U.S. PATENT AND TRADEMARK OFFICE

Revenue Accounting and Management System

(RAM)

Unique Investment Identifier: 006510101018002003071 17

USPTO Privacy Impact Assessment Statement

Prepared by: Brooks Hunt, Director, Office of Technical Plans and Policy
Reviewed by: Ron Hack, Acting Chief Information Officer

U.S. Patent and Trademark Office

USPTO Office of the Chief Information Officer (OCIO)

Privacy Impact Assessment (PIA)

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

The Revenue Accounting and Management (RAM) system collects fees for various USPTO goods and services and to obtain or retain benefits. 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, 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 person or in paper form via the mail. 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. RAM transactions are tied to the RAM operator performing the transaction for auditing purposes. This information is also used to identify which roles to assign the employee. 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 Deposit Account information is sent to Bank One, where our lockbox account is managed, for Deposit Account payment 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 and benefits. 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)?

The RAM Payment Server uses Secure Sockets Layer (SSL) encryption between the client browser and the Payment Server to collect financial information from the customer and relay this to the core RAM server for payment processing and storage. Once a payment is processed, the financial information is stored in RAM's own Oracle database. The core RAM server is managed by key personnel having role-based permissions to view and manage this data. The system is designed so there are

only a few key users that can view the complete credit card and banking information. RAM system operators and administrators are trained to keep financial information secure. RAM operator (employee) information is only available to the RAM administrators.

7) Is a system of records being created under the Privacy Act, 5 U.S.C. 552a.?

Yes. The RAM Oracle database stores the customer financial information as part of the historical record of the financial transactions. RAM operators can retrieve historical transaction information, based on credit card number, bank account information, or Deposit Account number for verification of payment processing.

The employee information is also stored in the RAM Oracle database and is retrievable by the RAM administrators by way of their RAM operator id to identify the RAM operators.