

**U.S. Securities and Exchange Commission**

---

**askHR System  
PRIVACY IMPACT ASSESSMENT (PIA)**



**October 12, 2021**

**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.

#### 1.3 Reason for completing PIA

- New project or system  
 This is an existing system undergoing an update  
First developed: 5/4/2017  
Last updated: 8/24/2021  
Description of update: This PIA updates the purpose of the system to include the collection of public health and safety information.

#### 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](http://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) utilizes the askHR workflow to simplify and streamline OHR's process to handle HR-related inquiries and information. The askHR workflow extends IT Service Management (ITSM) Service Desk and ticketing functionality to OHR by providing one location for OHR staff to receive and respond to HR-related inquiries and information from SEC employees. The platform is used for automating, measuring, and reporting business processes and utilizes user name and phone, address, and email from SEC's Active Directory (AD) for purposes of authentication and authorization.

The askHR inquiries and information may range from general inquiries to specific requests, to include requests and information about benefits and medical telework. The application may also be used to collect information subject to a declaration of a public health emergency. The ITSM solution focuses on self-service by (1) configuring an intuitive 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 submit inquiries within askHR and a HR Case associated with the responsible OHR business service is created. OHR staff manage the cases in askHR. However, OHR may also communicate with employees via email to gather additional information from them to resolve their case.

The platform is a cloud-based Platform-as-a-Service (PaaS) solution that is used by many Federal Agencies.

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

# Privacy Impact Assessment

AskHR

5 U.S.C. 302; Executive Order 13991; Executive Order 12196

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

Yes

No

Although the system does not request or deliberately collect SSN's through the intake form itself, employees submit forms through askHR that often contain SSNs and therefore SSN/PII data is in the system.

**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

**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 related to the purpose of the collection is using information provided for one purpose inappropriately. This risk is 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 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

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

Vaccination Information

Other:

Testing Results

# Privacy Impact Assessment

## AskHR

### Work-Related Data

- |   |  |  |
|---|--|--|
| <input checked="" type="checkbox"/> Occupation  | <input checked="" type="checkbox"/> Telephone Number           | <input checked="" type="checkbox"/> Salary       |
| <input checked="" type="checkbox"/> Job Title   | <input checked="" type="checkbox"/> Email Address              | <input checked="" type="checkbox"/> Work History |
| <input checked="" type="checkbox"/> Work Address  | <input checked="" type="checkbox"/> Certificate/License Number | <input type="checkbox"/> Business Associates     |
| <input checked="" type="checkbox"/> PIV Card Information  | <input checked="" type="checkbox"/> Fax Number                 |  |
| <input checked="" type="checkbox"/> Other: Employee Type (i.e., Federal Employee or Contractor)<br>Department |  |  |

### Distinguishing Features/Biometrics

- |  |   |  |
|--|---|--|
| <input type="checkbox"/> Fingerprints    | <input type="checkbox"/> Photographs      | <input type="checkbox"/> Genetic Information |
| <input type="checkbox"/> Voice Recording | <input type="checkbox"/> Video Recordings | <input type="checkbox"/> Voice Signature     |
| <input type="checkbox"/> Other:          |   |  |

### System Administration/Audit Data

- |  |   |   |
|--|---|---|
| <input checked="" type="checkbox"/> User ID    | <input checked="" type="checkbox"/> Date/Time of Access | <input checked="" type="checkbox"/> ID Files Accessed |
| <input checked="" type="checkbox"/> IP Address | <input checked="" type="checkbox"/> Queries Ran         | <input checked="" type="checkbox"/> Contents of Files |
| <input type="checkbox"/> Other<br>:            |   |   |

### 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 or could be mandatory fields on an HR form that can be attached to an 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 are stored in askHR. Any forms submitted through askHR are officially stored in the appropriate system of record once the form is processed. However, the initial version of the form itself is also retained in askHR as part of the employee's inquiry. For example, if the employee provides a completed benefits election form with a submission, the benefits election form is stored in "Electronic Official Personnel Folder" (eOPF) System as the official system of record, once it has been processed but a version of the form is also retained in askHR.

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

- SEC Employees  
Purpose: User submit inquiries and forms to OHR for processing.
- SEC Federal Contractors  
Purpose: Limited contractor information is collected in askHR related to the contractor submitting inquiries on behalf of an SEC employee. However, contractors do not submit inquiries on their own behalf.
- Interns  
Purpose: Users submit 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.

