U.S. Securities and Exchange Commission

Enterprise Talent Management System (ETMS)
PRIVACY IMPACT ASSESSMENT (PIA)

3/9/2018

Office of Human Resources

Section 1: System Overview

1.1 Name of Project or System

Enterprise Talent Management System (ETMS)

1.2 Is the system internally or externally hosted?

☒ Externally Hosted Contractor: Cornerstone On Demand (CSOD)

1.3 Reason for completing PIA

☒ This is an existing system

First developed: 6/2/2017

Description of update: This PIA documents privacy risks and controls to mitigate identified risks for ETMS Phase 1. ETMS Phase 2 updates are underway. This PIA will be updated to document new privacy risks as a result of any changes occurring in the system during Phase 2 implementation.

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 Enterprise Talent Management System (ETMS) is a unified talent management suite operated by Cornerstone. The solution provides the tools for the Office of Human Resources (OHR) to manage the employee lifecycle from recruiting through separation. ETMS enhances the SEC's ability to attract, engage, align, develop and retain high performing employees. The solution also enables increased strategic hiring, improved employee experiences and access to data and metrics to drive business decisions. The system is externally hosted at a FedRAMP-certified site; it will replace multiple disparate systems and automate a number of paper-based manual processes. ETMS is being implemented in two phases. This PIA assesses the privacy risks associated with phase 1. The ETMS PIA will be updated for phase 2.

Phase 1 of the project implements three modules: (1) Learning (replaced the former learning management system, Lead, Engage, Achieve, Perform (LEAP); (2) Performance Management (replacing the paper-based process); and (3) Succession (career management and workforce planning). In addition, Dashboard Reporting is included, which is attributed to all modules.

- **Learning Management Module:** All SEC federal employees and contractors will have access to the Learning Management module to complete their training requirements. This module allows users to register for instructor-led classes, take online classes, request external training, and access the Skillsoft online content training library. SEC employees are provided direct access to the system so they may plan, manage and evaluate their individual learning and career growth in alignment with office and agency strategic goals. The Learning Management module maintains and updates user records, training histories, individual development plans, course catalogs, training resources, and training requirements.
- **Performance Management**: Only SEC federal employees will have access as users to the Performance Management module. This module electronically documents performance expectations discussed by supervisors and SEC employees at the beginning of the performance period, records interim progress reviews and mid-year performance evaluations; and formally captures supervisory evaluations and employee performance ratings at the conclusion of the performance cycle. Reports may be run to help the agency identify employees who are performing well, and employees with a need for improvement. By identifying these types of employees, the SEC is able to take the appropriate steps to develop these employee's careers. In addition, gaps in skills and competencies can be identified through reporting and appropriate training can be recommended to overcome the gaps.
- **Succession**: Through the Succession module, the system provides SEC federal employees the ability to look at the skills and competencies needed for different positions at SEC and design a career path.
- **Dashboards and Reporting**: The system includes a multitude of canned reports, custom reports, and dashboards. Access to the dashboards is restricted based on user's permissions. The system provides OHR the ability to run workforce reports capturing position and employee data.

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; 5 U.S.C. § 4302, Establishment of performance appraisal system; 5 CFR Part 410, Training; 5 CFR Part 412, Supervisory, Management and Executive Development; and 5 CFR Part 430, Performance Management.

2.3 Does the project use, collect, or maintain Social Security numbers (SSNs)? *This includes truncated SSNs.*

☒ No

2.4 Do you retrieve data in the system by using a personal identifier?

☒ Yes. ETMS is covered by SORN SEC-39 "Personnel Management Employment and Staffing Files"

2.5 Is the information covered by the Paperwork Reduction Act of 1995 (PRA)?

☒ No. The ETMS does not collect information covered by the PRA.

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 clear 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 systems of records notices, privacy impact assessments and other notices, and limiting the information collected to what is truly necessary for the intended purposes. Also, forms (e.g., performance work plan (PWP), Form SF-182) and systems (e.g., Enterprise Human Capital Repository (EHCR), Federal Personnel and Payroll System (FPPS) ask for or ingest only the necessary information required for each module.

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	
☐ 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:				

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 ID, Location ID, Position ID, Cost Center ID, Grade ID, Hire Dates, Approvals, Approver ID, Manager ID, Retirement Eligibility/Plan, Supervisory Status, Employee Appointment Type, training histories, individual development plans, training requirements and performance assessment narratives.			

Distinguishing Features/Biometrics

☐	Fingerprints	☒	Photographs	☐	Genetic Information
☐	Voice Recording	☐	Video Recordings	☐	Voice Signature
☐	Other:	Click here to enter text.			

System Administration/Audit Data

☒	User ID	☐	Date/Time of Access	☐	ID Files Accessed
☐	IP Address	☐	Queries Ran	☐	Contents of Files
☐	Other:	Click here to enter text.			

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 completion of assigned training, manage training requirements, develop employee performance plans and goals, evaluate employee performance and provide assistance in the growth and development of the SEC workforce.

