

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



**Privacy Impact Assessment
for the
Planning and Budgeting Products (PBP)**

Reviewed by: David Chiles, Bureau Chief Privacy Officer (Acting)

- ☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

for Dr. Catrina D. Purvis	LISA MARTIN Digitally signed by LISA MARTIN Date: 2019.06.14 15:45:41 -04'00'	06/14/2019
Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer		Date

U.S. Department of Commerce Privacy Impact Assessment USPTO (PBP)

Unique Project Identifier: PTOC-030-00

Introduction: System Description

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

The response must be written in plain language and be as comprehensive as necessary to describe the system.

[Guidance: When completing this section, be sure to include only information suitable for public viewing since this is to be posted online. Do not include system information such as IP addresses, architecture diagrams, et.]

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

PBP is a Master System composed of the following four (4) subsystems: 1) Corporate Planning Tool (CPT), 2) Activity Based Information System (ABIS), 3) Analytics and Financial Forecasting (AFF), and 4) Enterprise Budgeting Tool (EBT).

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 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.

While CPT focuses on budget execution and compensation projections, it draws from and contributes to the strategic planning, fee workload analysis, and performance measurement reporting processes.

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.

Analytics and Financial Forecasting (AFF)

The Analytics and Financial Forecasting (AFF) system 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. The purpose of the system is to address identified business problems and risks associated with the current manually intensive processes through automation and to provide the USPTO with a powerful forecasting tool to provide inputs to other business processes and to decision-making.

Enterprise Budgeting Tool (EBT)

The USPTO Enterprise Budgeting Tool (EBT) is a central planning and budgeting application supporting various organizations across the USPTO. EBT will replace the Corporate Planning Tool (CPT) via a phased implementation. The software behind EBT, Oracle Hyperion Planning, provides automation throughout the USPTO's budgeting lifecycle. EBT will be incorporated under the Planning and Budget Products (PBP) Master System.

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

PBP transactions include generating, consolidating, and reporting business and financial information. Information can be reviewed and approved by the appropriate business units and then be shared among all business units, as needed.

(c) any information sharing conducted by the system

All information processed is for USPTO internal use only.

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

The legal authority to collect PII and/or BII derives from

- 31 U.S.C. 3322, 3512; 44 U.S.C. 3101, 3309
- Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claims Collection Act of 1966
- 5 U.S.C. 301
- 5 U.S.C. 301 and 35 U.S.C. 1, 2, and 42

(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.)*
- ☒ 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):					

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*	☐	e. File/Case ID	☐	i. Credit Card	☐
b. Taxpayer ID	☐	f. Driver's License	☐	j. Financial Account	☐
c. Employer ID	☐	g. Passport	☐	k. Financial Transaction	☐
d. Employee ID	☒	h. Alien Registration	☐	l. Vehicle Identifier	☐
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	☒	g. Date of Birth	☐	m. Religion	☐
b. Maiden Name	☐	h. Place of Birth	☐	n. Financial Information	☐
c. Alias	☐	i. Home Address	☒	o. Medical Information	☐
d. Gender	☐	j. Telephone Number	☐	p. Military Service	☐
e. Age	☐	k. Email Address	☐	q. Physical Characteristics	☐
f. Race/Ethnicity	☐	l. Education	☐	r. Mother's Maiden Name	☐
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	☒	d. Telephone Number	☒	g. Salary	☒
b. Job Title	☒	e. Email Address	☒	h. Work History	☐
c. Work Address	☒	f. Business Associates	☐		
i. Other work-related data (specify):					

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

System Administration/Audit Data (SAAD)					
a. UserID	☒	c. Date/Time of Access	☒	e. ID Files Accessed	☐
b. IP Address	☐	d. Queries Run	☐	f. Contents of Files	☐
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	☒	Hard Copy: Mail/Fax	☒	Online	☒
Telephone	☒	Email	☒		
Other (specify):					

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	☐	Other Federal Agencies	☐
State, Local, Tribal	☐	Foreign	☐		
Other (specify):					

Non-government Sources					
Public Organizations	☐	Private Sector	☐	Commercial Data Brokers	☐
Third Party Website or Application			☐		
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	☐	Biometrics	☐
Caller-ID	☐	Personal Identity Verification (PIV) Cards	☐
Other (specify):			

☒	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	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify):			

☒	There are not any IT systems 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	☐	For administering human resources programs	☐
For administrative matters	☒	To promote information sharing initiatives	☐
For litigation	☐	For criminal law enforcement activities	☐
For civil enforcement activities	☐	For intelligence activities	☐
To improve Federal services online	☐	For employee or customer satisfaction	☐
For web measurement and customization technologies (single-session)	☐	For web measurement and customization technologies (multi-session)	☐
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).

