U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment

Revenue Accounting and Management System (RAM)

PTOC-006-00

May 13, 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

Revenue Accounting and Management System (RAM) is a Major Application (MA) that collects fees for various USPTO goods and services related to intellectual property and the protection of intellectual property rights. Internet customers can pay these fees by credit card, Electronic Funds Transfer (EFT), or by a USPTO established Deposit Account via the RAM Payment Server. The Payment Server is a secure web server that allows the customer to interface with and pay for their fees using the Internet. Fees submitted by mail are processed through the "Core" RAM application by designated USPTO staff. The RAM information will only be shared with Pay.gov for credit card and ACH verification and processing.

RAM is an application developed and maintained by USPTO, which is composed of two pieces:
a client-server application that is only accessible via the internal USPTO network. The application is accessed by the staff that supports the Office of Finance to conduct day-today business processing. The second component of RAM is a web-based portion available to the public with access to the Internet. RAM provides the following functions:

- Process Receipts
- Point-of-Sale Processing
- Process Maintenance Fees
- Process Refunds
- Process Subscriptions
- Pass Fees to the World Intellectual Property Organization (WIPO), the European Patent Organization (EPO) and the Korea Intellectual Property Office (KIPO)
- Maintain Deposit Account
- Management Reporting
- Access Control Management:

The Office of Finance Imaging System (OFIS) is a web-based application that is used to enable the refund-processing workflow. It is designed to improve the efficiency of the business process for the Office of Finance by scanning the Fee payment document and associate it in OFIS, with the fee payment recorded in the RAM database and providing the capability to view the scanned documents. OFIS had interfaces with PALM, RAM, PTAS and TRAM to retrieve information about current application file location, status, bibliographic data and fee information. OFIS will use the CIDM services for managing documents.

OFIS provides the Office of Finance staff with the following capabilities for Refund Request tracking:

- Record incoming Refund Requests
- Record approved or denied status of the Refund Requests
- Scan/Upload documents for processing
- Provide the capability to view the scanned documents
- Interface with the Patent Application Location and Monitoring (PALM) database for bibliographic data
- Interface with the Trademark Reporting and Application Monitoring (TRAM) database for bibliographic data

- Provide access to the Revenue Accounting and Management (RAM) system for fee information
- Produce statistical and outline logs of Program Area reports for management
- Generate outgoing correspondence
- Store edited correspondence addresses in the OFIS database
- Maintain Program Area point of contact information for routing purposes
- Edit Code Table to update, add, or delete code values and descriptions
- Maintain Refund Request to maintain refund request details
- Refine the response correspondence design
- Receive, store, and index Patent and Trademark Assignment System (PTAS) credit card authorization documents in standard manner
- Standardize automated reports by accepting new office codes
- Scan the Fees payment document and associate it in OFIS, with the Fee payment recorded in the RAM database
- Produce Discrepancy Report for closed refund transactions
- Generate Operator productivity reports
- Generate a report of response time to satisfy refund request

QUESTIONNAIRE

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

   The Revenue Accounting and Management (RAM) system collects, but does not store credit card security codes. Information collected from the public includes that under OMB collection number 0651-0043, Payment of PTO Fees by Credit Card. RAM collects fees for various USPTO goods and services related to intellectual property and the protection of intellectual property rights. Public customers can pay these fees over the internet by credit card, Electronic Funds Transfer (EFT), or by a USPTO established Deposit Account through a secure HTTPS connection. For credit card payments, the cardholder's name, address, credit card type (Visa, MasterCard, Discover, or American Express), credit card number, credit card security code, and credit card expiration date are collected. Customers paying fees using electronic funds transfer must sign up for an account (one-time process).
   During the self-service registration process, RAM collects the bank account holder's name, address, bank name, bank routing code, bank account number, bank account type and classification (savings/checking and business/personal) contact phone number, and contact email address. For future fee payments once an EFT profile account is established, the customer only enters their EFT ID and password. For Deposit Account payments, the Deposit Account number, and the name of the Authorized Deposit Account User are collected. Customers not using the Internet for payment processing of their goods and services can send in payment information in paper form via USPS mail or commercial courier or in person at the USPTO. USPTO employees using the RAM application via client workstations manage the manual processing of these fee payments. These employees provide their name, work telephone number, work fax number, work organization name, office location, work email address, and workstation ID and proof of training in order to establish a RAM account. Each transaction processed in RAM by a USPTO employee (fee processor) has their RAM ID associated with it for auditing, archival, and research purposes.

