Privacy Impact Assessment
The Hub (Upgrade)

General Information

1. Name of Project or System.
The Hub

2. Describe the project and its purpose or function in the SEC’s IT environment.
The Hub is a centralized web-based system used by Enforcement to manage and track cases. It was originally released in 2007. The purpose of the Hub is to provide a centralized system for users agency-wide to track and manage enforcement cases. It was developed at first to supplement CATS 2000, providing users with functions not available in CATS 2000. The current version of the Hub system gives users case data capture and management, auditing and reporting abilities.

3. Requested Operational Date?

4. System of Records Notice (SORN) number?
The System of Records Notice (SORN) number is SEC-42.

5. Is this an Exhibit 300 project or system? If yes, this PIA must be submitted to OMB.
The Hub is not an Exhibit 300 project or system.

6. Is this an agency’s system or a contractor’s system?
This system is owned by the SEC, and was developed by contractors. This system is operated on SEC servers located at the SEC.

7. What specific legal authorities, arrangements, and/or agreements defined the collection of data?
15 U.S.C. 77s, 77t, 78u, 77uuu, 80a-41, and 80b-9. 17 CFR 202.5

Specific Questions

SECTION I – Data in the System

1. What data is to be collected?
Data collected pertains to Matters Under Inquiry, Investigations and Actions and includes:

   • Internal identification and status information, including:
     • Matter Name
     • Matter Number
     • Date Opened
     • Date Closed
   • Staffing information
   • Narrative summaries
   • Substantive categorizations of the matter (e.g., Insider Trading)
Privacy Impact Assessment
The Hub (Upgrade)

- Procedural steps taken (e.g., access grants, investigative testimony, Wells notices)
- Links to key documents (e.g., Complaints, Orders Instituting)
- Court and filing information for Actions, including:
  - Forum
  - Date filed
  - Violations alleged
  - Relief sought
  - Outcomes of Actions

2. Is the Social Security Number (SSN) Collected? - If YES, provide the function of the SSN and the legal authority to collect it.
   Yes. Social Security Numbers of persons related to investigations are collected, pursuant to Section 21(a) of the Exchange Act and related rules authorizing the Commission to conduct investigations of potential violations of the federal securities laws, to identify such persons accurately and assist in determining involvement in other matters.

3. What are the sources of the data?
   Enforcement Staff enter the data directly into the Hub.

4. Why is the data being collected?
   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 use the data collected for the management of the cases and reporting of Division case-related metrics.

5. What technologies will be used to collect the data?
   The Hub system uses web-based application software based on Java 2 Enterprise Edition software architecture supported by a relational database. The system runs on the Solaris operating system and use the Version Manager product for version management. The system uses standard AD authentication.

6. Does a personal identifier retrieve the data?
   The data will be retrieved by a search of an existing data element such as the matter number, matter name, or the name of a party related to the case.

SECTION II – Attributes of the Data (use and accuracy)
1. Describe all uses of the data.
   The data will be used to facilitate management of Enforcement cases, including resource allocation and staff distribution of caseloads, and to accurately report on Division cases, including the status and dispositions of case information to SEC management in an effective and efficient manner.

2. Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining)
   No. The Hub system does not analyze data.
Privacy Impact Assessment
The Hub (Upgrade)

SECTION III – Sharing Practices
1. Will the data be shared with any internal or external organizations?
The data is not shared externally (except for publishing in agency reports like the Public Accountability Report various Division information based on data in the system, such as the number of enforcement actions filed in a given year). Internally, outside of the Division of Enforcement, a limited number of accounts are provided to staff from other agency Divisions to provide Enforcement information for use in the pursuit of their objectives. In addition, a subset of Hub data is made available in the agency’s internal “NRSI” system.

2. How is the data transmitted or disclosed to the internal or external organization?
No data is transmitted externally. Internally, a limited number of accounts are provided to agency personnel from outside the Division (see item III.1 above).

3. How is the shared data secured by external recipients?
N/A

4. Does the system receive or share Personally Identifiable Information (PII) with any other SEC systems, including systems hosted by an SEC contractor?
Yes. The subsystems are: CATS 2000, NRSI and BO Reports.

SECTION IV – Notice to Individuals to Decline/Consent Use
1. Was notice provided to the individual prior to the collection of data? A notice may include a posted privacy policy, a Privacy Act Statement on forms, or a System of Records Notice published in the Federal Register. If notice was not provided, explain why not.
Notice is provided to individuals via SORN SEC-42, Enforcement Files, and this PIA. In the context of SEC investigations, disclosures are made to individuals when information is collected from them in such disclosures as SEC Form 1661 and 1662.

2. Do individuals have the opportunity and/or right to decline to provide data?
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 declining 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.

3. Do individuals have the right to consent to particular uses of the data? If so, how does the individual exercise the right?
No. Individuals do not have the right to consent to particular uses of the data for the same reason stated above. As noted above, the routine uses of information are provided to individuals from whom information is sought in SEC Forms 1661 and 1662.

SECTION V – Access to Data (administrative and technological controls)
1. Has the retention schedule been established by the SEC Records Officer? If so, what is the retention period for the data in the system?
Privacy Impact Assessment
The Hub (Upgrade)

These records will be maintained until they become inactive, at which time they will be retired or destroyed in accordance with records schedules of the United States Securities and Exchange Commission as approved by the National Archives and Records Administration.

2. What are the procedures for identification and disposition of the data at the end of the retention period?
The data will be identified and disposed of using the procedures stated above.

3. Describe the privacy training provided to users either generally or specifically relevant to the program or system?
   All SEC staff and contractors receive annual privacy awareness training, which outlines their roles and responsibilities for properly handling and protecting PII.

4. Will SEC Contractors have access to the system?
   Yes. The Office of Acquisition requires a signed non-disclosure agreement for all contractor personnel. The NDA contains a Privacy Act clause.

5. Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?
   Yes. Certification and Accreditation for the Hub was last completed in February 2012.

6. Is the system exposed to the Internet without going through VPN?
   No.

7. Are there regular (i.e., periodic, recurring, etc.) data extractions from the system?
   Yes. OIT has in place policy and procedures to ensure logging, safe handling, and discarding of PII data extraction in the GSS System Security Plan (SSP).

8. Which user group(s) will have access to the system?
   The following user groups in Enforcement 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.

9. How is access to the data by a user determined? Are procedures documented?
   The system uses roles to assign privileges to users of the system based on the role of the user.

10. How are the actual assignments of roles and rules verified according to established security and auditing procedures?
    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. Role assignments are tracked through the system audit table available to system administrators.
11. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of the data?

   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.

SECTION VI - Privacy Analysis

Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

The likely privacy risk for this data collection is unauthorized or inadvertent disclosure of non-public data. The HUB utilizes access controls to protect the data. Additionally audit procedures have been implemented which include review of audit logs to ensure appropriate uses. A timeout feature is in place that forces the user out of the system which requires users to login again after being away from their computers. This feature prevents unauthorized individuals from viewing data on unattended computer screens.