Patent Search System – Specialized Search and Retrieval
(PSS-SS)
Privacy Threshold Analysis /
Privacy Impact Assessment
(PTA/PIA)

Version 1.1
June 10, 2009

Prepared for:
Department of Commerce
United States Patent and Trademark Office
Office of Chief Information Officer
DOC50PAPT0905000

Record of Changes/Version History

PTA-PIA Template Version 6.2
October 1, 2008

Change/Version Number	Date of Change	Sections Changed	Description	Person Entering Change
v1.0	2/10/2008	All	Initial Submission	William Stryjewski
v1.1	6/10/09	All	FY ’09 Annual Assessment	Missing Link Security (MLS) Lisa Youngs

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Threshold Analysis (PTA)

Instructions: Complete the "Privacy Threshold Analysis" section of this document and return it to United States Patent and Trademark Office (USPTO) Senior Privacy Official. If it is determined that a PIA is required as noted in the "Designation" section, the "Privacy Impact Assessment" section will be required to be completed and returned to the USPTO Senior Privacy Official for review and approval.

1. Describe the Patent Search System – Specialized Search and Retrieval (PSS-SS) and its purpose:

The 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.

Furthermore, the PSS-SS system is made up of multiple applications that allow Patents examiners and applicants to effectively search the USPTO Patent data repositories.

2. Status of PSS-SS

☐ This is a new development effort.

☒ This is an existing system.

Date first developed:

Date last updated:

Documented in prior systems and inherited as such. The System was also modified to address version changes in load program.

3. Does the PSS-SS relate exclusively to the network infrastructure? [For example, is the system exclusively a Local Area Network (LAN) or Wide Area Network (WAN)]?

☐ No. Please continue to the next question.

☒ Yes. Is there a log kept of communication traffic?

☐ No. Please continue to the next question.

☒ Yes. What type of data is recorded in the log? (Please choose all that apply.)

☐ Header

☒ Payload

Transaction logs based on user and query type

4. Could the PSS-SS contain information that relates in any way to an individual?

□ No. Please skip ahead to question 5.

☒ Yes. Please provide a general description, below.

The PSS-SS processes, stores, or transmits inventor information, assignee information, attorney/agent information, user information.

5. Does the PSS-SS use or collect Protectable Personally Identifiable Information (PII) [1] or Publicly Releasable PII[2]? (Refer to the USPTO IT Privacy Policy for additional information specific to handling PII.)

□ No.

☒ Yes. Why does the PSS-SS collect PII?

To provide to public notice that these individuals are related to intellectual property

6. What information about individuals could be collected, generated or retained?

Name, business address; including city, state, country

[1] Protectable PII is defined as Information that can be used to uniquely identify (e.g., date of birth, gender, race, social security number, credit card account number, medical information, education information, etc.) contact (e.g., home address, phone number, etc.) or locate an individual (e.g., home or work address, etc).

[2] Publicly Releasable PII is defined as information identifiable to a specific individual that has been authorized for public release. The following information is publicly releasable PII:

- Non-financial information regarding business entities, such as business addresses, telephone numbers, web sites, e-mail; and
- Information available on the USPTO public website such as employee name, identification number, phone number and office location.

Designation

☐ This is NOT a Privacy Sensitive System – the system contains no Personally Identifiable Information.

☒ This IS a Privacy Sensitive System (Check all that apply)

- ☐ PTA sufficient at this time
- ☒ A PIA is required
- ☐ National Security System
- ☐ Legacy System
- ☐ HR System
- ☐ Financial System

I, as the System Owner for PSS-SS concur with the information contained in this Privacy Threshold Analysis.

William Stryjewski Date
System Owner for PSS-SS

I have reviewed this Privacy Threshold Analysis. I recommend that a Privacy Impact Assessment is required.

Rod Turk Date
Senior Agency Information Security Officer for PSS-SS

I have reviewed, and approve this Privacy Threshold Analysis. A Privacy Impact Assessment is required.

John B. Owens II Date
Co-Authorizing Official for PSS-SS

Margaret (Peggy) Focarino
Co-Authorizing Official for PSS-SS

cc: Deputy Chief Information Officer

Privacy Impact Assessment (PIA)

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

Name and residence address of intellectual property owner

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

For data dissemination to public based on requirements stated in USC statutory code 35

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

To identify individuals and organizations with intellectual property

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

Internal stakeholders (e.g. patent examiners), public

5. What opportunities do individuals have to decline to provide information (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 SP 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. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?

Yes, information is maintained in system records.

I, as the System Owner for PSS-SS, concur with the information contained in this Privacy Impact Assessment.

/s/ William Stryjewski 6/22/2009

William Stryjewski, Date
Special Assistant to the Chief Information Officer
System Owner for PSS-SS

I have reviewed this Privacy Impact Assessment, and recommend it be approved.

/s/ Rod Turk 7/20/2009

Rod Turk, Date
Senior Agency Information Security Officer for PSS-SS

I have reviewed, and approve this Privacy Impact Assessment.

/s/ John B. Owens II 7/28/2009

John B. Owens, II Date
Co-Authorizing Official for PSS-SS

/s/ Peggy Focarino 8/6/2009

Margaret (Peggy) Focarino
Co-Authorizing Official for PSS-SS

cc: Deputy Chief Information Officer