U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment

Information Dissemination Support System

PTOD-001-00

December 17, 2009

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

Information Dissemination Support System (IDSS) is a Major Application (MA) that supports the Trademark and Electronic Government Business Division, the Corporate Systems Division (CSD), the Patent Search System Division, the Office of Electronic Information Products, and the Office of Public Information Services. IDSS provides automated support for the timely search and retrieval of electronic text and images concerning patent applications and patents by USPTO internal and external users.
IDSS handles current and historical data for patent and trademark applications, whether assigned, certified, issued, or not. It contains interfaces to share data with other information systems throughout the PTOnet and the Internet. IDSS is considered a business-essential system with a Federal Information Processing Standard (FIPS) 199 security categorization of Moderate.

IDSS implements a large, distributed and complex computing environment and each of its automated information systems (AIS) physically reside on a collection of hardware and software components, and services, with various interfaces. The system uses the USPTO's network infrastructure to allow interaction between its subordinate information systems.

IDSS' subordinate information systems include the following:

Assignment Historical Database/ Assignments on the Web (AHD / AOTW)

AHD

The purpose of AHD is to provide a historical record(s) of changes affecting the transfer of ownership or rights of ownership to an intellectual property. It provides a search tool allowing both internal and external users with the ability to track changes in ownership to a patent or trademark property. It provides for a textual display and an image based display of the document submitted requesting recordation of assignment. The system is comprised of an Oracle database and a single web application deployed to different web environments, AHD is deployed to an IPlanet web server, supports PTOnet internal users which includes the Assignment Services Branch, other USPTO personnel such as patent and trademark examiners and their supporting staff and the Public Search Facilities staff users and public users. Data displayed in the public AHD is restricted to publicly available data (i.e., pending patent application data is not available to public customers via AHD).

- AHD is the permanent Oracle database that is used to store permanent textual data associated with recorded assignments for both patent and trademark properties.
- AHD provides a Web-based application with resource locator addresses that allow USPTO staff members to review and search assignment data related to patent or trademark properties. Public users have restricted access and may search only by publish application number (Pre-Grant Pub) and/or issued patent numbers as well as trademark application or trademark registrations.
- AHD extracts specific data elements for all recorded trademark assignments received on or after November 2, 2003 and transmits the file to ClearPath each week. The program generates two types of files: one contains owner names and addresses and the other file contains an indicator as to whether an assignment has been received. When an assignment is received, the program alerts Trademarks to set a flag to indicate that the Trademark examiner and/or paralegals should review the file when verifying ownership information in the Trademark Reporting and Monitoring System (TRAM) database.

- AHD extracts data for both patent and trademark-recorded assignments each month and contains an indicator with each record that identifies availability for public access. The file is copied to a UPWS server.
- The following data dissemination products are also created:
    - Patent Assignment XML file: This file is transmitted to the Executive for Customer Information Services daily. It contains only Patent Assignment records related to published applications and/or issued patent applications that were created / modified during the previous 24 hours.
    - Patent Assignment XML file: This file is transmitted to the Executive for Customer Information Services bi-monthly. It contains all patent assignment records related to published applications and/or issued patent applications maintained in the historical database that were created/modified during the previous two months.
    - Patent Assignment XML retrospective file: This file is currently transmitted to the Executive for Customer Information Services annually, but consideration is being given to a bi-annual transmission.
    - Trademark Assignment XML file: This file is transmitted to the Executive for Customer Information Services daily. It contains all trademark assignment records that were created / modified during the previous 24 hours.
    - Trademark Assignment XML file: This file is transmitted to the Executive for Customer Information Services bi-monthly. It contains all trademark assignment records maintained in the historical database that were created or modified during the previous two months.
    - Trademark Assignment XML retrospective file: This file is currently being transmitted to the Executive for Customer Information Services annually, but consideration is being given to a bi-annual transmission.

AOTW

AOTW provides the capability for external users of the USPTO as well as public users in the USPTO public search rooms (with access to the Internet) to query issued patent or published application patent assignment data and/or pending or registered trademark assignment data. The AOTW web application is deployed to the middleware environment running under Websphere web servers and is available to external customers/users of the USPTO (outside of PTOnet) via the Internet.

