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

# ServiceNow Enclave
# PRIVACY IMPACT ASSESSMENT (PIA)

**July 2, 2024**

**Office of Information Technology**

# Privacy Impact Assessment

ServiceNow Enclave

## Section 1: System Overview

### 1.1 Name of Project or System

ServiceNow Enclave

### 1.2 Is the system internally or externally hosted?

☐ Internally Hosted (SEC)

☒ Externally Hosted (Contractor or other agency/organization) — ServiceNow

### 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?

☐ 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

ServiceNow Enclave consists of several ServiceNow applications operating under one security authorization boundary. The Enclave provides project management, enterprise assessment management, change management, system development life cycle assurance, HR related inquiries, and help desk support for information technology (IT) to the SEC. The Enclave will grow as applications are added to the authorization boundary. Currently, the following ServiceNow applications are included in the Enclave:

- askHR (HRSD) – Searchable interactive knowledge base and customer service portal for agency human resources information and requests for related information.
- Change Management – Repository for IT Change Requests and tracking.
- Discovery – Auto populates the ServiceNow configuration management database (CMDB) with information for servers, network devices, security devices, workstations, and printers.
- askIT (ITSM) – Provides SEC staff with a convenient, central access point for making and tracking IT-related requests and incidents.
- PaLMS – PaLMS streamlines, integrates, and automates the SEC's Investment lifecycle, which includes Intake, Capital Planning and Investment Control (CPIC), Project Management and Service Delivery Framework (SDF). It consolidates and connects the entire Investment lifecycle, associated data, tracking tools and other activities on a single PPM portal, allowing the SEC to enhance governance, efficiency, collaboration, and information sharing.

- SecOps– Lays the foundations of Security Operations in ServiceNow. This application will support the automation of vulnerability tracking, remediation and reporting of data via application programming interface (API) integration with Tenable Security Center.

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

U.S.C. § 302 *Delegation of Authority* and 44 U.S.C. § 3101 *Records Management by Agency Heads*.
15 U.S.C. 77a *et seq*., 78a *et seq*., 80a-1 *et seq*., and 80b-1 *et seq*.
44 U.S.C. § 3534; Federal Information Security Act (Pub. L. 104-106, section 5113);
Electronic Government Act (Pub. L. 104-347, section 203);
Executive Order 9397 (SSN), as amended by EOs 13478, 9830, and 12107.
NARA Bulletin 2015-04: Metadata Guidance for the Transfer of Permanent Electronic Records
OMB/NARA Memorandum (M-19-21), *Transition to Electronic Records*, June 28, 2019

**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:

Truncated SSN is captured in the HR profile within the application of HRSD and utilized by SEC Office of Human Resources (OHR)

If yes, provide the legal authority:

The legal authority to collect the SSN is 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

Applications currently operating in the ServiceNow Enclave are covered by the following SORNs:

SEC-26 Mailing, Contact and Other Lists, (85 FR 85440, January 27, 2021)
SEC-33 General Information Technology Records, (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)

**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 privacy risk related to the purpose of the collection is that collected information may be used for an unintended purpose. This risk is mitigated by limiting information collected to that which is necessary to meet the purpose of the collection.

## 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: See Identifying Numbers in AskHR PIA located on the SEC Privacy site.

**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: See General Personal Data in AskHR PIA located on the SEC Privacy site.

**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: See Work Related Data in AskHR PIA located on the SEC Privacy site.

**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?**

Currently, HRSD is the only application in the Enclave that collects or maintains PII. PII may be collected in HRSD when necessary for OHR to process employee requests or resolve personnel issues.

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

☒ SEC Employees

Purpose: SEC employees may submit HR inquiries through HRSD to OHR.

☒ SEC Federal Contractors
Purpose: Limited contractor information may be collected in HRSD related to a contractor submitting inquiries for themselves or on behalf of an SEC employee.

☒ Interns
Purpose: Interns may submit HR inquiries through HRSD to OHR for processing.

☐ Members of the Public
Purpose:

☒ Employee Family Members
Purpose: SEC employees may provide family member information through HRSD for certain inquiries such as benefit changes.

☒ Former Employees
Purpose: Former employees may submit HR inquiries to OHR for processing through an inbound email action called HRSD alias.

☒ Job Applicants
Purpose: Job applicants may submit inquiries to OHR via HRSD alias.

☒ Vendors
Purpose: Vendors for an HR program may submit an inquiry to OHR regarding active or separated SEC employees.

☐ 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.**

HRSD collects the minimum PII that is necessary to process employee requests or resolve issues. Instructions, provided at the point of data entry, are used to minimize excessive PII input. PII collected is not used for testing, training, or research.

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

☒ Yes.
Multiple NARA schedules have been identified based on the available records within the platform.

| General Record Schedule | Item Description |
|---|---|
| GRS 2.7.063 Employee Health and Safety Records | Vaccination Attestations and Proof of Vaccination Records |
| GRS 03.1.020 General Technology Management Records | Information Technology Operations and Maintenance Records |
| GRS 03.1.040 Technology Management Records | Information Technology Oversight and Compliance Record |
| GRS 05.2.010 Transitory and Intermediary Records | Transitory Records |
| GRS 5.8.010 Administrative Help Desk Records | Technical and Administrative Help Desk Operational Recor |
| GRS 2.2.010 Employee Management Records | Employee Management Administrative Records |

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

Per each GRS, the identification and disposition procedures are as follows: System Administrators will destroy records based on the following business rules approved by OHR management and in accordance with the designated NARA GRS classification defined for different record types. Records are destroyed once retention period is reached. Process steps to identify and remove records are as follows:

- The OHR Program Manager will request for a report to show eligible records for deletion aligning with the OHR file plan.
- With concurrence of the appropriate OHR staff, the Records Liaison shall obtain approval from SEC Office of Records Management Services (ORMS) for deletion, pursuant to the Records Destruction Directive OP7-1C, or existing SEC Directive at the time of deletion action.
- Upon obtaining deletion approval from ORMS, the Records Liaison shall notify the System Administrator that the records past retention are ready for deletion, who will carry out deletion of data.
- Upon notification from the Records Liaison, system administrator shall execute deletion of records.
- Records identified for permanent deletion will not be recoverable.

| General Record Schedule | Disposition Instruction |
|---|---|
| GRS 2.7.063 Employee Health and Safety Records | Temporary – Destroy when 3 years old |
| GRS 03.1.020 General Technology Management Records | Temporary – Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded (longer retention is authorized if required for business use) |
| GRS 03.1.040 Technology Management Records | Temporary - Destroy 5 years after the project/activity/ transaction is completed or superseded, but longer retention is authorized if required for business use |
| GRS 05.2.010 Transitory and Intermediary Records | Temporary – destroy when no longer needed for business use, or according to agency predetermined time period or business rule |
| GRS 5.8.010 Administrative Help Desk Records | Temporary – destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate |
| GRS 2.2.010 Employee Management Records | Temporary – Destroy when 3 years old, but longer retention is authorized if required for business use |

**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 risks, related to the type of information collected in the Enclave, is inadvertent disclosure and unauthorized access of nonpublic information. To mitigate these risks, applications employ access control to limit user access to only the information for which they have need-to-know. Active Directory (AD) user authentication ensures that only authorized users may access applications in the Enclave.

## 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
Posted on HRSD homepage

☒ System of Records Notice
- SEC-26 Mailing, Contact and Other Lists, (85 FR 85440, January 27, 2021)
- SEC-33 General Information Technology Records, 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)

The following 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.

☒ Privacy Impact Assessment(s)
The askHR PIA is not provided to individuals prior to collection, but is available on the SEC website www.sec.gov.

Date of Last Update:

☐ Web Privacy Policy

☒ Other notice:
ServiceNow Services Privacy Statement

☐ 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 risk of inadequate notice is minimal because the SORNs, PIAs, and the ServiceNow Privacy Statement identified in section 4.1 provide adequate notice.

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

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

The system does not analyze collected data for any purpose.

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

☐ No
☒ Yes
Organizations: All SEC Divisions and Offices

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

The risk related to internal sharing is that information may be shared with SEC personnel who do not have a need to know the information. This risk is mitigated by using access controls and an enterprise-wide use of a System Access Request process for requesting application access within the platform. Use of these tools, restrict user access to only the information based on need to know or necessary to perform assigned work tasks.

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

☐ No

☒ Yes

Organizations: External organization cannot directly access data in the ServiceNow Enclave. However, the SEC may share information externally with other Federal and State authorities when required by law or policy. Information may also be shared externally from askHR pursuant to routine uses outlined in the applicable SORNs.

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

The risk to privacy from external sharing is minimal. Information from the ServiceNow Enclave is only shared with an external organization if required. If information is shared, encrypted email or data encryption protocols are used to transmit the information securely via the internet, 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): Enterprise Human Capital Repository (EHCR)

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

Information is provided directly by the individuals via forms in ServiceNow. Most of these forms are within the HRSD and ITSM applications. Additional information may be requested from an individual to respond to or complete an individual's inquiry or request. Individuals may upload supporting information to an active HR Case in HRSD. The Service Desk may also utilize some of the information already present, ingested from EHCR, in a User's ServiceNow Profile.

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

HR staff review information via HRSD and verify accuracy against existing SEC OHR systems in consultation with the individual. If information provided is determined to be inaccurate, the HR staff will contact the individual to request the correct information.

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

☐ No

☒ Yes.

System(s): Microsoft Outlook/Exchange, EHCR

**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?**

Identified privacy risks are inaccurate or outdated information populated in the Enclave. The risk is minimized because the information is collected directly from employees or is derived from information previously provided by the employee is assumed to be accurate. Where information is received from EHCR, EHCR is considered the authoritative source for that data and is responsible for data quality and integrity. Additionally, applications such as HRSD and ITSM have processes in place to request individuals "confirm" fulfillment of their inquiry, presenting 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.**

Use of the applications in the ServiceNow Enclave is voluntary. If an individual declines to use the ServiceNow applications, assistance may not be provided to the individual.

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

Users can directly access information previously submitted in HRSD and ITSM. In addition, individuals may submit a written request to 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?**

Individuals may amend information about themselves by submitting the amended information to HR through a new HRSD service ticket or submit a request in writing to the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-2736 or email foiapa@sec.gov.

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

Privacy risk related to individual participation and redress is that information may be incorrect and may require updates due to changes over time. This risk is mitigated by allowing individuals to voluntarily amend information, submitted about themselves, through a new HRSD service ticket or submit a request in writing to the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-2736 or email foiapa@sec.gov.

## Section 8: Security

**8.1 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 |

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

☒ No

**8.3 Does the site have a posted privacy notice?**

☐ No
☒ Yes

## 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.**

The residual risks include unauthorized access and disclosure. However, these risks are mitigated through access controls noted above in 8.2 and further mitigated by implementing security and auditing controls as discussed in sections 8.2 and 9.5.