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

☒ SEC Employees

Purpose: Maintaining training requirements, training histories, performance plans, performance reviews, and performance ratings.

☒ SEC Federal Contractors
Purpose: Maintaining training requirements and training histories.

☒ Interns
Purpose: Maintaining training requirements, training histories, performance plans, performance reviews, and performance ratings.

☐ Members of the Public
Purpose:

☐ Employee Family Members
Purpose:

☒ Former Employees
Purpose: Maintaining training requirements, training histories, performance plans, performance reviews, and performance ratings.

☐ 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.

A limited amount of live SEC data associated with EHCR was authorized for purposes of developing ETMS. The Authority to test (ATT) was signed on 2/14/17. The limited live data was used in the Production, Stage and Pilot environments during implementation. The user data is still in all three environments and still in use for testing and troubleshooting issues. Access is limited to authorized users. Stage and Production environments each contain their own domain and are segmented into two VLANs. The Web Farm and App servers are located on one VLAN, while the SQL Cluster, file storage, and domain controllers are located on a second VLAN. Communication between the two VLANs is limited. Firewalls and load balancers are used to segment the network.

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

☒ No.
The SEC Records Office is currently drafting a Record Retention Schedule for data

collected in ETMS. (GRS 3.1, Item 011 and 020)

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

These 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

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. Access permissions to System Administrators 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
Form SF 182 contains a Privacy Act Statement

☒ System of Records Notice
SEC-39,

☒ Privacy Impact Assessment
Date of Last Update: Current PIA

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 inadequate notice. Individuals may not be are aware of the use of their information in the ETMS system since the majority of the information is collected from other source systems. This risk is mitigated by ensuring that applicable SORNs are current and adequately describe the uses and disclosures of information contained in the ETMS. Also, by ensuring that PIA reports for ETMS 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 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?

☒ Yes

Organizations:	All internal organizations will have some level of access to the system as all employees and contractors will have access to the system for limited purposes. Users are authenticated via single sign on (SSO), and therefore, must have an active directory (AD) account to access the system.

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 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.

5.4 Will external organizations have access to the data?

☒ Yes

Organizations:	System performance data is available for upload to the Department of Interior's (DOI), FPPS via an outbound data feed.

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

PII is not shared with external organizations via ETMS.

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): Data feeds from OHR records, SEC-University (SECU) records and historical data from the SEC's former learning management system LEAP.

6.2 What methods will be used to collect the data?

A secure file transport protocol (SFTP) connection between an OHR accessible shared folder and ETMS is used for inbound and outbound data. Historical training courses and

transcript data was populated to ETMS through a one-time data load during the initial launch of the system. User data collected after the launch of the system is transmitted daily from a file from EHCR, which is placed in a secured directory. The file is then transferred through a SFTP connection to ETMS. New courses are periodically uploaded by SECU. Users of the system input data as part of the system's use (e.g., performance reviews, development plans, course surveys, etc.). Performance data collected in ETMS is available for upload to FPPS via a secure connection and learning data is available for upload to EHCR via a secure connection. The EHCR centralized database is used as a reference database for ETMS. However, the original source of the data uploaded remains the authoritative source of the data as identified in the EHCR PIA. The original sources include FPPS, WebTA, and Contractor Personnel (CP) list (for contractors). The source data is pulled in to EHCR, which is then used to compile the census and send the data to Cornerstone. Until EHCR is automated, a full user census is loaded to ETMS every two weeks. In the Performance Management module, employees, supervisors, and rating officials provide input in performance plans and appraisal forms.

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

Employees have access to their own records and can input and modify some limited data (performance reviews, development plans, and course surveys) as part of the system's use but subject to access permissions. If an employee notices an error in their data, they can notify one of the OHR system administrators. The system administrator will work to get the data corrected at the original source, which will then update the system with the next data feed. Until EHCR is automated, a full user census is loaded to ETMS every two weeks. As a stop-gap measure, until the automated daily feed is completed we will occasionally update the supervisor field on the user record once we've confirmed that the change was made in the source data. For users who onboard or off board in between data feeds, we may activate or deactivate an existing Leap account. Accounts are only activated once the system administrator has confirmed that the user has a LAN account. If the user is a contractor, we also check the contractor personnel list and/or contact the COR to confirm they should be active. Any changes made by a system administrator to a user record will be overwritten with the next data feed. Any changes made to a user record are documented in a spreadsheet tracker with the date of the request, date of the change, askHR ticket number (or requestor name), user's LEAP username, and the change made.

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

☒ Yes.
System(s): EHCR, FPPS, and Active Directory

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. As individuals discover errors in their data and work with the administrators to have their information corrected at the source, the system will send updated information in the next data feed.

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.

The ETMS receives pre-determined PII from certain SEC systems and shared Federal systems. There is no ability to consent to particular uses of information in ETMS or for individuals to decline to have their information included in the system.

