U.S. Securities and Exchange Commission

askHR System
PRIVACY IMPACT ASSESSMENT (PIA)

May 4, 2017

Office of Human Resources

Privacy Impact Assessment
AskHR

Section 1: System Overview

1.1 Name of Project or System

askHR System

1.2 Is the system internally or externally hosted?

☐ Internally Hosted (SEC)

☒ Externally Hosted (Contractor or other agency/organization) askHR is a cloud-based application hosted on the ServiceNow platform.

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?

☐ 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

The Office of Human Resources (OHR) currently manages 60 or more different shared mailboxes in Outlook to respond to SEC employees' inquiries. The askHR system will simplify and streamline OHR's process to handle the inquiries. The askHR system leverages the existing ServiceNow platform to extend Help Desk and ticketing functionality to OHR by providing one location for OHR staff to receive and respond to inquiries. The inquiries can range from general to specific requests, to include requests about benefits or medical telework. The solution will focus on self-service by (1) configuring an initiative HR knowledgebase and (2) designing a generic ticket resolution workflow, with canned email notifications, Service Level Commitments (SLC), and generic surveys to evaluate OHR customer satisfaction. Employees will be able to submit inquiries within askHR and a HR Case associated with the responsible OHR business service will be created. OHR staff will manage the cases in askHR. However, OHR may also communicate with employees via email to gather additional information from them to resolve their case.

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

15 U.S.C. 77a et seq., 78a et seq., 80a-1 et seq., and 80b-1 et seq.

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

☐ Yes

☒ No

There are no PII data elements in askHR. The inquiry form contains only two free text fields allowing for customers to respond. OHR will not request or directly collect SSNs from employees. However, some employees may inadvertently include their SSNs when submitting their inquiries. OHR will make every effort to communicate to employees to not provide their SSNs in their submissions. As a safeguard, data collected in askHR will be encrypted at rest and in transit, in accordance with National Institute of Standards and Technology (NIST) standards.

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

☐ No
☐ Yes, a System of Records Notice (SORN) is in progress
☒ Yes, there is an existing SORN

This system operates under both the SEC's system of records notice, SEC-56, Mailing, Contact and Other Lists, (July 22, 2009, 74 FR 36281) and the government-wide SORN OPM/GOVT-1 General Personnel Records (June 19, 2006, 71 FR 35342)

SEC-56 covers the collection of general contact information provided in the askHR system for the purpose of responding to inquiries. OPM/GOVT-1 may cover the collection of information that is being provided in support of an individual's inquiry. For example, the collection of information provided on an official Office of Personnel Management (OPM) Form submitted as part of an askHR inquiry may be covered by OPM's *OPM/GOVT-1* SORN. Official forms will be stored in the official system of records, not askHR, once it has been processed.

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 purpose of the collection is to allow OHR staff to effectively manage inquiries from SEC employees. The privacy risk identified is the over-collection of information and unauthorized disclosure of sensitive personally identifiable information (PII). The privacy risks are mitigated by deployment of encryption of data-in-motion and data- at-rest in accordance with NIST standards. Additionally HR Cases will only be accessible to those individuals with specific roles or in specific groups that need access to resolve the matters, or to provide support for development and Operation and Maintenance (O&M) functions of the system.

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
☒ Taxpayer ID
☒ Employee ID
☒ File/Case ID
☐ Other:

☐ Alien Registration
☐ Driver's License Number
☐ Passport Information
☐ Credit Card Number

☐ Financial Accounts
☐ Financial Transactions
☐ Vehicle Identifiers

General Personal Data

☒ Name
☒ Maiden Name

☒ Date of Birth
☒ Place of Birth

☒ Marriage Records
☒ Financial Information

☒ Alias
☒ Gender
☒ Age
☒ Race/Ethnicity
☐ Civil or Criminal History
☐ Other:
☒ Home Address
☒ Telephone Number
☒ Email Address
☒ Education Records
☒ Zip Code
☒ Medical Information
☒ Military Service
☒ Mother's Maiden Name
☒ Health Plan Numbers

Work-Related Data

☒ Occupation
☒ Job Title
☒ Work Address
☒ PIV Card Information
☐ Other:
☒ Telephone Number
☒ Email Address
☒ Certificate/License Number
☒ Fax Number
☐ Salary
☒ Work History
☐ Business Associates

Distinguishing Features/Biometrics

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

System Administration/Audit Data

☒ User ID
☒ IP Address
☐ Other:
☒ Date/Time of Access
☒ Queries Ran
☒ ID Files Accessed
☒ Contents of Files

3.2 Why is the PII listed in Question 3.1 collected, used, shared, or maintained by the system or project?

There are no PII elements in askHR. The inquiry form contains only two free text fields allowing customers to respond. Because of the nature of the inquiries to be submitted, i.e., related to human resources matters, a wide variety of PII data elements may be provided by employees in their inquiries. The PII data elements selected above in 3.1 may be provided in the free text fields as part of an employee's inquiry. There may be scenarios where OHR will require additional information from the user in order to accommodate and/or process the user's inquiry. Information and documents that employees may submit will generally be stored in askHR. However, if the employee submits a formal HR form with an inquiry, that form will be stored in the appropriate HR system, not askHR, once the form is processed. For example, if the employee provides a completed benefits election form with a submission, the benefits election form will stored in "Electronic Official Personnel Folder" (eOPF) System as the official system of record, once it has been processed.

