U.S. PATENT AND TRADEMARK OFFICE

Enterprise Data Warehouse

Unique Investment Identifier: 006510101018003004021 29

USPTO Privacy Impact Assessment Statement

Prepared by: Brooks Hunt, Director, Office of Technical Plans and Policy
Reviewed by: Ron Hack, Acting Chief Information Officer

U.S. Patent and Trademark Office

USPTO Office of the Chief Information Officer (OCIO)

Privacy Impact Assessment (PIA)

1. What information is to be collected (e.g., nature and source)?

The information to be collected by the system includes financial transactions; USPTO employee payroll transactions; budget information including allocation, expenditures and available funds; general ledger; Patent Production; Personnel data; Cost Accounting information; and Revenue data.

The data sources include FFS (Federal Financial System), NFC (National Finance Center), USPTO's Office of Human Resources, and the following internal USPTO systems: Revenue Accounting and Maintenance (RAM), Patent Application Locating and Monitoring Post-Exam (PALM EXPO), Activity Based Modeling (ABM), and Momentum.

2. Why is the information being collected (e.g., to determine eligibility)?

The collection of the information makes it possible that financial, personnel and patent data are linked into one single system The Enterprise Data Warehouse (EDW) such that USPTO employees making business decisions and analysis, including real-time budget and general ledge, reconciliation of Federally mandated requirements, have immediate access to summary and transaction-level detailed information.

The EDW is maintained by the USPTO and it resolves the data access and presentation difficulties in providing strategic business information to analysts and managers. Use of the EDW enables the USPTO to operate more efficiently and economically by bringing together widely disparate systems and platforms containing data that needs to be shared. The use of the Business Objects COTS application ensures a user-friendly front-end interface to a single database.

3. What is the intended use of the information (e.g., to verify existing data)?

The information is used in supporting the decision making activities of managers and analysts in the USPTO business areas. The EDW project makes this possible. It is a Corporate IT investment that provides access in one single system to integrated USPTO General Ledger, Revenue, Payroll, Cost Accounting, Patent Case and Patent Examiners production data.

4. With whom the information will be shared (e.g., another agency for a specified programmatic purpose)?

The information is shared within USPTO with authorized parties only. There is no other agency involved.

5. What opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

The data warehouse does not create data and it only integrates existing data from multiple sources. It makes data comparisons available for analysis.

6. How will the information be secured (e.g., administrative and technological controls)?

Management Controls:

The USPTO uses the Life Cycle review process to ensure that management controls are in place for the EDW. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the Security Plan, which is a document prepared during the Concept Phase of the project's life cycle. The Security Plans specifically address the management, operational and technical controls that are in place, and planned, during the operation of the enhanced system. Additional management controls include performing national agency check on all personnel, including contractor staff.

Operational Controls:

Operational controls include securing all hardware associated with this system in the USPTO Data Center. The Data Center is controlled by access card entry, and is manned by a uniformed guard service to restrict access to the servers, their operating systems and databases. Contingency planning has been prepared for the data center as a whole and is documented in the Infrastructure Disaster Recovery Plan (updated 08/2002). Backups are performed on the processing databases every production day (Monday through Friday). The backups include all file directories (except the operating system directory) and the database. Backups are stored on tape and are secured off-site. The Office of System and Network Management (OSNM) are responsible for ensuring the security of the backups or other tapes. Additional operation controls include: (1) Logical edit checks to ensure proper sequence of actions; (2) Physical terminal identification; (3) Database UserID; (4) Restricted data display, as required; and (5) Restricted access.

Technical Controls:

Technical Controls such as password authentication (userid and passwords) on the server are accomplished by using operating system userids and passwords on the host, and database userids and passwords. At the client PCs, access is managed through a password authentication (userid and password) based on certification on a Financial Application Security Registration form. The security form must be signed by a supervisor, and requires additional approval from Human Resources based on a justification of need.

7. Is a system of records is being created under the Privacy Act, 5 U.S.C. 552a.?

The data warehouse does not create data and it only integrates existing data from multiple sources. The EDW is not a system of record but a compilation of data from other systems of record which have their own PIA and controls.

Privacy Impact Assessment (PIA)

The data in the system contains employee social security numbers and banking information. However, the information is retrieved only by authorized individuals and is transferred only when necessary for payroll transactions and personnel purposes. Electronic transmission of such data occurs only through secure, encrypted communication paths.