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

All users are authorized to view their personal and individual training and performance management information, as applicable, at any time.

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

Users of the system can input and modify some limited data (e.g., performance reviews, development plans, training requests, and course surveys) as part of the system's use but subject to access permissions. Administrators can also correct limited inaccurate information at the source; The system will send updated information in the next data feed.

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

The primary privacy risk is lack of access to personal information, which increases the risk of poor-quality, outdated data. This risk is mitigated by OHR ensuring that individual have a process available to correct inaccurate information.

Section 8: Security

8.1 Has the system been authorized to process information?

☒ Yes

SA&A Completion Date: 5/17/2017

Date of Authority to Operate (ATO) Expected or Granted: 5/19/2017

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

☒ Users

Roles: Access to their own information in system data

☒ Contractors
Roles: Access to their own information in system data

☒ Managers
Roles: Access to subordinate's information on a need-to-know

☒ Program Staff
Roles: Role-based access as Basic Instructor, Trainers, Training Coordinator, Report Only users, and View and Search Only users.

☐ Developers
Roles:

☒ System Administrators
Roles: Access to system data and configurations. Manage access/permissions, make configuration changes, and perform other administrative actions in support of the system.

☐ Others:
Roles:

8.3 Can the system be accessed outside of a connected SEC network?

☒ No Access is only provided from within the SEC. There is no access to ETMS from outside the SEC Network. CSOD staff cannot access the ETMS application from outside the SEC Network. They do, however, have access to the servers and database.

8.4 How will the system be secured?

Cornerstone is a web-based, multilayered architecture application built on Microsoft server technologies. With an emphasis on Microsoft .NET and object development methodologies, maintenance and expansion of features are performed rapidly. The back-end business logic is built on an object oriented system, implementing a fully normalized relational database management system (DBMS) design consisting of Transact-SQL stored procedures on Microsoft SQL Server. Users connect to the application via https over a web browser. User access is restricted by the SEC providing Cornerstone with the SEC "white" list, which is a list of acceptable IP addresses for accessing the portal. The portals are Akamai accelerated so there is no finite IP assigned to the portal.

The SEC utilizes Cornerstone's SSO functionality. The SSO is SP (Service Provider) initiated and uses Security Assertion Markup Language (SAML) and Active Directory Federation Services (ADFS).
Cornerstone is fully contained within a FedRAMP compliant infrastructure hosted outside of the SEC network boundary. Cornerstone leverages a defense-in-depth strategy that is isolated from the public Internet and from the corporate Intranet. The presentation layer is also isolated from the data by a firewall. A DMZ (utilizing multiple firewalls and encrypted VPN access to sensitive data and system administration) protects the system's production suite. Network infrastructure security includes managed firewalls, port filtering, and network address translation via load balancers. Stage and Production environments each contain their own domain and are segmented into two VLANs. The Web Farm and App servers are located on one VLAN, while the SQL Cluster, file storage, and domain controllers are located on a second VLAN. Communication between the two VLANs is limited. Firewalls and load balancers are used to segment the network.
The Cornerstone application is entirely rights and roles-driven. The application features security permissions, related to its features, which can be configured to roles or individual users. For example, general rules may be established for certain types of administrators, but each user may also be granted their own unique permissions. These permissions are all stored as part of the user's information.
Redundant firewalls are installed between all client data and external connections. All firewalls and routers log critical events such as authentication attempts and configuration changes to a centralized syslog server for alerting and forensic analysis.

The SEC has its own independent databases (hosted by Cornerstone) for its Production, Pilot, and Stage portals. Cornerstone preforms back up on the databases daily and the backups are written onto tapes for recovery.

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

☒ No

8.6 Does the site have a posted privacy notice?

☒ N/A

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

☒ No

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.

There is a risk that other clients of Cornerstone will be able to gain access to SEC data over the Cornerstone database. This privacy risk is mitigated by the fact that at Cornerstone, 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 Cornerstone support personnel.

Section 9: Accountability and Auditing

9.1 Describe what privacy training is provided to users, either general or specific to the system or project.

The SEC provides the required privacy and security awareness training to all employees and contractors, 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?

☒ 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?

☒ Yes

ETMS maintains an audit log of all changes to the data on a record-by- record basis. 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.

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?

ETMS utilizes technical controls to ensure that information is used in accordance with the stated practices in this PIA. The records are protected from unauthorized access through password and/or PIV card authentication using AD, role-based access, firewalls, and other system-based protections. All SEC employees and contractors have basic user role-based access to the system. Privileged user access is granted by system administrators. In addition, Administrator roles are restricted so that System Administrators will only have access to the offices or divisions for which they are responsible.

In addition, ETMS has a robust network/security alert system in place to notify members of the operation team, including deployment of a log aggregation, performance monitoring, and reporting tool, Splunk, which allows administrators to quickly filter for information, receive alerts based on user-defined criteria, and receive trending, analysis, and correlation information.

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.

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.