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

   The USPTO collects customer financial information for fee processing. Under 35 U.S.C, Section 41 and 15 U.S.C. Section 11 13, as implemented in 37 CFR, the USPTO charges fees for processing and services related to patents, trademarks, and information products. In the case of EFT payments, we collect the contact phone number and contact email address in order to communicate with the customer in case there are any problems with the EFT information or the EFT feesale. All employee information is collected in order to identify the RAM fee processor and organization in which they work. The RAM system is set up with role-based privileges, so an employee only has access to those specific functions permitted within their organization or by their required duties.

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

   The customer financial information is used to validate and process the fee sales. After a sale is completed, the information is stored as a historical transaction along with the identifying mark of the sale item. This historical sale information is used to verify a customer has paid the appropriate fees for their goods or services. For EFT payments, the contact phone number and contact email address are used in order to communicate with the customer in case there are any problems with the EFT information or the EFT fee sale. The employee information is used to identify and contact the RAM fee processor or to identify a specific transaction performed by a specific RAM operator. For example, a RAM operator in Trademarks would not have access to process Patent fees, and a RAM fee processor would have fewer privileges than a RAM supervisor role.

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

   Information about customers' credit card transactions are sent to (the U.S. Treasury's) Pay.gov system for authorization (real-time) and settlement (same day) and customers' banking information is sent to the Pay.gov system (daily batch- not real-time) for pre-notifications (new account verification-zero dollar transaction) and for EFT processing. Employee information is not shared with any other system or agency.

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?

   All financial information for payment processing described herein is required to obtain services related to intellectual property and the protection of intellectual property rights. All employee information for identifying and assigning RAM operator accounts described herein is required. Customers do have payment options, so they have the opportunity to decline the provision of credit card information if they would rather use a deposit account or a check. Also, there is no additional use of the information beyond the required use and therefore no "consent process" is necessary.

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

   Management Controls:

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

   Operational Controls:

   1. Automated operational controls include securing all hardware associated with RAM 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 offsite. 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 are 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 a 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.

Technical Controls:
RAM is secured by the USPTO's infrastructure systems and other OCIO established technical controls to include password authentication at the server and database levels.

In supporting fee collection via Internet Web storefronts, RAM uses a secure, three-tiered architecture. When a fee payment is required, users are redirected to a Secure Hypertext Transfer Protocol (HTTPS) URL from their specific AIS storefront Web pages. After requesting a purchase transaction, the client's web browser is redirected to the load balanced edge servers located in the USPTO Sensitive DMZ. Then the requests are directed to RAMPS servers located in PTONet that sit behind intrusion detection and prevention appliances. The RAMPS Web pages access Java Server Pages (JSPs) on RAMPS to handle user interface and access functionality on the RAM database server on PTOnet. HTTPS is used for all data transmissions to and from the Internet, USPTO DMZ, and PTOnet. A dedicated Secure Sockets Layer (SSL) Accelerator is used to perform SSL encryption and decryption.

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

   USPTO implements the following practices to protect PII data:
   No extracts of sensitive data may be copied onto 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.
   All laptop computers allowed to store sensitive data must have full disk encryption.
   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. 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?

   No, there is no new system of records being created. Existing systems of records cover the information residing in the data base. This includes the COMMERCE/PAT-TM-10 Patent Deposit Accounts System.

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:

Gita Zoks — 5/21/15

Gita Zoks — Date

Information System Owner

Agreed: — 5/22/2015

John Pardun — Date

Senior Information Security Officer

Agreed: — 5/27/15

Tony Chiles for John B. Owens II — Date

Chief Information Officer

Co-Authorizing Official

Agreed: — 5/29/15

Anthony Scardino — Date

Chief Financial Officer

Co-Authorizing Official