U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE (USPTO)

Privacy Impact Assessment

Intellectual Property Leadership Management Support System (IPLMSS)

PTOL-001-00

February 24, 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, and 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 process that must be completed prior to beginning the PIA. In many cases, the PTA will be the only required artifact to satisfy DOC privacy considerations.

SYSTEM DESCRIPTION

The components of the IPLMSS are primarily located at 600 Dulany Street, Alexandria, VA 22314, on the 3rd floor, east wing at the Data Center. The IPLMSS system resides on the USPTO network (PTOnet).

The purpose of the Intellectual Property Leadership Management Support System (IPLMSS) is to provide automated support to USPTO internal and external users for the timely search and retrieval of electronic text and images concerning Patent Practitioners, Patent Appeals Board cases and Trademark Trial and Appeals Board information by dissemination.

The system supports the Office of General Counsel (OGC).

IPLMSS system users are internal users of the USPTO. Users of the individual components of IPLMSS are contained within the Active Directory (AD) for PTONet and are managed through group assignment to the individual applications.

QUESTIONNAIRE

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

The information to be collected by the information systems includes Admittance to Practice and Roster of Registered Patent Attorneys and Agents Admitted to Practice Before the USPTO; Practitioner Records Maintenance, Disclosure and Discipline Before the USPTO; Legal Processes; and Patent Appeals and Interferences.

The IPLMSS data sources are the following:

- Office of General Counsel – private practitioners, practitioners, and the Patent Application Locating and Monitoring Post-Exam (PALM EXPO).
- Trademark Trial and Appeal Board (TTAB) systems – name and address of practitioner, contact phone number, and email address.
- Adjudicated Cases and Interferences – name and address, telephone number, email address and attorney registration number.
- Enrollments and Discipline – legal name of applicant, address, citizenship status, date of birth, place of birth, telephone number, examination waiver status, reinstatement status (if applicable), examination performance, bar status, disciplinary and background information, and education.
- Work history information is also provided by former USPTO employees.

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

The USPTO is responsible for regulating and managing the listing of attorneys and agents as it pertains to practicing before the USPTO.

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

The information is used to render decisions in accordance with Administrative Patent Law, regulate discipline and communicate, as necessary, with attorneys and agents who are registered to represent applicants for Patent protection.

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

The information is used within USPTO with authorized parties only. There are no other agencies involved unless involvement with the Federal Courts ensues. Individual records may be shared with Federal Courts, but not the system of record.

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?

Individuals are provided a privacy act statement at which time they may opt to decline to provide information. However, individuals must submit the required information in order to have requests for intellectual property

protection processed. Similarly, an agent or attorney who wishes to practice before the USPTO must comply in full with the request for registration information.

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

In accordance with NIST 800-18 Rev. 1 and NIST 800-53 Rev. 2 the IPLMSS System Security Plan (SSP) addresses the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment. The SSP is reviewed on an annual basis. In addition, annual assessments, Continuous Monitoring reviews, and triennial assessments are conducted on the IPLMSS data. The USPTO ITSMG conducts these assessments and reviews based on NIST SP 800-53 Revision 2, *Recommended Security Controls for Federal Information Systems* and NIST SP 800-53A Final *Guide for Assessing the Security Controls in Federal Information Systems*. The results of these assessments and reviews are documented in the IPLMSS Security Assessment Package as part of the system's Certification & Accreditation (C&A) process.

Management Controls:

A. The USPTO uses the Life Cycle review process to ensure that management controls are in place for the IPLMSS. 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 checks on all personnel, including contractor staff.

B. The USPTO Personally Identifiable Data Removal Policy

Operational Controls:

A. Automated operational controls include securing all hardware associated with the IPLMSS 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 operational 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.

B. Manual procedures shall be followed for handling extracted data containing sensitive PII which is physically transported outside the USPTO premises. In order to remove data extracts containing sensitive PII from USPTO premises, users must:

   i. 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.

   ii. 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.

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

iv. 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).

v. 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.

vi. 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.

Technical Controls:

A. 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. A supervisor must sign the USPTO desktop security form before the user has access to the computer.

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

No. There is no new system of records for these records. Existing Systems of Records cover the information already residing in the databases. These include: COMMERCE/PAT-TM 1, Attorneys and Agents Registered to Practice Before the Office; COMMERCE/PAT-TM 2, Complaints, Investigations and Disciplinary Proceedings Relating to Registered Patent Attorneys and Agents; COMMERCE/PAT-TM 5, Non-Registered

Persons Rendering Assistance to Patent Applicants; and COMMERCE/PAT-TM 6, Parties Involved in Patent Interference Proceedings.

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.

I have reviewed and approve the attached Privacy Impact Assessment document(s).

/s/ John B. Owens II 4/6/2010

John B. Owens II Date
Co-Authorizing Official for IPLMSS

/s/ Raymond Chen 3/28/2010

James A. Toupin Date
Co-Authorizing Official for IPLMSS