U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment

Service Oriented Infrastructure (SOI)

March 4, 2015

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

The Service Oriented Infrastructure (SOI) provides a feature-rich and stable platform upon which USPTO applications can be deployed. SOI consists of the following components:

Windows Web Servers and UNIX Web Servers

SOI includes web servers running Apache and HTTP servers. Load Balancers and iPlanet reside on the UNIX platform, and web servers running Internet Information Services (IIS) and SunOne Web Server on the Windows platform. These web servers are responsible for accepting HTTP and HTTPS requests from web clients and passing the requests to the application servers.

WebSphere, and Documentum

SOI also provides services that support WebSphere and Documentum. These services are generally considered the middle and back-end tiers of n-tier application architecture. The presentation tier is outside the scope of the SOI Authorization boundary and is managed by the major applications that require the use of a front-end client to display information.

The middle tier consists of Web Servers and WebSphere. The web servers are responsible for accepting and passing HTTP and HTTPS requests from web clients to the application servers that are utilizing the WebSphere infrastructure. WebSphere is an application deployment infrastructure for Java 2 Enterprise Edition (J2EE)-compliant applications that include enterprise messaging services, data transformation, Message Driven Beans running in the WebSphere environment, and portal services for all web-based applications.

The back-end tier consists of Documentum, which serves as the enterprise content management software allowing business units to create, process, and manage workflows and documents.

JBoss

The JBoss Enterprise Application Platform (EAP) and Enterprise Service Oriented Architecture (SOA) platform provide the foundation for decoupled interoperability between USPTO systems by providing a service gateway framework. Combined with JBoss EAP and SOA-P, the framework provides an enterprise-class service bus or ESB which is used for designing and implementing the interaction and communication between mutually interacting software applications within a SOA at USPTO. The JBoss ESB provides Business Process Monitoring, Integrated Development Environment, Human Workflow User Interface, Business Process Management, Connectors, Transaction Manager, Security, Application Container, Messaging Service, Metadata Repository, Naming and Directory Service, Distributed Computing Architecture.

eNewsletter

The eNewsletter system is an enterprise solution that allows business areas to communicate to large groups of stakeholders via e-mail with eNewsletter. The USPTO encapsulates many business areas that support and work with multiple internal or external stakeholder groups. These business units need to have the ability to send mass eNewsletters to these stakeholder groups. The individuals in the stakeholders groups have the ability to add, delete and edit their eNewsletter offerings. The business units that use the system have reporting features available to them to understand the effectiveness of their communications.

www.uspto.gov

www.uspto.gov (Internet) provides the public and key stakeholders with information from USTPO about all aspects of intellectual property. It serves as the main web-based information dissemination channel for the Agency and provides links to public-facing, web-based applications used to conduct the Agency's day-to-day operations.

Image Gallery

The Image Gallery will establish the ability to catalog, track, and make available a curated set of approved images for use on USPTO web properties. The solution is based on an open source product (Gallery) and is targeted at a limited user group of USPTO internal users.

PTOWeb

PTOWeb is the USPTO's corporate intranet website serving as the primary internal communication, information dissemination and collaboration system for employees and contractors. Offices within the USPTO are able to utilize the Intranet Website to meet everyday business goals on ptoweb.uspto.gov web site.

Helix

Helix is a full-featured streaming media server that delivers files such as Flash, Windows Media, and QuickTime. Helix-1 is the public-facing server used to deliver on-demand video files, and Helix-2 is used for internal audiences.

Broadcast Notification System

The Broadcast Notification System (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).

RDMS

The Reference Document Management Services (RDMS) system is designed to serve as USPTO's enterprise-wide content management solution for reference and guidance documents – a critical tool for patent and trademark examiners and applicants. The current RDMS system state allows intranet web-based access to Manual for Patent Examination Procedures (MPEP) and the Trademark Manual for Examination Procedures, the primary guidance document utilized by Patent and Trademark examiners. RDMS was just recently upgraded to allow public internet access to applicants who wish to submit patent and trademark applications.

