U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment

Enterprise Data Warehouse

PTOC-003-00

April 5, 2010

Privacy Impact Assessment

This Privacy Impact Assessment (PIA) is a requirement of the Privacy Act of 1987 and OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.* A PIA documents the due diligence and oversight placed upon information associated with the project or system in question. Written from the System Owner's perspective for the American public, the PIA discloses what information is being collected, and how that information is protected. The intent is to build confidence that privacy information is secure, processes that utilize this information comply with Federal requirements, and more importantly, inform the privacy expectations of the American public.

The Privacy Threshold Analysis (PTA) is a separate artifact that must be completed prior to beginning this PIA. In many cases, the PTA will be the only required artifact to satisfy DOC privacy considerations.

SYSTEM DESCRIPTION

EDW is a network-connected system. It is implemented using Transmission Control Protocol/Internet Protocol (TCP/IP) on a Microsoft Windows and HPUX client/server architecture, which uses the PTOnet for connectivity to the EDW production server, Oracle Database and to the users' Windows client workstations. EDW is installed in the USPTO Data Center facility, which occupies Madison West Building, 3rd Floor, Alexandria, VA 22314. This system is supported/maintained by government and contract staff. The key features of the EDW are:

Enterprise Reporting – which is an interface that allows users to have access to pre-run reports and Business Objects based on security privileges. The only way to access the EDW is via Enterprise Reporting. This tool gives users access to pre-run reports and Business Objects.

Business Objects – which is an application tool that provides user access based on security privileges and allows the user to access the data through a user-friendly interface.

The EDW provides the following services or functions in support of the USPTO mission: The purpose of EDW is to provide access to integrated USPTO General Ledger, Revenue, Payroll, Cost Accounting, Human Resources, Budget, Compensation Cost Projection, Patent Case, and Patent Examiner Production data to support the decision making activities of managers and analysts in the USPTO's business areas as needed to achieve USPTO's business goals. EDW is intended to help managers and analysts within USPTO to answer, using quantitative enterprise business information, a variety of strategic and tactical business questions. Specifically, the system will provide a tool that enables managers and analysts to analyze business processes, resource use and needs, and other facets of the business. This information, properly presented, will bring the USPTO closer to the goal of being a world-class office.
EDW supports the following categories of users and the approximate numbers of users for each category.

External Affairs	7
General Counsel	16
Office of Chief Administrative Officer (OCAO)	91
Office of Chief Financial Officer (OCFO)	257
Office of Chief Information Officer (OCIO)	184
Patents	276
Trademarks	10
Under Secretary	9

QUESTIONNAIRE

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

   The information to be collected by the system includes USPTO's business information about USPTO General Ledger, Revenue, Payroll, Cost Accounting, Human Resources, Budget, Compensation Cost Projection, Patent Case, Patent Examiner Production and Job Application Rating System (JARS), Time and Attendance, Federal Procurement and Corporate Planning data to support strategic and tactical decision-making.

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

   The information is collected to provide a single data source to facilitate ad-hoc queries and analysis of data by managers and analysts in the USPTO's business areas at their desktop without assistance from information technology specialists. Specifically, the system will provide a tool that enables managers and analysts to analyze business processes, resource use and needs, and other facets of the business and provide the USPTO with the means of performing at a more efficient, accurate, and cost effective level.

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

   This information is collected to support the decision making activities of managers and analysts in the PTO's business areas to analyze USPTO data necessary to supply parameter data derived from actual historical information needed by analytical models, such as OPBudget and OCIO Executive Information System to achieve USPTO's business goals. EDW is intended to help managers and analysts within USPTO to answer, using quantitative enterprise business information, a variety of strategic and tactical business questions. Specifically, the information will provide managers and analysts the ability to analyze business processes, resource use and needs, and other facets of the business at their desktop without assistance from information technology specialists.

4. With whom will the information 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 do 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 can individuals grant consent?

   Information is not directly provided by individuals. The Data Warehouse 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. 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 operation systems and databases. Contingency planning has been prepared for the data. Backups are performed on the processing databases. Backups are stored on tape and are secured off-site. Additional operation controls include: (1) Logical edit checks to ensure proper sequence of action s; (2) Physical terminal identification; (3) Database UserID; (4) restricted data display, as required; and (5) restricted access.

Technical Controls:
Technical Controls include password authentication (userid and passwords). At the client PCs, access is managed through a password authentication (userid and passwords) based on certification on a Financial Application Security Registration form. The security corm must be signed by a supervisor, and requires additional approval from Human Resources based on a justification of need.

7. How will the data extract log and verify requirement be met?

USPTO has not developed a centralized logging system for PII data extracts. Such a system would track the following categories of information:
Who performed the extract,
When extract was done,
What was the extract,
Where was the extract taken from,
Has the extract been deleted and,
If not deleted after 90 days, to monitor that it is still needed in 90 day intervals.

Until a system is implemented, USPTO is using the following compensating controls to protect PII data:
No extracts of sensitive data may be copied on to portable media without a waiver approved by the DoC CIO. The request for a waiver must include specifics as to how the data and device are protected, how long the data will be maintained, and how the data on the device will be deleted when no longer required.
All laptop computers allowed to store sensitive data must have full disk encryption.
All remote access to public USPTO systems containing sensitive data must be encrypted. All remote access to internal USPTO systems containing sensitive data must fully comply with DoC Remote Access Policy requirements.
All flexiplace/telework agreements for working off site require that adequate data protection be in place.

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

   No, there is no new system of records being created. Existing Systems of Records cover the information pulled from other systems residing in the Enterprise Data Warehouse. These include: Commerce/PAT-TM-3, Employee Production records; Commerce/PAT-TM-7, Patent Application Files; Commerce/PAT-TM-10, Patent Deposit Accounts System; and Commerce/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies.

9. Are these records covered by a record control schedule approved by the National Archives and Records Administration (NARA)?

   No. GRC 20 allows agency determination that certain electronic records are authorized for erasure or deletion when they are no longer needed for administrative, legal, audit, or other operational purposes. Electronic records that represent hard copy records can be deleted after expiration of the retention period authorized for the hard copy records.

SIGNATORY AUTHORITY

	/s/ Gita Zoks	4/27/2010
Agreed:	_____	_____/_____/_____
	Gita Zoks	Date
	Information System Owner	
	/s/ Rod Turk	4/29/2010
Agreed:	_____	_____/_____/_____
	Rod Turk	Date
	Senior Agency Information Security Officer for EDW	
	/s/ John B. Owens II	5/4/2010
Agreed:	_____	_____/_____/_____
	John B. Owens II	Date
	Co-Authorizing Official for EDW	
	Mark Olechowski (Deputy CFO)	5/10/2010
Agreed:	_____	_____/_____/_____
	Karen Strohecker	Date
	Co-Authorizing Official for EDW	