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

Privacy Threshold Analysis
for the
Revenue Accounting and Management System (RAM)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Revenue Accounting and Management System

Unique Project Identifier: PTOC-006-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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.

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.

Questionnaire:

1. What is the status of this information system?

    ____ This is a new information system. *Continue to answer questions and complete certification.*

    ____ This is an existing information system with changes that create new privacy risks.
    Complete chart below, continue to answer questions, and complete certification.

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

    ____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

    _x_ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?
   NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

    _x_ Yes. RAM 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. These activities require the use of PII to complete the fee collection.

    ____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

__x__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

    __x__ Companies
    __x__ Other business entities

_____ No, this IT system does not collect any BII.

4. Personally Identifiable Information
4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__x__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

    _____ DOC employees
    _____ Contractors working on behalf of DOC
    __x__ Members of the public

_____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__x__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

_____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

__x__ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__x__   I certify the criteria implied by one or more of the questions above **apply** to the Revenue Accounting and Management System and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____   I certify the criteria implied by the questions above **do not apply** to the Revenue Accounting and Management System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): _____Gita Zoks_____

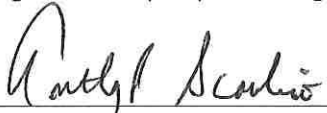Signature of ISSO or SO: _____[signature]_____ Date: _5/22/2018_

Name of Senior Information Security Officer (SISO): ___Rami Dillon_____

Signature of SISO: _____[signature]_____ Date: _5/24/18_

Name of Authorizing Official (AO) & Bureau Chief Privacy Officer (BCPO): _David Chiles_

Signature of AO & BCPO: _____[signature]_____ Date: _6/15/2018_

Name of Authorizing Official (AO) or Designated Representative: ____Anthony Scardino____

Signature of AO: _____[signature]_____ Date: _6/26/18_