Broadcast Notification System (BNS)

The BNS provides, from a centrally managed location, day-to-day information to kiosks located in the building lobbies located around the USPTO campus. Each kiosk holds a 40-inch monitor and a workstation. The monitors display via the PTOnet various types of dynamic information at the locations throughout the Alexandria and Arlington USPTO campuses. BNS informs visitors and staff of upcoming events, general interest information, management presentations, and security notices via large displays placed in building lobbies. The system was implemented as another way to increase communication by the displays providing relevant textual, graphical, or video information to people in a USPTO building lobby, or other significant area(s).

Data File Delivery (DFD)

Data File Delivery (DFD) delivers subscription patent and trademark data files, on the day of issue, to customers via electronic transmission. The system authenticates users through the use of a User ID and password prior to allowing user-initiated transmission of daily, weekly, monthly, bi-monthly, and yearly subscription patent and trademark files.

Emergency Notification System (ENS)

- AtHoc Notifications Server – provides central application functionality, as well as web based administration and alert activation console.
- AtHoc Publisher, including Alerts Publisher and Manager – web based application to publish and manage alerts, including pre-defined alerts, based on alert type and publisher's rights and permissions.
- Web based administration console - allowing for central system administration using a role and permissions based secure access model.
- Desktop Alerts Software – small footprint standard based software client installed on end-user desktops, deployed via Microsoft System Management Server (SMS) or other remote installation applications. The desktop software is responsible for the timely communication with the AtHoc Notification Server via HTTP or HTTPS to receive alerts and display the desktop popup visual and audio cues.
- Alert Targeting Server Module – a module running on the Notifications Server, enabling publishers to target alerts to specific groups of users based on groups defined in the base's user directory (i.e. LDAP or Active Directory). Integration with LDAP or Active Directory is required to enable use of this module.

File Tracking System (FTS)

The purpose of FTS is to provide automated file control functions in the File Information Unit (FIU) including:

- Warehouse order receipt.
- Warehouse order tracking.
- Warehouse order return.
- Client file wrapper orders.
- Client file wrapper order status.
- Client file wrapper order check-in/out.
- Client Authentication.

Order Entry Management System / Certification (OEMS)

Primarily, OEMS manages the entry and fulfillment of orders for certified or uncertified copies of patents, trademarks, and related documents such as Patent Application Publications under Pre-Grant Publications (PGPubs) received by the Document Services Branch (DSB) of the Public Records Division (PRD). OEMS assists in performing a critical part of the information dissemination mission for the United States Patent and Trademark Office (USPTO). It helps to provide revenue through efficient automation of several tasks involved in order management and administration through gathering, processing, and reporting statistics. OEMS also provides customers with the capability to enter orders directly, receive the orders, and make inquiries via the Internet.

Document retrieval and printing is performed by the Patent and Trademark Copy Sales (PTCS) Migration Project (P2MP) and InfoPrint subsystems. P2MP functions as a document retrieval and print subsystem to OEMS and provides a batch mode interface and real-time interface to OEMS. P2MP also retrieves the patent fax requests from OEMS and faxes the requested patent to the customers.

On-Line Access Card (OLAC)

The OLAC system provides automated support and internal controls to allow public access to USPTO search systems. The system includes the creation of plastic access cards to validate public users. Data collected consists of the public user's name, street address, e-mail address, and telephone number; where name and

address are required fields. Based on OLAC system privileges, each user has the capability to access administrative functions, such as:

- Report generation
- Password management
- User permissions management
- System preferences management

Patent and Trademark Assignment System (PTAS)

The Patent and Trademark Assignment System (PTAS) supports processing of assignment documents through electronic submission, image capture, OCR text capture, automated workflow processing, management and inventory reporting and generation of computer output microfilm of recorded documents from electronic images. PTAS also provides Web based applications via the Internet referred to as the ETAS (Electronic Trademark Assignment System), which allows submission of a trademark assignment, and the EPAS (Electronic Patent Assignment System), which allows submission of a patent assignment.

