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

Privacy Threshold Analysis
for the
Financial Budget and Planning Systems (FBPS)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Financial Budget and Planning Systems (FBPS)

Unique Project Identifier: PTOC-030-00

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 Senior Agency Official for Privacy (SAOP).

Description of the information system and its purpose: *Provide a general description of the information system and its purpose 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).

The Financial Budget and Planning System (FBPS) is a Master System comprised of five (5) subsystems: 1) Corporate Planning Tool (CPT), 2) Activity Based Information System (ABIS), 3) Transit Subsidy System (TSS), (4) Automated Fee Forecasting (AFF) and 5) Financial Enterprise Data Management Tools (FEDMT). FBPS is located at the USPTO Data Center in Alexandria, Virginia.

Corporate Planning Tool (CPT)

CPT improves the efficiency and effectiveness of the business processes for which the USPTO Office of Planning and Budget (OPB), Financial Resources Management Division (FRMD) of OCIO, and Office of Financial Management Systems (OFMS) are responsible. CPT is a COTS product and possesses the ability to integrate and streamline the USPTO's execution, compensation projection and performance processes. In addition, the tool serves as an improved means of gathering, analyzing, and reporting pertinent information.

CPT leverages information from all OPB, FRMD OCIO and OFMS processes but focuses primarily on the budget execution and compensation projection processes. With COTS software, OPB, FRMD OCIO and OFMS are able to create a consistent process for generating, consolidating, and reporting information. Information can be reviewed and approved by the appropriate OPB, FRMD OCIO, and OFMS staff and then be shared among all OPB, FRMD OCIO and OFMS staff as well as the USPTO program areas. CPT also allows OPB, FRMD OCIO, and OFMS staff to store and retrieve historical information.

Activity Based Information System (ABIS)

ABIS utilizes a COTS product, SAP's Profitability and Cost Management (PCM), to streamline and automate business processes. The system capabilities include: 1) develop, update and maintain the Activity Based Costing (ABC) models, 2) assist in preparing quarterly reports and briefings which are utilized to communicate with Program Managers and Executives in USPTO; 3) assist in preparing quarterly Statement of Net Cost and supporting notes, and 4) provide cost input and analysis for the Annual Performance and Accountability Report perform ad hoc cost studies on proposed fee legislation, OMB and Congressional inquiries and internal management requests. ABIS does not contain PII.

Transit Subsidy System (TSS)

TSS is a web-based application for USPTO employees in Alexandria VA, and satellite regions (Detroit, Denver, Dallas/Ft. Worth, and Silicon Valley) to submit requests for transit subsidy via the intranet and a database to store transit subsidy program data for operations, inventory, reporting, and audit purposes. The Office of Finance administers the transit subsidy program. TSS supports the application for both SmarTrip/SmartBenefits and TranBen Vouchers. SmarTrip/SmartBenefits is the preferred fare media for use in the Washington Metropolitan Area Transit Authority (WMATA) system. TranBen Vouchers are a paper fare media used in the Washington Metropolitan Area Transit Authority (WMATA) system in the case of new employees and claim of non-receipt of electronic fare media, and is the fare media distributed in all satellite regions.

Automated Fee Forecasting (AFF)

AFF improves and supports the analysis of fee collection information and decision-making by providing the ability to load, manipulate, query, model, analyze, and report fee collections and forecasting data as needed. In addition, it simplifies, standardizes, and adds visibility to the performance measurement process. The purpose of the system is to address identified business problems and risks associated with the current manually intensive processes through automation. AFF does not contain PII.

Financial Enterprise Data Management Tools (FEDMT)

FEDMT is a web-based application to support administrative staff in the Office of Finance to store and manage reference data. The first database within FEDMT is the Program, Project, and Activity (PPA) Code database, which will be used by the Activity Based Information Division to enter, manage and approve PPA codes. From this managed source, extracts will be available for routing to the Momentum financial system for transactional usage and the Enterprise Data Warehouse for reporting purposes. The system will have a small number of data entry and approver personnel in ABI and the OCIO FRMD office. FEDMT does not contain PII.

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.*

☒ This is an existing information system in which changes do not create new privacy risks. *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):					

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.

☐ Yes. *Please describe the activities which may raise privacy concerns.*

☒ 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.).”

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

☐ Companies

☐ 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...”

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

☒ DOC employees

☒ Contractors working on behalf of DOC

☐ 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?

☒ 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.

☐ 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

☒ I certify the criteria implied by one or more of the questions above **apply** to the Financial Budget and Planning 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 Financial Budget and Planning 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 SO: Gita Zoks Date: 5/8/17

Name of Senior Information Security Officer (SISO): Rami Dillon

Signature of SISO: Date: 5/10/17

Name of Authorizing Official (AO) & Bureau Chief Privacy Officer (BCPO): John B. Owens II

Signature of AO & BCPO: Date: 5/11/17

Name of Authorizing Official (AO) or Designated Representative: Frank Murphy

Signature of AO: Frank Murphy Date: 05/10/2017