U.S. Securities and Exchange Commission

HUB
PRIVACY IMPACT ASSESSMENT (PIA)

September 19, 2019

Division of Enforcement

Privacy Impact Assessment

HUB 10.2

Section 1: System Overview

1.1 Name of Project or System

HUB 10.2

1.2 Is the system internally or externally hosted?

☒ Internally Hosted (SEC) Division of Enforcement

☐ 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: 11/27/2012

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

☐ 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 HUB system is an internally hosted system and used by the SEC Division of Enforcement to manage cases within the Division of Enforcement. The following user groups in Enforcement, and those internal to the SEC, have access to the HUB: Enforcement staff working on, or supporting those working on, investigations and litigation generally have access to HUB, upon completion of a satisfactory request for access. This includes Enforcement attorneys, accountants, paralegals, legal techs, case management specialists and certain approved contractors. The system uses roles to assign privileges to users of the system based on the role of the user.

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-42 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 primary privacy risk for this data collection is unauthorized or inadvertent disclosure of sensitive PII or non-public investigatory material or case information. This risk is mitigated by implementing strict role-based access controls; requiring Commission staff and supporting contractors to submit access requests to the System Owner granted on a valid need-to-know/need-to-share basis and determined by assigned official duties; obtaining access subject to their role. Finally, all SEC staff and contractors receive annual privacy awareness training, which outlines their roles and responsibilities for properly handling and protecting PII. Also, audit logs are available for review to ensure appropriate usage.

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:		

General Personal Data

Any of the below data elements could "potentially" be in an attached document or in a narrative of a case but we do not intentionally collect any more of these fields in the Hub than what is selected below. For instance, there is no field that captures "Place of Birth." However, because of the nature and character of the information that may appear in a case file, any of the data elements listed below may be contained in documents in the case file.

☒ 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

Since there is no distinction between home and work in the system, Telephone Number, Email Address, Fax Number and Work Address are selected below.

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

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?

The HUB system collects data from direct entry by the Enforcement Staff. The HUB system tracks Matters Under Investigation (MUIs), Investigations, Actions, related party information, and other enforcement-related data. Enforcement staff uses the data collected for the management of the cases and reporting of Division case-related metrics.

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

☒ SEC Employees
Purpose: Track staffing information and usage of employees in the system.

☒ SEC Federal Contractors
Purpose: Track staffing information and usage of contractors in the system.

☐ Interns
Purpose:

☒ Members of the Public
Purpose: The information collected is for the purpose of supporting Enforcement Matters Under Inquiry, Investigations, and/or Actions. The HUB system collects data from direct entry by the Enforcement Staff. The HUB system tracks Matters Under Investigation (MUIs), Investigations, Actions, related party information, and other enforcement-related data. Enforcement staff uses the data collected for the management of the cases and reporting of Division 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.

PII is not being used for testing, training, or research efforts. Dummy data is used for testing, training, or research.

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

☒ No.
HUB retention schedule is pending with NARA but not yet approved.
☐ Yes.

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

The HUB retention schedule pending with NARA identifies the cut off at the end of the calendar year when case is closed or becomes inactive. The proposed schedule for HUB data is that data will be destroyed/deleted 50 years after cutoff or when no longer needed for business purposes. The proposed schedule is pending and has not been approved by NARA.

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 HUB system is storing PII on individuals who are in some way involved with an Enforcement matter or investigation. The primary risk is inadvertent or unauthorized disclosure of this sensitive PII. This risk is mitigated by utilizing role-based access controls to protect the data. Access is limited to the certain Commission staff and supporting contractors who require access to the information. Access is limited to specific data fields and functions. Staff assigned to the case can view the full SSN but the last four digits of SSN are masked from non-assigned staffed. The HUB does not generate reports that include SSN. Audit usage logs are available to ensure appropriate usage.

