U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment

PE2E

PTOP-008-00

November 04, 2013

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 purpose of PE2E is to provide office action processing, workflow management, and role-based administration examination tools for the Patent Examiner's Dockets to track and manage the cases and view documents in text format.

PE2E is used for the following purposes:

1. Provides the Patent Examiners with tools to facilitate the examination of cases and help store, track, and receive case-based knowledge and state information as the examiner accumulates it.
2. Creates a text-based and text-driven patent examination platform.
3. Ensures that the solution provides value to the wider audience of patent examiners.
4. Implements a stable architectural framework using SOA-based principles that allows for the modular addition and modification of well-defined components and services, allowing the system to change as needed over time without significant overhauls.

QUESTIONNAIRE

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

PE2E collects and maintains information from patent applicants (inventors) or their legal representative as part of the patent application submission process. Information from the applicant must be submitted on the patent application form either electronically or in paper copy. PE2E contains information provided as part of the patent application, which includes; full name, address, phone number, email address, and citizenship status of patent applicant (inventor). Additional information is collected for each additional inventory, company, Legal Representative under 35 U.S.C. 117, or Party of Interest under the authority of 35 U.S.C. 118.

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

Information is collected to issue a U.S. patent to the inventor (patent applicant). "This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to .process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14 ."

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

Information is collected to issue a U.S. patent to the inventor (patent applicant).

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

1.) The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2.) A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3.) A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4.) A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5.) A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

6.) A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CPR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

7.) A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

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?

Furnishing of information is voluntary. As part of the patent application process, individuals consent to providing this information for the primary purpose of processing and/or examining the submission related to a patent application or patent. All applicants are notified that this submission is voluntary. However, the USPTO may not be able to process and/or examine the patent application submission.

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

Information is protected in PE2E through a layered security approach which incorporates the use of secure authentication, access control, mandatory configuration settings, firewalls, VPN, and encryption, where required. PE2E adheres to the principles of least privilege, least functionality. In addition, PE2E utilizes secure authentication via username and password credentials.

Management Controls:

1. The USPTO uses the Life Cycle review process to ensure that management controls are in place for the PE2E system. 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 (DRAFT)

Operational Controls:

1. Automated operational controls include securing all hardware associated with the PE2E System 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 data bases. 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 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.

f. 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?

Due to the nature of information shared in PE2E, this is not applicable. At this point, PE2E only houses already published patent data submitted for Re-Examination. If sensitive PII data were to be extracted, the following procedures are in place at USPTO.

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 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.

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: _____ 11/18/14

William Stryjewski — Date

Information System Owner

Agreed: _____ 11/19/14

John Pardun — Date

Senior Agency Information Security Officer

Agreed: _____ 11/24/14

John B. Owens II — Date

Co-Authorizing Official

Agreed: _____ 11/24/14

Margaret Focarino — Date

Co-Authorizing Official