regarding adequate notice for EHCR. Individuals providing their information using source systems are informed of the uses of their information through that system's applicable SORN. There is no SORN or other notice for the EHCR system itself as it only serves as a centralized repository for information collected from those other sources. In addition, this PIA is publicly available and provides additional notice to individuals.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

Data is analyzed via search and reporting capabilities through the BI system, 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: Divisions/offices do not directly access data in EHCR. However, they may access limited data from EHCR downstream applications such as ServiceNow and BI.

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

There is a risk that the information in EHCR may be shared with SEC personnel who do not have a need-to-know the information to perform their work duties. The risk is mitigated by using role based access control to assign authorized users the least privileges required to perform their job functions. Prior to being provisioned access to the system, prospective users are required to sign a non-disclosure agreement (NDA).

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.

Not applicable because information 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):
1. DOI Datamart (WTTS/FPPS): This feed provides employee data and triggers for activating the employee record, including pay position, grade, salary, clearances, and department.
2. US Access: This feed provides Enrollment (ID), SSN, name, and adjudication status information.
3. LEAP: This feed provides details on completed training courses.
4. Active Directory: This feed provides employee e-mail, and office telephone number
5. CP List: This feed provides CP start date, name, email, office location, phone number.

6. Archibus: This feed provides employee and contractor workplace location information.
7. HR4ME: This feed provides employee telework agreements, and CPA and Bar membership details.
8. WebTA: This feed provides employee supervisor's name and organization.

6.2 What methods will be used to collect the data?

Data is ingested from various source systems using SEC's enterprise ETL tools. ETL jobs are executed daily by automated scripts. They may also be executed manually.

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

Data accuracy and completeness is checked by the source system which collected the data. Data updated in the source system is replicated in EHCR. EHCR does not validate or change the information received from sourced systems.

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

☐ No
☒ Yes.
System(s): Data is ingested from source systems using SEC's enterprise ETL tools for the purpose of aggregating a single view of SEC workers and contractors. Source Systems include: DOI Datamart (WTTS/FPPS), US Access, LEAP, Active Directory, CP List, Archibus, HR4ME and WebTA.

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 incomplete or inaccurate information. However, data quality and integrity is controlled by the source system. Data errors are corrected in the source system and the corrected data is ingested into EHCR.

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 do not have the option to consent, decline or opt out of having their information ingested into EHCR. Any opportunities for individuals to decline to provide information, opt out, or consent to uses of their information occurs at the point of collection from the original source system.

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

Individuals cannot directly access their information in EHCR. Information is ingested into EHCR and may be access by individuals from the source system as described in the PIA for the source system.

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

Individuals cannot directly amend information about themselves in EHCR. Information is ingested into EHCR and may be amended in the source system as described in the PIA for the source system.

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

There is no privacy risk related to participation and redress for ECHR because individual participation and redress is handled by the source system where information is collected. Any risk and mitigation is addressed in the PIA for the source system.

Section 8: Security

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

☒ No
☐ Yes
Public
URL:

8.2 Does the site have a posted privacy notice?

☒ No
☐ Yes
☐ N/A

8.3 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

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.

Although access to this system is limited only to authorized SEC staff, the expected residual risk related to access, given the sensitivity of the PII in the system, can include the inadvertent handling or misuse of data. Examples include but are not limited to the unauthorized distribution of PII, sharing of username and password credentials,

and sharing proprietary system information. To mitigate this risk, user accounts for employees are synchronized with SEC's AD and system privileges are granted based on defined roles.