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-42 Enforcement Files

☒ Privacy Impact Assessment
Date of Last Update: 11/24/2014

☐ 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 times the individuals whose information may be found in the documents are sometimes not the suppliers of the information. However, the SEC has taken steps to provide transparency by publication of this PIA and SORN-SEC-42. Also, the law enforcement exemption is applicable insofar as investigatory materials are compiled for law enforcement purposes are collected.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

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

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes

Organizations: The following user groups in Enforcement, and those internal to the SEC, have access to the HUB: Enforcement staff working on, or supporting those working on, investigations and litigation generally have access to HUB, upon completion of a satisfactory request for access. This includes Enforcement attorneys, accountants, paralegals, legal techs, Case Management Specialists and certain approved contractors. The system uses roles to assign privileges to users of the system based on the role of the user.

Outside of the Division of Enforcement, a limited number of accounts are provided to staff from other agency Divisions through a robust approval process which is managed by Enforcement (CF, DERA, IM, TM, OCOO, OCIE, OCR, OEC, OFM, OGC, OHR, OIG, OIA, OIEA, OPA, OS) to provide Enforcement information for use in the pursuit of their objectives.

The Hub also has interconnections with other SEC systems that are governed by ASIs (Agreement to Share Information). These agreements detail what data is transferred from the Hub and at what frequency.

All sharing occurs through SEC LAN and involves internal systems only.

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

A privacy risk associated with internal sharing is that sensitive PII in HUB could be erroneously or inadvertently disclosed. This privacy risk is mitigated by implementing role-based access controls; limiting sharing of sensitive PII with downstream applications; and executing Agreements to Share Information (ASIs) with any party that has a system with which the Enforcement Division shares information. The ASIs are system specific, e.g., Palantir, EBIR, and are signed by both parties and renewed periodically detailing what fields are shared. They include the recipients need for Hub data, the number of users, data to be provided, system security requirements and other terms.

5.4 Will external organizations have access to the data?

☒ No
☐ Yes
Organizations:

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

HUB data is not shared with external entities.

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 and have privileges to add content. The Enforcement Division may receive information from many sources during an investigation. Enforcement may receive documents from other government administrative or law enforcement agencies. In an investigation, multiple requests for information could also result in information being provided by several branches of a corporate entity in addition to individuals. Depending on the circumstances, documents may be provided directly by an individual or by the individual's corporate employer.

6.2 What methods will be used to collect the data?

Enforcement staff manually uploads documents to HUB. The data comes from various sources including internal documents and action memos and Federal Court records. Staff are able to 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?

Data quality is governed by internal guidance for accuracy which involves referencing supporting documentation. The HUB system does not perform accuracy or completeness checks.

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

☐ No
☒ Yes

SECDATA database – 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 the Commission may rely on outdated or inaccurate information. Where feasible data collected in HUB is supported by documentation, thus minimizing risks to 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. Individuals from whom information is sought via subpoena 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 for the same reason stated above.

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

Although individuals may request access to information about themselves contained in a SEC system of records through the SEC Privacy Act/Freedom of Information Act (FOIA) procedures, Enforcement records are exempt from the access and correction provisions of the Privacy Act (see SORN SEC-42 "Enforcement Files"). This system is exempted from the Privacy Act insofar as it contains investigatory materials.

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

As mentioned above, individuals may request access to and correction of their information under the SEC Privacy Act/FOIA procedures, however, the data may be exempt from access and correction provisions under the PA and therefore access to such records will be restricted.

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

Given that individuals are not generally permitted to access or correct records about themselves available in the HUB system, there is a risk that inaccurate or erroneous information about an individual could be used by SEC personnel. This system is exempted from the Privacy Act insofar as it contains investigatory materials. This system is exempted from the Privacy Act insofar as it contains investigatory materials compiled for law enforcement purposes. This risk is mitigated by SEC personnel researching materials; conducting the proper due diligence before taking an adverse action against an individual; maintaining chain of custody records for the documents to demonstrate how they were received and processed; and verifying through testimony and litigation the accuracy of the documents and data.

