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

# HUB OWB Modernization
# PRIVACY IMPACT ASSESSMENT (PIA)

**March 20, 2022**

**Division of Enforcement**

# Privacy Impact Assessment

HUB OWB Modernization

## Section 1: System Overview

### 1.1 Name of Project or System

HUB OWB Modernization

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

☒ Internally Hosted (SEC)

☒ 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: 1/1/2007

Last updated: 3/4/2021

Description of update: Update HUB technology to cloud environment and migrate HUB Matters Under Investigation (MUIs), Investigations, Enforcement Actions, Validation, Documents, and Related Names functionality. In addition, a module was added to manage and support the ENF Office of the Whistleblower (OWB). Both HUB Legacy and HUB OWB Modernization systems are operating concurrently until HUB Legacy is retired.

### 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

HUB is the SEC Division of Enforcement (ENF) case tracking system for Matters Under Inquiry (MUI), Investigations and Actions (i.e., litigations). The HUB modernization effort migrates the existing HUB system to the Cloud, a FedRAMP Moderate authorized case management/Business Process Management (BPM) platform. HUB OWB provides ENF investigators and litigators the ability to better manage and produce attorney work product, track evidentiary documents, manage records, and effectively track and manage whistleblower matters.

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

Securities Exchange Act of 1933, Sections 15 U.S.C. 77s, 77t, and 77uuu; Securities Exchange Act of 1934, Section 78u; Investment Company Act of 1940, Section 80a-41; and Investment Advisors Act of 1940, Section

80b-9; 17 CFR 202.5

**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 Commission may use social security numbers to identify individuals uniquely for enforcement purposes.
If yes, provide the legal authority: Executive Order 9397

**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
SEC-17 Enforcement Files

**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 include personal information is collected without a clear purpose or without clear legal authority. This risk is mitigated by collecting information as authorized and in accordance with the collection purpose identified in SORN SEC-17.

## 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: 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: Click here to enter text. | | |

**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: Click here to enter text. | | |

**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?**

PII is collected and used to track Matters Under Investigation (MUIs), Investigations, Actions, related party information, and other enforcement-related data. ENF staff uses information collected for the management of cases and the reporting of case-related metrics.

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

☒ SEC Employees
Purpose: Track user information and system access

☒ SEC Federal Contractors
Purpose: Track user information and system access

☐ Interns
Purpose:

☒ Members of the Public
Purpose: The HUB system tracks MUIs, Investigations, Actions, related party information, and other enforcement-related data. The OWB module collects data to track tasks and application for award workflow. Enforcement staff uses the data collected for the management of the cases and reporting of Division case-related metrics. OWB staff uses the data collected for the management of award claims and reporting of Office case-related metrics.

☐ Employee Family Members
Purpose:

☐ Former Employees
Purpose:

☐ 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.**

The system collects required PII information through use of a data entry form. It is critical that HUB-OWB has representative data in the stage environment to ensure performance and functionality is tested in an environment equivalent to HUB production. ATT-00039 was issued to authorize the use of production data for testing in the HUB stage environment. The ATT was subsequently updated to authorize the use of Claims Tracker data from the SharePoint for testing and validation of HUB OWB Modernization.

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

☐ No.

☒ Yes.
DAA-0266-2019-0001 Division of Enforcement Case Management and Tracking System (HUB*)*

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

DAA-0266-2019-0001 identifies the cutoff date for records as the end of the calendar year when the case is closed or becomes inactive. Data is disposed/deleted 50 years after.

**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 risk is inadvertent or unauthorized disclosure of sensitive PII. This risk is mitigated by utilizing role-based access controls to protect the data. Access is limited to authorized SEC Commission staff and supporting contractors who require access to the information. Access is further limited to specific data fields and functions. For instance, only staff assigned to the case can view the full SSN and the last four digits of SSN are masked from non-assigned staff.

## 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
SEC Form 1661: "Privacy Act of 1974" noted on page 4 under Section G.13 Routine Uses of Information
SEC Form 1662: "Privacy Act of 1974" noted on page 4 under Section H.13 Routine Uses of Information
☒ System of Records Notice
SORN SEC-17, "Enforcement Files" is not provided to individuals prior to collection, but is published in the Federal Register and available on the SEC's website.
☒ Privacy Impact Assessment
The HUB PIA is not provided to individuals prior to collection, but is available on the SEC's website.
Date of Last Update: 9/19/2019

☐ 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 a risk that individuals included in investigative materials are not made aware of the collection of their information. This privacy risk is inherent given the nature of investigative material and often the individuals whose information is in the documents are not the suppliers of the information. This risk is mitigated by the publication of this PIA, SORN SEC-17 and that the law enforcement exemption is applicable insofar as investigatory materials are compiled for law enforcement purposes.