Trademark Assignment and Data Dissemination Services (TADDS/TDXF)

TADDS is comprised of two sub systems, 24 Hour Box and Trademark Daily XML File (TDXF). The 24 Hour Box function/purpose is to provide copies of Trademark application drawing files in electronic format. There are two programs responsible for providing these image files. The primary 24 hour box program retrieves images files submitted via electronic filing. During the processing of Trademark filings, the images files as submitted are copied to a specific location that the 24 Hour Box program uses to package and delivery to an EIPD server. The second program "supplemental" 24 hour box accesses a directory on a different Trademark Server to obtain copies of cropped image files submitted in paper form. Before the paper filed drawings are used in Trademark there are first cropped to a required image size. It is the cropped images that the 24 hour Box supplemental program copies and packages for delivery to an EIPD server. TDXF is a collection of programs that operate individually from each other to create an individual product that EIPD uses for dissemination to external customers. The TDXF's function/purpose is to provide bibliographic (textual) data related to Trademark Intellectual properties in extensible Markup Language (XML) files. Three separate different business areas maintain responsibility for the Trademark Intellectual property data. The three products are comprised of Trademark Application and/or Registration records, recorded Trademark Assignment data and Trademark Trial and Appeal Board records.

USPTO Customer Contact Management System/Sales Order Management System (UCCMS/SOMS/SOMS)

UCCMS/SOMS/SOMS provides the USPTO with a customer contact and problem management system to help the following agencies better track and manage customer inquiries:

- The USPTO Contact Center (UCC).
- The Trademark Assistance Center (TAC).
- The Inventors Assistance Center (IAC).
- The Patent Electronic Business Center (PEBC).
- The Public Search Facility (PSF).
- The Assignment Services Branch/Public Records Division (ASB/PRD).
- Application Assistance Unit (AAU) formed with merger of The Office of Initial Patent Examination (OIPE) and Office of Patent Pub.
- The Receipts Accounting Department (RAD) under the Office of Finance.

- The Trademark Trials & Appeals Board (TTAB) under the Office of General Counsel.
- The Office of Governmental Affairs (OGA).
- The Office of Chief Administrative Officer (CAO) Tele work database.
- The Global Intellectual Property Academy (GIPA).
- The Office of Intellectual Property Policy and Enforcement (OIPPE)

This system is primarily a Siebel Call Center, a commercial-off-the-shelf (COTS) product that provides a Web-based system that allows Customer Service Representatives (CSRs) in the call centers to better manage their customer service process, customer information, and respond to customer questions using a knowledge-based system. In addition, UCCMS/SOMS supports the order entry, order processing, and order tracking capabilities required by the Electronic Information Products Division (EIPD) for tracking data product customers and subscriptions. To reduce the workload for EIPD staff, UCCMS/SOMS developed a Web-based application called Lower-Cost Trademark Bulk Data (LCTBD) to enable public users to register and download the trademark bulk data. The UCCMS/SOMS also includes application enhancements to support the Office of Governmental Affairs (OGA), Office of Chief Administrative Officer (CAO) Tele work database, Global Intellectual Property Academy (GIPA), and Office of Intellectual Property Policy and Enforcement (OIPPE).

Universal Public Workstation/CD-ROM Reference Library (UPWS/CRLS)

The purpose of the UPWS project is to provide a client-server solution to:

- Provide public user access to United States Patent and Trademark Office (USPTO) automated applications.
- Automate the fee collection processes within the Public Search Facilities (PSF).
- Provide service and managerial information and reports.

QUESTIONNAIRE

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

UCCMS/SOMS captures customer service data including for external USPTO public customers. This data includes customer name, phone number, address, email address, fax numbers, agent name, and customer number. This is currently provided on a voluntary basis except for the EIPD web interface, which requires an email address for registration to download electronic information products; no other personal identifiable fields are required.

The **OLAC** system requires the user's first and last name in order to gain access to UPWS and FTS. The UPWS system provides the core functionality of secure user access, application launch, application utilization, fee collection, print services fee collection, and administrative services. Data collected includes user name, password, customer name, phone number, address, email address, fax numbers, and payment information.

OEMS provides certified and uncertified copies of Patent and Trademark documents to world wide customers. In order to process customers' requests, OEMS collects:

- Customer information: name, phone number, address, email address, and fax number (Source – Customer)
- Order Information (Source – Customer)
- Payment Information (Source – Customer)
- Patent and Trademark images (Source - Multiple AIS's within PTO– eDAN/IFW, AIRS, PIRS and TICRS)

The **PTAS** system processes a Request for Recordation of Assignment for both Patents and/or Trademarks. PTAS collects correspondence data such as name and address, phone number, fax phone number, seller name, buyer name and address, intellectual property identified in the assignment transaction, type of assignment transaction (sale, lien, merger, and many others) – all data is provided by the customer at filing time. PTAS information collected is forwarded (93% of the time) to AHD for permanent retention.