MyUSPTO

MyUSPTO is an external-facing web site application intended for public access. The purpose of the system is to reduce the number of logins for external USPTO customers and to provide a single location from where they can conduct their business with the USPTO. MyUSPTO Release 1 provides the following capabilities:

- Provide external stakeholders with one unified place to register with the USPTO, manage their contact information and other identifying information, and manage their fees.
- Present a uniform look and feel to USPTO web services and web site information.
- Provide a foundation architecture which allows other NG applications to interact with MyUSPTO and provide data consistency for all customer account information.

QUESTIONNAIRE

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

   MyUSPTO collects the following information from an interested party that has successfully completed the user registration and account profile process.

   - E-mail address (Primary and/or alternate)
   - First name and last name
   - Phone number (cell, home, and/or work)
   - Address (e.g. street, city, state, zip, country)
   - Security question answers to at least 3 of the following questions:
     - Father's middle name,
     - First pet's name,
     - All-time favorite sports team,
     - High school mascot,
     - Name of first school,
     - City/town of birth,
     - Favorite comic book hero,
     - Favorite hobby,
     - Mother's middle name,
     - Color of first pet
     - The year the individual met their spouse/partner, and
     - The number of bedrooms in the individual's house/apartment

   No other SOI component collects information requiring disclosure in this PIA.

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

   MyUSPTO allows the general public to create a single account to serve as a single identity for interacting with USPTO services that have integrated with MyUSPTO. This information is being collected to verify the identity of customers using these services.

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

   The collected information is intended to be used by the USPTO service desk verify the identity of customers interacting with MyUSPTO.

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

   The information collected will not be shared with any other agency. This information is to be used only by the USPTO for the purpose of identity proofing and verification.

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?

   External customers who wish to use MyUSPTO must create an account via an online self-registration process. As part of the first step in the registration process, a user must click on a checkbox that explicitly states, "I understand and agree with USPTO's Terms of Use and Privacy Policy." Links are provided to the Terms of Use and Privacy Policy detailing the authorized uses of collected information. After this initial consent, an individual must complete the registration process by filling out their account profile. At this stage in the process, the individual can refuse to provide the required information, but will not be able to complete the self-registration process. Successful submission functions as consent for use of the information for the intended purpose.

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

   The information will be secured in accordance with USPTO policies, Federal laws, and NIST guidance (e.g. Risk Management Framework).

   In accordance with the Federal Information Security Management Act and the Risk Management Framework, the SOI System Security Plan (SSP) documents all management, operational, and technical controls for MyUSPTO that are in place, and planned. The SSP is a catalog of all minimum security controls based on NIST SP 800-53 rev.4 and is assessed annually by the USPTO Cybersecurity Division. The SSP is reviewed quarterly through continuous monitoring and when changes occur to the system impacting the implementation of security controls.

   USPTO uses the SDLC and ORR process to ensure that all changes to implemented security controls are analyzed and documented for SOI. During the development or enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the System Security Plan (SSP).

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

   The USPTO has established OCIO-POL-23, "Personally Identifiable Data Removal Policy." Per USPTO policy, the data extra log and verify requirement will be met by the following:

   1. 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.
   2. 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.
   3. Obtain management concurrence in the log, if an extract aged over 90 days is still required.
   4. 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 VPN.
   5. 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.

6. 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.

In addition, the USPTO CIO Command Center (C3) has implemented near-real time monitoring of SOI audit logs. These logs are monitored by authorized C3 personnel.

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

N/A. The USPTO Records Management team has been consulted and a SORN is not required at this time. All of the USPTO Systems of Records Notices can be found at the following address: http://www.uspto.gov/web/doc/privacy_sorn.htm

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

Yes, The OCIO IT Management of Records Policy (OCIO-POL-33) provides the requirements applicable for the creation, maintenance, use, and disposition of all records and other documentary materials in compliance with established Federal Records Management requirements.

The USPTO's Comprehensive Records Schedule is updated every year and lists the NARA-approved record series and dispositions for Agency documents, both from the unique agency schedules and from the federal-wide General Records Schedules.

SIGNATORY AUTHORITY

Agreed: Lyn A Donaldson 4 / 23 / 2015

Lyn Donaldson Date

Information System Owner

Agreed: 02 / 11 / 2015

Bob Simms Date

Information System Owner

Agreed: for 6 / 10 / 15

John Pardun Date

Senior Information Security Officer

Agreed: 6 / 12 / 15

John B. Owens II Date

Authorizing Official