# Privacy Impact Assessment

## AskHR

- Job Applicants  
Purpose: Future state of the askHR System may allow 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.

PII is not used for testing or training.

### 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.

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

AskHR stores 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 have the capability to delete HR Cases that meet the retention criteria. The system is able to generate a scheduled report that emails 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?

The primary privacy risk relating to the type of information collected is risk of inadvertent or unauthorized access/disclosure of nonpublic information. To mitigate these risks, the system uses role-based access and leverages AD for authentication to mitigate the potential for unauthorized access of data. In addition, encryption of data-in-motion and data-at-rest mitigate potential for unauthorized disclosure.

## 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

# Privacy Impact Assessment

## AskHR

SEC-26, Mailing, Contact and Other Lists, (85 FR 85440, January 27, 2021)  
OPM/GOVT-1, General Personnel Records (80 FR 74815, November 30, 2015)  
OPM/GOVT-10, Employee Medical File System Records (80 FR 74815, November 30, 2015)

- Privacy Impact Assessment  
Date of Last Update: 8/24/2021
- Web Privacy Policy
- 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?

The primary privacy risk is individuals may not have notice on the use of their information via the system. This potential risk is mitigated by ensuring that applicable SORNs are current and adequately cover the categories of records and individuals and this PIA is updated and published.

## Section 5: Limits on Uses and Sharing of Information

### 5.1 What methods are used to analyze the data?

The data collected is not analyzed to determine patterns.

### 5.2 Will internal organizations have access to the data?

- No
- Yes  
Organizations: OIT

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

The risk is that information may be shared with SEC personnel who do not have a need to know the information during the course of official duties. This risk is mitigated by restricting access to data via system access request (SAR). Users granted privileged roles must undergo approvals from their manager or contracting officer.

### 5.4 Will external organizations have access to the data?

- No
- Yes  
Organizations: Information from the askHR may be shared externally pursuant to routine uses outlined in the applicable SORNs listed in Section 4.1.

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

The primary privacy risk related to external sharing is 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): OHR staff may also import data into the system in support of the individual's inquiry.

# Privacy Impact Assessment

## AskHR

### 6.2 What methods will be used to collect the data?

Individuals provide information at the time of an inquiry when they reach out to OHR for support. OHR may request additional information from individuals 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 verifies the accuracy against existing HR systems and consults back to the customer. If information provided is deemed inaccurate, then HR staff requests 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 risks related to data quality and integrity is inaccurate or outdated information. This risk is mitigated by obtaining the information in the inquiry directly from the individual to whom it applies or by verifying as appropriate information submitted on the individual's behalf. In addition, the platform requires individuals to "confirm" fulfillment of their inquiry, which presents an opportunity to correct data submission before closing the inquiry.

## 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 ability to consent to uses of their information. Individuals may decline to provide information but doing so may impact obtaining information related to their inquiry or request.

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

Persons wishing to obtain information on the procedures for gaining access to the contents of records may contact the FOIA/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736.

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

Persons wishing to obtain information on the procedures for amending information about themselves may contact the FOIA/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736.

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

There is minimal risk related to individual participation. askHR records are covered by existing SORNs, which afford Privacy Act redress options. In addition, 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 Does the project or system involve an online collection of personal data?

# Privacy Impact Assessment

AskHR

- 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 annual privacy awareness training, which outlines their roles and responsibilities for properly handling and protecting PII.

### 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

The application utilizes out-of-the-box audit recording and reporting functions. Only users with an administrator role have access to the audit logs. Furthermore, no one (even admins) has the ability to delete logs. OIT Security Teams work collectively in sharing and reviewing audit-related findings to enhance overall support and maintenance of the platform when areas of improvement are identified.

The platform contains functionality to record, store and report on various activities and events occurring in the platform and capturing that history in comprehensive audit logs. HR Case records are audited with the action that was performed (i.e., field updates), when the change occurred, and who made the change. In addition, data such as user and group management, event types (changes, enablement, etc.), table impacts, failed login attempts, system integration, property settings and modifications, etc. are all recorded within the platform. Currently, the logs are maintained and are not configured to be offloaded to a separate system.



# Privacy Impact Assessment

## AskHR

### **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 identified risks include unauthorized access and disclosure. However, these risks are 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 secured in transit and at rest.