

**U.S. Department of Commerce
U.S. Patent and Trademark Office**



**Privacy Impact Assessment
for the
Revenue Accounting and Management System (RAM)**

Reviewed by: John B. Owens II, Senior Agency Official for Privacy

- Concurrence of Senior Agency Official for Privacy
- Non-concurrence of Senior Agency Official for Privacy

Signature of Senior Agency Official for Privacy

Date

U.S. Department of Commerce Privacy Impact Assessment USPTO Revenue Accounting and Management System

Unique Project Identifier: PTOC-006-00

Introduction: System Description

Provide a description of the system that addresses the following elements:

(a) a general description of the information in the system

The RAM Master system is composed of 2 AIS's:

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.

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

(b) a description of a typical transaction conducted on the system

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 Customer Deposit Account

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 customer financial 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
- Store edited correspondence addresses in the OFIS database
- Maintain Program Area point of contact information for routing purposes
- Maintain Refund Request to maintain refund request details
- Receive, store, and index Patent and Trademark Assignment System (PTAS) credit card authorization documents in standard manner
- 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

(c) any information sharing conducted by the system

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.

(d) a citation of the legal authority to collect PII and/or BII

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

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system

Moderate

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- This is a new information system.
- This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>	g. New Interagency Uses	<input type="checkbox"/>
b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input type="checkbox"/>	h. Internal Flow or Collection	<input type="checkbox"/>
c. Significant System Management Changes	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character of Data	<input type="checkbox"/>
j. Other changes that create new privacy risks (specify):					

- This is an existing information system in which changes do not create new privacy risks. Continue to answer questions, and complete certification.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (Check all that apply.)

Identifying Numbers (IN)					
a. Social Security*	<input type="checkbox"/>	e. File/Case ID	<input type="checkbox"/>	i. Credit Card	<input checked="" type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input checked="" type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input checked="" type="checkbox"/>
d. Employee ID	<input type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					
*If SSNs are collected, stored, or processed by the system, please explain if there is a way to avoid such collection in the future and how this could be accomplished:					

General Personal Data (GPD)					
a. Name	<input checked="" type="checkbox"/>	g. Date of Birth	<input type="checkbox"/>	m. Religion	<input type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	h. Place of Birth	<input type="checkbox"/>	n. Financial Information	<input checked="" type="checkbox"/>
c. Alias	<input type="checkbox"/>	i. Home Address	<input checked="" type="checkbox"/>	o. Medical Information	<input type="checkbox"/>
d. Gender	<input type="checkbox"/>	j. Telephone Number	<input checked="" type="checkbox"/>	p. Military Service	<input type="checkbox"/>
e. Age	<input type="checkbox"/>	k. Email Address	<input checked="" type="checkbox"/>	q. Physical Characteristics	<input type="checkbox"/>
f. Race/Ethnicity	<input type="checkbox"/>	l. Education	<input type="checkbox"/>	r. Mother's Maiden Name	<input type="checkbox"/>

s. Other general personal data (specify):

Work-Related Data (WRD)					
a. Occupation	<input type="checkbox"/>	d. Telephone Number	<input type="checkbox"/>	g. Salary	<input type="checkbox"/>
b. Job Title	<input type="checkbox"/>	e. Email Address	<input type="checkbox"/>	h. Work History	<input type="checkbox"/>
c. Work Address	<input type="checkbox"/>	f. Business Associates	<input type="checkbox"/>		
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	<input type="checkbox"/>	d. Photographs	<input type="checkbox"/>	g. DNA Profiles	<input type="checkbox"/>
b. Palm Prints	<input type="checkbox"/>	e. Scars, Marks, Tattoos	<input type="checkbox"/>	h. Retina/Iris Scans	<input type="checkbox"/>
c. Voice Recording/Signatures	<input type="checkbox"/>	f. Vascular Scan	<input type="checkbox"/>	i. Dental Profile	<input checked="" type="checkbox"/>
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>	e. ID Files Accessed	<input type="checkbox"/>
b. IP Address	<input type="checkbox"/>	d. Queries Run	<input type="checkbox"/>	f. Contents of Files	<input type="checkbox"/>
g. Other system administration/audit data (specify):					

Other Information (specify)					

2.2 Indicate sources of the PII/BII in the system. (Check all that apply.)

Directly from Individual about Whom the Information Pertains					
In Person	<input checked="" type="checkbox"/>	Hard Copy: Mail/Fax	<input checked="" type="checkbox"/>	Online	<input checked="" type="checkbox"/>
Telephone	<input checked="" type="checkbox"/>	Email	<input checked="" type="checkbox"/>		
Other (specify):					

Government Sources					
Within the Bureau	<input type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		
Other (specify):					

Non-government Sources					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input type="checkbox"/>		
Other (specify):					

- 2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
-------------------------------------	--

Section 3: System Supported Activities

- 3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	There are not any IT system supported activities which raise privacy risks/concerns.
-------------------------------------	--

Section 4: Purpose of the System

- 4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility	<input type="checkbox"/>	For administering human resources programs	<input type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input type="checkbox"/>
For litigation	<input type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>
For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input type="checkbox"/>	For employee or customer satisfaction	<input type="checkbox"/>
For web measurement and customization technologies (single-session)	<input type="checkbox"/>	For web measurement and customization technologies (multi-session)	<input type="checkbox"/>
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

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 fee sale. Any employee/contractor 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.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. (Check all that apply.)

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private sector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input checked="" type="checkbox"/>	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: U.S. Treasury/Pay.gov
<input type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to

process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. (*Check all that apply.*)

Class of Users			
General Public	<input checked="" type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. (*Check all that apply.*)

<input type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input type="checkbox"/>	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: _____.	
<input type="checkbox"/>	Yes, notice is provided by other means.	Specify how:
<input checked="" type="checkbox"/>	No, notice is not provided.	Specify why not: 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.

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: 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.
<input type="checkbox"/>	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

<input type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an	Specify why not: There is no additional use of the information

	opportunity to consent to particular uses of their PII/BII.	beyond the required use and therefore no "consent process" is necessary.
--	---	--

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Customers have the opportunity to update account information at any time.
<input type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. (*Check all that apply.*)

<input checked="" type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: 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.
<input checked="" type="checkbox"/>	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>June 2015</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input checked="" type="checkbox"/>	Contracts with customers establish ownership rights over data including PII/BII.
<input checked="" type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input type="checkbox"/>	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

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.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C.

§ 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

<input type="checkbox"/>	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i> :
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input checked="" type="checkbox"/>	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

<input type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule:
<input type="checkbox"/>	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	<input type="checkbox"/>	Overwriting	<input type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

<input type="checkbox"/>	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input checked="" type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels.
(Check all that apply.)

<input type="checkbox"/>	Identifiability	Provide explanation:
<input type="checkbox"/>	Quantity of PII	Provide explanation:
<input type="checkbox"/>	Data Field Sensitivity	Provide explanation:
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: USPTO charges fees for processing and services related to patents, trademarks, and information products. PII is collected in order to communicate with the customer in case there are any problems with fee sale or to identify the RAM fee processor and organization.
<input type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation:
<input type="checkbox"/>	Access to and Location of PII	Provide explanation:
<input type="checkbox"/>	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required business process changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required technology changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.