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

Information such as user name, password, customer name, phone number, address, email address, fax numbers, payment and financial transactions are collected to determine access eligibility, forward customer requests to the appropriate business areas, provide customer service request follow up, and properly carry out functionalities each information system was designed to perform/capture.

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

Information collected is used to process transactions, manage customer orders, document delivery, retrieve data, and capture documents related to the ownership of intellectual properties for both patents and trademarks. The intended use is to carry out the duties of the USPTO as outlined in 35 U.S.C. concerning the dissemination of information, and more specifically, to provide for public customer call center services. This includes tracking responses to customer requests. Data is used to ensure quality customer service for

general agency information and assistance. This includes quality control purposes. In addition, the information may be used to conduct surveys of customer experience and satisfaction, and to obtain customer service recommendations.

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

The information is not shared with any outside entities and is for internal use only. Only certified and uncertified copies of Patent and Trademark images are provided to entitled and authorized customers. Information may be subject to General Routine uses (Privacy Act) Nos. 1-5, 9-10, and 12-13 as found at 46 CFR 63501-63502.

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?

All information requested is provided on a voluntary basis. Certain information such as name and phone number would be required to complete the processing of the request or if the customer requires a follow-up on their original service request and for quality control purposes.

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

The information is in accordance with the NIST 800-53, Revision 2 control set. Certification and Accreditation activities are routinely conducted for IDSS. Secured technical architecture is incorporated into the system to prevent any unauthorized access to pending cases. Data is maintained in areas accessible only to authorize personnel and systems are password protected.

Management Controls:

1. The USPTO uses the Life Cycle review process to ensure that management controls are in place for IDSS. 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.

2. The USPTO Personally Identifiable Data Extracts Policy

Operational Controls:

1. Automated operational controls include securing all hardware associated with IDSS 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. 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 actions; (2) Physical terminal identification; (3) Database UserID; (4) Restricted data display, as required; and (5) Restricted access.

2. Manual procedures shall be followed for handling extracted data containing sensitive PII which is physically transported outside of the USPTO premises. In order to remove data extracts containing sensitive PII from USPTO premises, users must:
    a. Maintain a centralized office log for extracted datasets that contain sensitive PII. This log must include the date the data was extracted and removed from the facilities, a description of the data extracted, the purpose of the extract, the expected date of disposal or return, and the actual date of return or deletion.

    b. Ensure that any extract which is no longer needed is returned to USPTO premises or securely erased, and that this activity is recorded on the log.

    c. Obtain management concurrence in the log, if an extract aged over 90 days is still required.

    d. Store all PII data extracts maintained on an USPTO laptop in the encrypted My Documents directory. This includes any sensitive PII data extracts downloaded via the USPTO Virtual Private network (VPN).

    e. Encrypt and password-protect all sensitive PII data extracts maintained on a portable storage device (such as CD, memory key, flash drive, etc.). Exceptions due to technical limitations must have the approval of the Office Director and alternative protective measures must be in place prior to removal from USPTO premises.

USPTO has not developed a centralized logging system for PII data extracts. Such a system would track the following categories of information:

a. Who performed the extract,
b. When extract was done,
c. What was the extract,
d. Where was the extract taken from,
e. Has the extract been deleted and,
f. 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:

a. 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.
b. All laptop computers allowed to store sensitive data must have full disk encryption.
c. 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.
d. All flexiplace/telework agreements for working off site require that adequate data protection be in place.

Encrypt and password-protect prior to transmission any sensitive PII data extracts that are sent to an external e-mail address via the Internet. The password key should be forwarded to the recipient in a separate e-mail from the attached file.

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:

a. Who performed the extract,
b. When extract was done,
c. What was the extract,
d. Where was the extract taken from,
e. Has the extract been deleted and,
f. 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:

a. 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.
b. All laptop computers allowed to store sensitive data must have full disk encryption.
c. 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.
d. 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?

A system of records exists. "COMMERCE/PAT-TM-20 Customer Call Center, Assistance and Satisfaction Survey Records, August 2007."

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

Agreed: /s/ Judy Johnson Joyner 3/8/2010

Judy Johnson-Joyner
System Owner for IDSS

Date