Section 8: Security

8.1 Has the system been authorized to process information?

☒ Yes
Date of Authority to Operate (ATO) Expected or Granted: 9/29/2019
☐ No

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

☒ Division of ENF Staff
Roles: Have ability to update and save records to which they are assigned.

☒ Division of ENF Contractors
Roles: Have ability to update and save records to which they are assigned.

☒ Select Commission Staff Outside the Division of ENF
Roles: Have the ability to search records.

☒ Senior Officers in the Division of Enforcement
Roles: Same rights as Enforcement Staff and the ability to approve opening of matters and certain workflows.

☒ Local Case Management Specialist (CMS)
Roles: Ability to update and save records on all regional matters.

☒ National Case Management Specialist (CMS)
Roles: Ability to update and save records on all matters. Ability to validate records and view privacy information.

☒ Case Management Systems and Reporting Staff (CMSR) Staff:
Roles: Application Administrator rights.

8.3 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

8.4 How will the system be secured?

The breadth of the PII that may be contained in the case file is taken into consideration for implementing the appropriate controls as noted below:

To enter and remain in facilities where the system is housed, all persons must provide and wear their SEC badges. Security monitors all persons with physical personnel along with card readers and CCTV monitoring. Access to SEC machines further requires a PIV badge/credential for login. The HUB system and servers are only available to authorized users and are not accessible outside of the SEC network.

TLS 1.2, AES with 256 bit encryption and VPN are used by the application to ensure transmitted information is not modified or destroyed, and strong ciphers are used.

Infrastructure related protocols and services are monitored under GSS by using network monitoring tools like firewalls, IDS/IPS.

The System Owner identifies authorized users of the information system and specifies access rights/privileges.

The System Owner grants access to the information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. Additionally, HUB audit reports are reviewed routinely by the HUB development team and delivered to the COR, or more often in the event of elevated risk.

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.

Unauthorized access into the system through entry of an authorized user's account information is a risk to the system. However, this risk is mitigated through the GSS system protections employed at the SEC ensuring account verifications. Also, this system logs administrative events and would allow system administrators to see unusual activity. External risks are minimized as this system is housed and utilized entirely within the SEC.

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. In addition, the Hub User Guide is available either during onboarding or the Hub application.

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

☐ No
☒ Yes
Application reports are only available to those that have HUB access and may contain individual matter details. Reports can be downloaded from the application and the standard SEC rules governing protection of PII would apply.

Additional reports (e.g. management reports) can be generated and are summary in nature and do not generally contains PII and outside the application. However, these reports are treated with the same confidentiality as application reports.

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 HUB offers monitoring of security events through its auditing reporting feature and allows audit tables and reports that system administrators can use to monitor login, searches, views and saves. HUB also logs security-related events, including changes to reference data, recording who made the change and when. The HUB also logs who views audit reports and when; this will allow the HUB system owners to increase the granularity and frequency of audits in response to a perceived change in the threat environment.

The Audit record content for the HUB includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event.

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 electronic records are protected from unauthorized access through password identification procedures, limited access as per role based, firewalls and other system-based protections, among other appropriate methods. Changes to transaction data are logged in transaction logging tables in the database available to database administrator (DBA) personnel. Changes to reference data are logged in the system audit table available to system administrators.

The System Owner grants access to the information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The business Owner requires proper identification for requests to establish information system accounts and approves all such requests. The owner ensures unnecessary accounts are removed, disabled, or otherwise secured. Anonymous accounts and default accounts (including guest) are not allowed on internal systems per SEC policy.

System monitoring is done throughout the day by the Sybase Contractor Staff. Scripts are constantly monitoring error logs on the production servers. The Sybase staff is alerted when an error occurs and they handle it appropriately.

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.

Access to the system is limited to those that have a business need, and editing of specific details or viewing of matters is limited only to those users assigned to the matter and their managers. External access is not permissible.