USPTO Privacy Impact Assessment Statement

Revenue Accounting and Management System (RAM)

Unique Investment Identifier: 006510101018002003071117

Prepared by: Heidi Sibayton, Corporate Systems Division, Executive for Systems Development and Maintenance Services, OCIO

Reviewed by: David J. Freeland, Chief Information Officer

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

Information collected from the public includes that under OMB collection number 0651-0043, Payment of PTO Fees by Credit Card.

The Revenue Accounting and Management (RAM) system 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.

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.

For EFT payments, the bank holder's name, address, bank name, bank routing code, bank account number, contact phone number, and contact email address are collected.

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 as part of identifying them as a RAM operator.

2. Why is the 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 1113, 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 fee sale.

All employee information is collected in order to identify the RAM operator 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 the 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 operator 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 operator would have fewer privileges than a RAM supervisor role.

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

The credit card information is sent to Vital Processing, our credit card processor, for credit card verification and processing. The EFT information is sent to Mellon Bank, our merchant bank, for EFT verification and processing. The 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 individuals can 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:

RAM system operators and administrators are trained to keep financial information secure. RAM operator (employee) information is only available to the RAM administrators.

Operational Controls:
The information is managed by key personnel having role-based permissions to view and manage this data.

Data Center/Access Controls:
The RAM production servers and storage are secured in the USPTO's Data Center Facility which has a 24x7x365 guard presence. In addition, access to the Data Center Facility is limited to authorized personnel and requires an access card with appropriate levels of security to gain entry to the facility.

Technical Controls:
The RAM Payment Server (RAMPS) uses Secure Sockets Layer (SSL) encryption between the client browser and the Payment Server to collect financial information from the customer. The information is then relayed to the core RAM server (RAMPROD2) for payment processing and storage. RAMPS is not directly accessible from the Internet, but instead, all transactions must pass through the SSL Accelerator.

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 RAM Payment Server (RAMPS) located in the USPTO DMZ security zone. The RAMPS Web pages access Java Server Pages (JSPs) on RAMPS to handle user interface and access functionality on the RAMPROD2 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. 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 database. This includes the COMMERCE/PAT-TM-10 Patent Deposit Accounts System.

UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

Revenue Accounting and Management System (RAM) UII: 006510101018002003071 17

/s/
Robert Cobert for 4/12/2006

Prepared by
Heidi Sibayton Date

/s/
Joyce English 4-12-06

Approved Date
Joyce English
Director, Systems Development and Maintenance

I have reviewed and approve the attached Privacy Impact Assessment document(s).

/s/
David J. Freeland 6/29/06

David J. Freeland Date
Chief Information Officer

cc:
Griffin Macy, Deputy Chief Information Officer
David Larsen, Acting Director, Enterprise IT and Security Management