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

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

HUB OWB does not analyze data to derive new data or create new data about an individual through aggregation from the information collected.

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

☐ No
☒ Yes

Organizations: ENF, Division of Corporate Finance (CF), Division of Economic and Risk Analysis (DERA), Division of Investment Management (IM), Division of Trading and Markets (TM), Office of the Chief Operating Officer (OCOO), Division of Examinations (EXAMS), Office of Credit Ratings (OCR), Office of the Ethics Counsel (OEC), Office of Financial Management (OFM), Office of the General Counsel (OGC), Office of Human Resources (OHR), Office of the Inspector General (OIG), Office of International Affairs (OIA), Office of Investor Education and Advocacy (OIEA), Office of Public Affairs (OPA), and Office of the Secretary (OS).

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

Privacy risk associated with internal sharing is that sensitive PII in the HUB system and the OWB module could be inadvertently disclosed. This risk is mitigated by implementing role-based access controls where a role is assigned to authorized users, from the internal organizations identified in section 5.2, to limit access to information that is needed to perform official duties.

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

☒ No
☐ Yes

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

The primary privacy risk associated with external sharing is that information could be erroneously disclosed to unauthorized parties or for an unauthorized purpose. This risk is minimized by ensuring that information is not

shared externally, other than with Federal entities or regulators in accordance with the routine uses identified in SORN SEC-17 and SEC Forms 1661 and 1662.

## 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): Enforcement staff and users who have access to the HUB system have privileges to add content. The Enforcement Division may receive information from many sources during an investigation pursuant to Form 1661, *"Supplemental Information for Entities Subject to Inspection by the Commission and Directed to Supply Information Other Than Pursuant to Commission Subpoena"* or from other individuals pursuant to SEC Forms 1662.

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

Enforcement staff manually uploads documents and completes form information in HUB OWB. The data comes from various sources including internal documents and action memos and Federal Court records. Staff can search a Master Entity list to add entities one at a time to a matter.

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

Case Management Specialists manually check HUB OWB data against case-related supporting documentation such as court dockets, Litigation Releases, Administrative Orders and Final Judgments.

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

☐ No

☒ Yes.

System(s): Enterprise Human Capital Repository (EHCR) – Retrieves SEC Employee information

**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 privacy risk is that HUB-OWB may contain outdated or inaccurate information on individuals. The risk minimized because, where feasible, data collected is supported by documentation which is used to ensure data quality and integrity.

## 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.**

Where information is sought from individuals, disclosures are made in such forms as SEC Forms 1661 and 1662. Individuals from whom information is sought voluntarily have the right to decline to provide it.
If information is sought via subpoena, individuals may decline to provide information pursuant to a subpoena based upon a valid assertion of privilege, Fifth Amendment, or other legitimate basis. Such assertions may be litigated depending on the facts and circumstances of the assertion. Individuals do not have the right to consent to particular uses of the data.

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

Individuals seeking access to their information contained in the system may submit a request in writing to the FOIA/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736 or may submit online. Information tracked in HUB OWB for investigation, litigation, or Whistleblower purposes is exempted from the Privacy Act's access to records rule, as noted in SORN SEC17.

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

Individuals seeking to amend information about themselves contained in the system or seeking to contest its content may submit a request in writing to the FOIA/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736 or may submit online. Information tracked in HUB OWB for investigation, litigation, or Whistleblower purposes is exempted from the Privacy Act's access to records rule, as noted in SORN SEC17.

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

The primary risks are lack of access to information and inability to seek redress and correction. This risk is mitigated by providing individual access or correction of the records as expressly permitted by the Privacy Act. HUB-OWB is exempted from certain Privacy Act provisions regarding participation and redress because the system contains investigatory materials compiled for law enforcement purposes.

## 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
☐ Yes

Public URL: Click here to enter text.

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

☐ No
☐ Yes
☒ N/A

## 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 users complete the Privacy and Information Security Awareness training prior to being granted access to SEC information and information systems. In addition, users 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.

**9.2 Does the system generate reports that contain information on individuals?**

☐ No

☒ Yes

Application reports may contain individual matter details. Additional reports (e.g. management reports) may be generated but do not contain PII. HUB-OWB does not generate reports that contain SSNs.

**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 expected residual risk related to access is inadvertent disclosure of data. To mitigate this risk, access to the system is limited by role based access control where SEC users are assigned a role to permit access to data based on need to perform official work duties.