U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment

Patent Search System – Specialized Search (PSS-SS)

PTOP-007-00

July 7 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 PSS-SS is an Application information system, and provides support to the Patent Cost Center. It is considered a mission critical “system”. PSS-SS provides access to highly specialized data that may include annual submissions of nucleic and amino acid sequence or prior-art searching of polynucleotide and polypeptide sequences, other types of information that may be more scientific or technology-based, Patent Linguistic Utility Service (a query by example search system), Chemical Drawing ability, and Foreign Patent Data.

The PSS-SS system is made up of multiple applications that allow Patents examiners and applicants to effectively search the USPTO Patent data repositories. The following section identifies the information subsystems supported by the system or network.

QUESTIONNAIRE

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

   Some patent applications, including ABSS, collect Some Patents applications require Business or Individual Name, Address, Telephone number, Nationality and email address.

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

   To provide a comprehensive prior art search capability and the retrieval of patent and related information for dissemination to the public based on requirements stated in USC statutory code 35 U.S.C. Section 122.

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

   To provide user access to search the USPTO Patent data repositories, which allows Patent Examiners and public users to search and retrieve application data and images, Patents examiners and applicants to identify individuals and organizations with intellectual property, pre-grant, and published applications.

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

   Data repositories allows information to be shared with internal stakeholders (e.g. patent examiners), and to the public.

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?

   There is no opportunity to opt out or consent to particular user of information.

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

Refer to the SSP for all NIST 800-53 controls in place

Management Controls:

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

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 has been created for Patent Application Files and USPTO PKI Registration and Maintenance System.

Source: http://www.uspto.gov/web/doc/privacy_sorn.htm

Application Data Sheet 37 CFR 1.76, PTO/SB/14 (07-07), Approved for use through 06/30/2010. OMB 0651-0032, U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE, http://www.uspto.gov/ebc/portal/efs/sb0014_fill.pdf, http://www.uspto.gov/ebc/portal/privacy.htm, and Certificate Action Form, http://www.uspto.gov/ebc/documents/certificateactionform.pdf

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.

IGNATORY AUTHORITY

Agreed: _____ 5/27/15

William Stryjewski — Date

Information System Owner

Agreed: _____ 6/4/15

John Pardun — Date

Senior Agency Information Security Officer

Agreed: _____ 6/8/15

John B. Owens II — Date

Co-Authorizing Official

Agreed: Margaret A Focarino 6/9/15

Margaret A. Focarino — Date

Co-Authorizing Official