U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE (USPTO)

Privacy Impact Assessment

PCAPS-ES

PTOP-005-00

3/18/2010

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, 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

PCAPS-ES is a Major Application (MA) composed of 14 AISs providing the capabilities and functionality detailed below:

EBCIS

The purpose of the Electronic Business Center Imaging System (EBCIS) is to develop an automated document management system to provide the capabilities of accessing, scanning, indexing, retrieving, and searching documents to users via the PTO Intranet. EBCIS provides the following capabilities:

- Displays the Patent Application Information Retrieval (PAIR) User Manager (PURM) certificate holder name.
- Allows the user to upload the Administrative Certificate Action Form Part A, Part B and Part C forms.
- Allows the user to search by administrator name and number.
- Allows the user to update the name, address, phone number, email address of the administrator.
- Allows the user to add and delete the sponsoring attorneys
- Displays a confirmation message that the sponsoring attorney should be deleted.
- Allows the user to add the registration number associated to the sponsoring attorneys.
- Allows the user to generate the notice letter sent to the administrator.
- Displays the Administrator number column in the Public Key Infrastructure (PKI) New and Recovery reports.
- Keeps a history of the changes made to the certificate record by user ID and timestamp.

  Specifically, the EBCIS AIS includes the following functionalities:

  - Recording incoming documents.
  - Scanning/uploading documents for processing.
  - Providing the capability to view the scanned documents.
  - Editing the code table to update, add, or delete code values and descriptions.
  - Maintaining incoming documents details.
  - The enhanced system will be compliant with Section 508 of the Rehabilitation Act of 1973.

eDAN

The Electronic Desktop Application Navigator (eDAN) is a Graphical User Interface (GUI) application which accesses documents and displays an examiner's docket and corresponding document images. eDAN is a web-based system accessible to patent examiners and managers.

IFW

The Image File Wrapper (IFW) system uses image technology to replace the standard paper processing of patent applications currently used in the Office. The application's paper contents (all documents including the specification, oath or declaration, drawings, information disclosure statements, amendments, Office Actions, and file jacket notations) are scanned into electronic image files, assigned a document code that correlates with the contents of the documents, and indexed into IFW for desktop retrieval. The major IFW functions are:

- ***Capturing*** - IFW is capable of importing documents that have been:
    - Soft-scanned via the Enterprise Application Integration Hub (EAI-Hub)
    - Soft-copied (using existing documents and creating modified versions)
    - Electronically filed via the EAI-Hub
- ***Storage*** - All documents are stored online on EMC. Logically, the documents and data are stored in the Document Archive (jPXI) and Dossier Management System (jDMS).
- ***Distribution*** - Based on data introduced when a document is acquired, e.g. the application number and/or a document code, the system automatically creates and, according to a flexible set of rules, delivers a Message to the Mailbox of a Team or Team Member who will deal with the new document.
- ***Retrieval*** - To simplify navigation through large numbers of documents jDMS creates a Table of Contents (ToC) for every application and collections or procedures within it. The user is able to retrieve documents by selecting an item in the list. Any new documents for action are retrieved automatically.
- ***Viewing*** - The documents can be viewed on screen using a powerful viewer. Most documents are available at sub-second rates through intelligent caching mechanisms.
- ***Printing*** - Extensive print options are offered: printing complete applications or only specific parts; printing with or without annotations; printing single or double sided; and printing on distributed or local printers. Using "overlays," new or modified documents can be created by the user. Different information and control sheets can also be created for printing with the documents.
- ***Exporting*** - External systems or organizations can be provided documents from IFW. Documents may be extracted for further processing outside the system e.g. for publication. These documents are requested from jPXI together with data from the jDMS. All the data is put into output queues (or written onto CD-Rs/DVDs) for collection by the requesting party. The rules for which documents to export, in which format and to which medium are highly flexible.
- ***External Interfaces*** - Interfaces are provided to allow services to be used with minimal modification. These interfaces are available in four key areas:
    - Display of bibliographic data from Legacy systems in the GUI through so called "Status Screens."
    - Logon/security/authentication mechanisms.
    - Distribution, where external algorithms may determine the Mailbox to which Messages should be sent.
    - In the presentation framework where the USPTO may develop and plug-in its own java applications.

OACS

The Office Action Correspondence Subsystem (OACS) serves as a central word processing system tool used to cite prior art references. OACS provides the following capabilities:

- The creation, modification, review, approval, and routing of Red Folders within OACS.
- The support of multiple levels of the Red Folder review, approval, and rejection.
- The import of externally generated Portable Document File (PDF) documents and associated metadata into the Red Folders.
- The user provision of metadata for imported documents, where metadata is missing or incomplete.

- The automatic indication of document mailing status based on the document code.
- The central storage of the Red Folder documents and data.
- The automatic control of the Red Folder document access, modification, and deletion privileges.
- The tracking of all Red Folder life cycle status changes.
- The on-demand provision of current and historical statuses, based on user privilege.
- The application of electronic signatures and initials to the individual OACS documents.
- The preparation and printing of mail ready Red Folders to support the existing mail process.
- The preparation and actuation of the scan ready Red Folders to support the existing soft scan process.