CPT: While CPT focuses on budget execution and compensation projections, it draws from and contributes to the strategic planning, fee workload analysis, and performance measurement reporting processes. PII is utilized for administrative purposes.

ABIS utilizes a COTS product, SAP's Profitability and Cost Management (PCM), to streamline and automate business processes. ABIS does not contain PII.

AFF:

The system 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. AFF does not contain PII.

EBT: EBT does not contain PII at this time. The initial release of this system is infrastructure only and all baseline out of COTS. It does not contain any data or models at this time.

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	☐	☐	☐
DOC bureaus	☐	☐	☐
Federal agencies	☐	☐	☐
State, local, tribal gov't agencies	☐	☐	☐
Public	☐	☐	☐
Private sector	☐	☐	☐
Foreign governments	☐	☐	☐
Foreign entities	☐	☐	☐
Other (specify):	☐	☐	☐

☒ 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.

☒	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: USPTO Systems: • Enterprise Data Warehouse (EDW) • Patent Capture and Application Processing System – Examination Support (PCAPS-ES) - o Patent Application Location Monitoring (PALM) Infrastructure System (INFRA) The information transmitted between the systems is protected within USPTO's secure perimeter through the Network and Security Infrastructure (NSI) and the Enterprise Monitoring and Security Operations (EMSO) systems.
☐	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	☐	Government Employees	☒
Contractors	☒		
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.*)

☐	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
☐	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: _____.	
☒	Yes, notice is provided by other means.	PBP receives PII indirectly from other application systems (i.e. front-end systems). Individuals may be notified that their PII is collected, maintained, or disseminated by the primary application ingress system.
☐	No, notice is not provided. Specify why not:	

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

☐	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: PBP receives PII indirectly from other application systems (i.e. front-end systems). These front-end systems provide this functionality for the data that is being collected. FBPS has no authorization to decline any type of information since it is owned by the primary application.

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

☐	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: PBP receives PII indirectly from other application systems (i.e. front-end systems). These front-end systems provide this functionality for the data that is being collected.

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

☒	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Employees have the opportunity to update account information in PALM/AD at any time.
☐	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.*)

☒	All users signed a confidentiality agreement or non-disclosure agreement.
☒	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: The PBP system has implemented logging, auditing, and monitoring tools to track access to PII.
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 8 July 2018 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	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).
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish ownership rights over data including PII/BII.
☒	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

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

Personally identifiable information in PBP is secured using appropriate administrative, physical, and technical safeguards in accordance with the applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

All access has role based restrictions, and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access.

Additionally, PBP is secured by various USPTO infrastructure components, including the Network and Security Infrastructure (NSI) system and other OCIO established technical controls to include password authentication at the server and database levels.

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.”

☒	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>): COMMERCE/DEPT-1: Attendance, Leave, and Payroll Records of Employees and Certain Other Persons ☐ COMMERCE/DEPT-9: Travel Records (Domestic and Foreign) of Employees and Certain Other Persons ☐ COMMERCE/DEPT-18: Employees Personnel Files Not Covered By Notices of Other Agencies ☐ COMMERCE/PAT-TM-3: Employee Production Records
☐	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u>.
☐	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.)*

☒	There is an approved record control schedule. Provide the name of the record control schedule: Cost accounting for stores, inventory, and materials: GRS 1.1:040 Output records: GRS 4.3:031
☐	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:
☒	Yes, retention is monitored for compliance to the schedule.
☐	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	☒	Overwriting	☐
Degaussing	☒	Deleting	☒
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.

☒	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
☐	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☐	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.)

☒	Identifiability	Provide explanation: Name, home address, email address, telephone number
☐	Quantity of PII	Provide explanation:
☐	Data Field Sensitivity	Provide explanation:
☒	Context of Use	Provide explanation: PII is used for administrative purposes only.
☒	Obligation to Protect Confidentiality	Provide explanation: Based on the data collected USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974.
☒	Access to and Location of PII	Provide explanation: Due to obtaining PII, necessary measures must be taken to ensure the confidentiality of information during processing, storing and transmission.
☐	Other:	Provide explanation:

Section 12: Analysis

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

☐	Yes, the conduct of this PIA results in required business process changes. Explanation:
☒	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.

☐	Yes, the conduct of this PIA results in required technology changes. Explanation:
☒	No, the conduct of this PIA does not result in any required technology changes.