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

☒ SEC Employees
Purpose: User will be submitting inquiries to OHR for processing.

☒ SEC Federal Contractors
Purpose: Limited contractor information may be collected in askHR related to the contractor submitting inquiries on behalf of an SEC employee. However, contractors will not be submitting inquiries on their own behalf.

☒ Interns
Purpose: Users may be submitting inquiries to OHR for processing.

☐ Members of the Public
Purpose:

☒ Employee Family Members
Purpose: SEC employees may need to provide the information of their family members for inquiries such as benefit changes.

☒ Former Employees
Purpose: User may be submitting inquiries to OHR for processing.

☒ Job Applicants
Purpose: Future state of the askHR System may allow for user to submit inquiries to OHR for processing.

☐ 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.

Testing and training for askHR will be performed on non-production systems that do not contain PII. Also, there are no PII elements in askHR. The inquiry form contains only two free text fields allowing customers to respond. In the background and after submission, additional information is captured on the HR Case – HR Case number (unique), State, Top-Level Program, Item, Opened By, Opened [date], Created by, Requested For.

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

☐ No.

☒ Yes.

The applicable records retention schedule is the Employee Management Records, GRS 2.2, Item 010, (pending). Until GRS 2.2 becomes effective, the records will be kept in accordance with the current applicable record retention schedule.

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

AskHR will store all service tickets for HR Cases. The system has reporting capabilities to generate records based on fielded data such as date fields. The system administrators will have the capability to delete HR Cases that meet the retention criteria. The system will be able to generate a scheduled report that will email the administrators a report containing all of the HR Cases meeting the destruction policy criteria in the calendar year.

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?

Considering the type of data that may be collected or maintained in the system, the privacy risks identified are the over-collection of information and the unauthorized disclosure of sensitive PII. The privacy risks are mitigated by deployment of encryption of data-in-motion and data- at-rest in accordance with NIST standards. Additionally HR Cases will only be accessible to those individuals with specific roles or in specific groups that need access to resolve the matters or to provide support for development and O&M functions of the system.

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-56, Mailing Contact and Other Lists
OPM/GOVT-1, General Personnel Records

☒ Privacy Impact Assessment

☐ Web Privacy Policy

☒ Other notice: An *SEC Today* notice is planned to announce the askHR System as OHR's new centralized system for OHR inquiries, and to highlight key features.

☐ 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?

Information within the askHR system is provided by the individual, such as an employee, to whom it applies or is derived from information the individual supplies, as appropriate. Insufficient notice of the routine uses of the data collected is an identified privacy risk. This risk is mitigated by the published SORNs, SEC-56 and OPM/GOVT-1, and ultimately, this privacy impact assessment (PIA). Both documents will be published on the SEC's website to provide notice of how the SEC uses the information collected by the system.

For official forms, notice may be provided at the original point of collection on the forms. Notice is not provided to individuals via the askHR system. askHR is currently an internal system synched with SEC's Active Directory, which allows employees to interface with askHR after first logging onto the SEC network.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

The data collected will not be analyzed to determine patterns.

5.2 Will internal organizations have access to the data?

☒ No
☐ Yes
Organizations:

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

There are no associated risks identified with internal sharing.

5.4 Will external organizations have access to the data?

☐ No

☒ Yes

Organizations: The askHR System does not provide direct access to external organizations for information sharing nor is it integrated in any way with other systems. The SEC may share information from the system externally with other Federal and State authorities when necessary or required, such as the Office of Personnel Management (OPM), Equal Employment Opportunity Commission (EEOC), Federal Labor Relations Authority (FLRA), Merit Systems Protection Board (MSPB), arbitrators, courts and other tribunals, and Congress. Unless required to be provided, all identifying information is redacted from data before it is shared. The SEC has outlined the ways in which information from the askHR may be shared externally under the "Routine Uses" section of its SORN, SEC-56– Mailing, Contact and Other Lists. In addition, uses of the data may be made as outlined in OPM/GOVT-1, General Personnel Records.