OPBudget

The Patent Modeling and Budget Administration System (OPBudget) is a Decision Support System (DSS) that provides automated support and controls to the Office of Patent Resources Administration (OPRA) to formulate estimated budgets for the USPTO, monitors Congressionally-approved budgets, and projects the revenue of the patent process.

PALM EXPO

The Patent Application and Location Monitoring (PALM) Examination and Post-Examination (EXPO) subsystem deals with tracking patent application prosecution, publication, the physical location of application, GAU, examiner productivity, patent issuance, quality review, file inventory, and lost file reconstruction. It also supports the production of reports related to examination and publication processes. PALM EXPO interfaces with Revenue Accounting and Management (RAM), Pentent Application Security System (PASS), and Image File Wrapper (IFW) in addition to other PALM subsystems. PALM EXPO also provides external services for PASS, IFW, Patent Enterprise Access Integration (PEAI), and Electronic Desktop Application Navigator (eDAN) to enable these AISs to access PALM data.

PALM FOS

The File Ordering System (FOS) tracks the physical location and status of issued or abandoned patents, as well as registered or abandoned Trademark files. The enhanced FOS functions replace all of the existing FOS subsystem functionality, including single and multiple FOS subsystem capabilities. FOS replaces file repository operations, including the printing of file orders, enhances the user interface, and provides interfaces with other USPTO systems such as ClearPath, the Infrastructure subsystem, Pre-Exam, Examination and Post-Examination (EXPO), the OEMS, and the File Tracking System (FTS).

The PALM FOS is part of the migration effort of the existing PALM system from the ClearPath mainframe environment to open system architecture. The FOS component provides the following, high-level, file ordering, business activities:

- Ordering a patent or trademark case file from the USPTO File Repositories by PTO employees and from either the File Information Unit (FIU) or the Trademark Search Library (TSL) by the public.
- Receiving and dispatching a case file to and from the FIU, TSL, PTO File Repositories, predetermined PTO central locations, and PTO employee locations.
- Conducting file repository operations, such as printing file orders, receipt, and dispatch.

FOS provides the functionality to manage the creation and modification of physical object data, which includes:

- Managing the type and barcode of the physical object along with what Patent or Trademark application to which the physical object is assigned.

- Tracking the location and lost file status of the physical object.
- All functions related to file order requests and the processing of the requests at the Patent or Trademark Repositories.

PALM INFRA

The Patent Application and Location Monitoring Infrastructure (PALM) subsystem supports the management of basic information and contact details about the USPTO (its organizational structure, workers, and physical locations – including special purpose locations such as search rooms and how they interact with each other). The PALM INFRA subsystem provides:

- Web-based, online query functionality
- Employee Locator, Universal Resource Locator (URL) = 'PALM' on the Intranet
- Report(s) generation capability
- Data download capability to support the production of telephone directories
- Move (relocation) planning support
- Search Room Relocation planning support

PEAI FIU

The Patent Enterprise Access Integration – File Inspection Utility (PEAI FIU) provides an internal web based application used by examiners to review (read-only) patent applications data published and unpublished. PEAI FIU is accessible to internal patent examiners only on the USPTO Network (PTONet). PEAI FIU utilizes the PTONet Websphere portal to allow internal PTONet access to authorized users, who are authenticated with MS Active Directory through LDAP authentication. The data accessed via PEAI FIU is the same data as PEAI Public PAIR and PEAI Private PAIR. PEAI FIU provides a USPTO internal only access to patent examiners.

PEAI Private PAIR

The PAIR Private allows restricted Internet access to patent application status to patent applicants and/or their designated legal representative(s) without compromising the confidentiality or security of applicants' data. PEAI Private PAIR requires all users to be registered and to be issued an x.509 digital certificate by USPTO. Digital certificates are managed in the PURM. The x.509 digital certificate issued to the customer performs access control for PEAI Private PAIR.

PEAI Public PAIR

The Patent Enterprise Access Integration (PEAI) Public PAIR allows public access to published patent applications and additional information regarding published patents. PEAI Public PAIR provides a web based interface for the public at large to access published patent applicants. This data has been publicly released and is accessible to everyone in read-only format.\

PEAI TDA

The Trilateral Document Access System supports the trilateral partners, the United States Patent and Trademark Office (USPTO), the European Patent Office (EPO), and the Japan Patent Office (JPO), in the electronic exchange of intellectual property documents. It encompasses the subsystems, File Wrapper Access (FWA) and Priority Document Exchange (PDX). FWA enables the real-time exchange of patent documents images among the participating Intellectual Property (IP) offices. PDX enables the exchange of priority documents (PDs) electronically among the participating IP offices.