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

There is the risk of unauthorized disclosure to a third party. This risk is mitigated by providing the data through secure channels, such as encrypted email, with appropriate data sharing agreements in place to ensure parties understand the safeguards for handling the information.

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): The system collects the data directly from the employees to whom it applies or the information may be derived from information that the employee supplies.

6.2 What methods will be used to collect the data?

Individuals may provide information at the time of an inquiry when they reach out to OHR for support. OHR may request additional information from individual in order to complete/respond to the individual's inquiry. Information is provided directly in the askHR system. In addition, supporting information may be scanned, uploaded or attached to an HR Case, as appropriate.

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

HR Staff that receives the information will verify accuracy against existing HR systems and consult back to the customer. If information provided is deemed to be inaccurate, then HR staff will request an update to obtain the correct information.

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

☒ No

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 privacy risk identified is inaccurate or outdated information. This risk is mitigated because the information in the inquiry is collected directly from the employees to whom it applies or is derived from information that the employee supplies. Additionally, there is a risk of over-collection of information, which may impact data integrity. However, employees are the initial source of the information collected. Therefore, they have the ability to limit the information that they provide in their inquiries as well as correct any information that is erroneous, inaccurate or irrelevant.

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 agree to the voluntary submission of information in support of their inquiry, e.g., reasonable accommodation requests or medical telework. Individual use of the system and information that is provided is strictly voluntary.

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

Users will be able to see and review their respective past or previously submitted HR Cases.

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

Users can update information specific to their HR Cases as long as it has not been resolved by OHR or closed by the system.

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

Because the interactions that result in information collection are generally voluntary, the privacy risks associated with this collection are minimal. askHR does not provide for direct identifying PII; there are two free text fields. Employees choose what and how much information they share with the OHR, and they have opportunities to change or update information that is erroneous, inaccurate, or irrelevant.

Section 8: Security

8.1 Has the system been authorized to process information?

☐ Yes
SA&A Completion
Date:
Date of Authority to Operate (ATO) Expected or Granted:

☒ No
SA&A pending

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

☒ Users
Roles: askHR General Users, askHR Power User, askHR Admin User

☒ Contractors
Roles: askHR General Users, askHR Power User, askHR Admin User

☒ Managers
Roles: askHR General Users, askHR Power User, askHR Admin User

☒ Program Staff
Roles: askHR General Users, askHR Power User, askHR Admin User

☒ Developers
Roles: ServiceNow Solutions Center Developers

☒ System Administrators
Roles: ServiceNow Solutions Center System Administrators

☐ Others:
Roles:

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

☒ No

8.4 How will the system be secured?

Records are maintained in a secured environment with access limited to authorized personnel whose duties require access. User accounts for employees are synched with SEC's Active Directory that allows them to interface with askHR, once logged onto the SEC network. OHR staff responsible for responding to inquiries will require role-based access based on the defined roles described in 8.2 above.

8.5 Does the project or system involve an 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.

There are inherent risks and threats associated with cloud computing as users typically lose a degree of control over their data. The identified privacy risks typically relate to data that is transferred to, stored and processed in the cloud, including unauthorized access or disclosure by a third party. Because of this possibility, appropriate security and access controls listed in this PIA are in place. The responsibility for protecting the information is shared between the SEC and ServiceNow.

Access Controls. Access controls limit access to the application and/or specific functional areas of the application. These controls consist of privileges, general access, password control and discretionary access control. User accounts for employees are synched with SEC's Active Directory that allows them to interface with askHR. Additionally, each user is associated with one or more database roles as noted above in 8.2.

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 complete the Privacy and Information Security Awareness training prior to being granted access to SEC information and information systems. Also, employees are trained on SEC Rules of the Road governing their activities related to safeguarding SEC information. Privacy and Information Security Awareness is provided on a continuous basis to keep users alert to the privacy and security requirements and safeguards, including visual effects of constant reminders to ensure users always remain aware of their responsibilities.

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

Yes. HR Case records are audited with the action that was performed (i.e., field updates), when the change occurred, and who made the change.

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?

The askHR System uses audit capabilities to record system events. The askHR System generates audit records for the following events:

- Account Logon and Logoff
- Field changes
- System Events
- File creation and deletion
- Account privilege changes

Access to the audit history requires the appropriate role. askHR Admin and ServiceNow Solution Center (SNSC) team members will have access to the individual HR Case history.

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 identified risks include unauthorized access and disclosure. However, this is mitigated through access controls noted above in 8.2 and further mitigated by auditing features, which allow review and examination of records, activities, and system parameters, to assess the adequacy of maintaining, managing and controlling events that may degrade the security posture of the application. Auditing ensures data integrity, and that data has not been altered or destroyed in an unauthorized manner. In addition, data in the askHR is secure in transit and at rest, which mitigates these risks.