TDA interfaces with Patent Application Location and Monitoring (PALM) Expo, electronic Desktop Application Navigator (eDAN) and Enterprise Application Integration (EAI) Hub to retrieve, update and store information and content relating to a patent application.

QRS

The Quality Review System (QRS) provides a web-based interface to the reviewers to view the patent applications in order to review, evaluate and create reports for the examiners work. QRS (formerly called as Patent Quality Review System (PQRS)) provides interfaces for the Technology Centers (TCs) and Office of Patent Quality Assurance (OPQA) personnel to enter data on Allowed Reviews, In Process Reviews (IPRs), New Application Reviews, Amendment Reviews, and New Examiner Reviews. QRS provides the following functionality to authorized users.

QRS functionality includes the following:

- Import of patent cases from PALM system
- Review of patent cases
- Track reviewer production
- Communication between offices
- Report generation - Provides tailored reporting capabilities based on user roles
- System administration and configuration
- Review data captured and updated through review forms
- Dockets with personalized functionalities based on user roles
- Selection and import of patent cases from PALM based on predefined criteria
- Allows users to set and track fiscal year review goals for reviewers
- Allows users to log all actions taken to resolve errors found in cases
- Allows users to set fiscal year review goals for examiners
- Allows administrators to manage user interaction through role-based functionality

The purpose of this system is to support the USPTO Patent Office by storing patent applications and related metadata in electronic form, processing applications electronically, reporting patent application processing and prosecution status, and retrieving and displaying patent applications. PCAPS-ES supports the lifecycle processing and day to day processing of Patent applications by USPTO Patent examiners.

SCORE

The Supplemental Complex Repository for Examiners (SCORE) provides a non-image repository that allows examiners access to unpublished mega content associated with a patent application. Mega content will typically include the following: Sequence Listings, Mega Tables, Search Results, Computer Program Listings, Design drawings, Protein Crystals, Mathematical formula, Chemical Formula, Yellow Book, Red Book, Fep and Unclassified. SCORE has the capabilities to:

- Provide customers with an interface to render Bio-Sequence Listings in the proper format.
- Provide examiners with enhanced access to all Pending, Published, and Issued sequence data, thus allowing the eDAN user retrieval of sequence data in text format, without unnecessary duplication of data in the IFW.

- Create a certified Enterprise Resource Management (ERM) system that hosts part of the official record of patent documents.
- Create an internal and secure component that will host and render all pending mega data, relieving the IFW of the burden of scanning and rendering thousands to millions of pages of tables, drawings, and listings.
- Create a repository to store general non-image data, such as three-dimensional protein crystal tables, chemical drawings, mathematical equations, computer source code, other format files as needed, and any mega data that is submitted (to be implemented in a future phase).
- Automate the process of loading and exporting large content.

QUESTIONNAIRE

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

PCAPS-ES collects 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. PCAPS-ES 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.

Source: 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 http://www.uspto.gov/ebc/documents/certificateactionform.pdf

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 ."

Source: 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 http://www.uspto.gov/ebc/documents/certificateactionform.pdf

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). Once the application is published the patent is released to the public, unless otherwise requested by the patent applicant at the time of submission. This information is also used to construct a unique name (distinguished name) and to communicate with user about the certificate grant and software distribution process.

Source: 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

4. With whom will the information be shared (e.g., another agency for a specified programmatic purpose)?
Information collected remains confidential until the patent application is published. Once published, information is publicly released. Information may be shared with the following:

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 related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6.) A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7.) 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.

8.) 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 CFR 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.

9.) 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.

Source: 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

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.

Source: 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

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

Information is protected in PCAPS-ES through a layered security approach which incorporates the use of secure authentication, access control, mandatory configuration settings, firewalls, VPN, and encryption, where required. PCAPS-ES adheres to the principles of least privilege, least functionality. In addition, PCAPS-ES utilizes secure authentication via username and password credentials. Electronic patent application (e-filer) transmissions from patent applicants are encrypted via a secure HTTPS (SSL/TLS) and Public Key Infrastructure (PKI) x.509 digital certificates. Digital certificates are utilized to authenticate patent applicants or their legal representatives, where required for access to PCAPS-ES information.

Management Controls:

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

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 the extract was done,
c. What was the extract,
d. Where the extract was 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 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 and

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 AUTHORIES

	/s/ William Stryjewski	3/30/2010
Agreed:	_____	_____/_____/_____
	William Stryjewski	Date
	Information System Owner	
	/s/ Rod Turk	4/8/2010
Agreed:	_____	_____/_____/_____
	Rod Turk	Date
	Senior Agency Information Officer	
	/s/ John B. Owens II	4/26/2010
Agreed:	_____	_____/_____/_____
	John B. Owens II	Date
	Chief Information Officer/ Co-Authorizing Official	
	/s/ Robert L. Stoll	4/30/2010
Agreed:	_____	_____/_____/_____
	Robert L. Stoll	Date
	Commissioner for Patents/ Co-Authorizing Official	