Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Patent Business Management Information (PBMI) System

Reviewed by: Henry J. Holcombe, Bureau Chief Privacy Officer

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

JENNIFER GOODE Digitally signed by JENNIFER GOODE
Date: 2025.06.20 12:59:40 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
USPTO Patent Business Management Information (PBMI) System

Unique Project Identifier: PPL-PBMI-02-00

Introduction: System Description

Provide a brief description of the information system.

Patent Business Management Information (PBMI) is a master system portfolio consisting of a collection of Automated Information Systems (AIS) under the Patents product line. The goal of PBMI is to facilitate and support examiner production, quality assurance, and report dissemination to United States Patent and Trademark Office (USPTO) employees and contractors. PBMI provides access to easy-to-acquire validated data and metrics.

PBMI contains the following subsystems:

- **Patents Reporting Oversight (PRO)** which is a reporting system and collection of reports. For example, PRO generates reports and daily summaries for Examiners' production. PRO, via its interfaces, supports the entire Patent Corps and other organizations. Examples of reports include Pendency Overall Distribution, which shows average application disposition times by Technical Center, and Biweekly Combined Examiner Time and Activity Report which shows production results for all examiners. PRO receives information from applicants and/or representatives, who request Examiner Interviews. PRO then sends emails to the public confirming interview requests where applicable. *Contains PII/BII.*
- **Web, Marketing, and Communications (WMC)** which is a collection of web services/applications providing business solutions to Patents and to the enterprise. *Contains PII/BII*
- **Integrated Quality System (IQS)** is designed for use by the Office of Patent Quality Assurance and the Patents Technology Centers to conduct quality reviews of patent examiners' office actions. *Contains PII/BII*
- **Supervisory Management Database (SMD)** which is used to track employee performance and to process employee ratings. SMD includes Management Award and Rating System (MARS), which enables rating processing for other Patents employees including supervisors. SMD contains production, docket management and quality data, Performance Appraisal Plan (PAP) information, and with that information enables award processing. SMD covers other examining processes such as signatory authority, part time programs, and Department of Commerce Form CD-81 (Authorization for Paid Overtime, Holiday Work) *Contains PII/BII*

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system
PBMI is a major application.

(b) System location

PBMI is located in Manassas, VA.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

Each subsystem in PBMI interconnects to the following:

PRO	• PE2E Patent End to End (PE2E) - retrieves examination related data, fee data and application data • Enterprise Unix Services (EUS) - server OS support to drive applications which house the web serving & database applications along with supporting actions to automate tasks (cron jobs) • Integrated Quality System (IQS) - captures application related metadata to be displayed in generating of reports/webpages • PE2E Patent End to End (- reports office action posting information and posting information and docket management information Enterprise Data Warehouse (EDW) - stores historical employee WebTA charge codes and hours claimed, employee salary history, and employee leave and compensatory time balances IQS, SMD (outlined below)
WMC	• PE2E Patent End to End (PE2E) – retrieves employee name and worker information
IQS	• PE2E Patent End to End (PE2E)- retrieve worker job code • Official Correspondence (OC) - retrieve office action count, post and mail date; office action ids • Fee Processing Next Generation (FPNG) - retrieve amendment fee information • Database System (DBS) - internal database infrastructure to provide support for report generation and web page support One Patent Service Gateway (OPSG) – retrieve data about production pay periods and quarters
SMD	• Patents Reporting Oversight (PRO) - retrieves DM Award data (DM Planner), salary information, employee details, Employee title, Overtime catch-up information, Signatory Program Information, Production Scare Information

	• Database System (DBS) - internal database infrastructure to provide support for report generation and web page support • PE2E Patent End to End (PE2E) - retrieves examination related data, fee data and application data • Enterprise Data Warehouse (EDW) - excel file download

(d) The way the system operates to achieve the purpose(s) identified in Section 4

PBMI is a web-based system that provides interactive reports and interfaces in order to allow retrieval, processing, and dissemination of information to USPTO employees and USPTO contractors.

(e) How information in the system is retrieved by the user

USPTO employees and USPTO contractors, Patent Examiners, Legal Instrument Examiners (LIEs), system administrators, examination support staff, and PTONet internal users can retrieve the information through a PTONet connection. Access granted using a least-privileged policy. Retrieval is done via intranet web-interfaces, database interfaces, and network interfaces.

(f) How information is transmitted to and from the system

Hypertext Transfer Protocol Secure (HTTPS) and SSL are used for all data transmissions to and from the Internet, USPTO DMZ, and PTONet.

(g) Any information sharing

PRO receives information from applicants and/or representatives, who request Examiner Interviews. PRO then sends emails to the public confirming interview requests where applicable.

WMC shares information via its web interface to internal USPTO employees and contractors.

IQS shares information via its web interface to authorized internal USPTO employees

SMD shares information via its web interface to internal USPTO employees and contractors.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting,

maintaining, using, and disseminating the information

Title 5 U.S.C.; 35 U.S.C. 2; and 44 U.S.C. 3101 and 3309

(i) The Federal Information Processing Standards (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	☐	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.
☐ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

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*	☐	f. Driver's License	☐	j. Financial Account	☐
b. Taxpayer ID	☐	g. Passport	☐	k. Financial Transaction	☐
c. Employer ID	☐	h. Alien Registration	☐	l. Vehicle Identifier	☐
d. Employee ID	☒	i. Credit Card	☐	m. Medical Record	☐
e. File/Case ID	☐				

n. Other identifying numbers (specify): Patent Application Number
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

General Personal Data (GPD)					
a. Name	☒	h. Date of Birth	☒	o. Financial Information	☐
b. Maiden Name	☐	i. Place of Birth	☒	p. Medical Information	☐
c. Alias	☐	j. Home Address	☒	q. Military Service	☐
d. Gender	☐	k. Telephone Number	☒	r. Criminal Record	☐
e. Age	☒	l. Email Address	☒	s. Marital Status	☐
f. Race/Ethnicity	☐	m. Education	☐	t. Mother's Maiden Name	☐
g. Citizenship	☒	n. Religion	☐		
u. Other general personal data (specify): City/State/Country					

Work-Related Data (WRD)					
a. Occupation	☒	e. Work Email Address	☒	i. Business Associates	☒
b. Job Title	☒	f. Salary	☒	j. Proprietary or Business Information	☒
c. Work Address	☒	g. Work History	☐	k. Procurement/contracting records	☐
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	☒		
l. Other work-related data (Official duty station and alternate duty station): history of roles and work examiners have done at USPTO					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	f. Scars, Marks, Tattoos	☐	k. Signatures	☒
b. Palm Prints	☐	g. Hair Color	☐	l. Vascular Scans	☐
c. Voice/Audio Recording	☐	h. Eye Color	☐	m. DNA Sample or Profile	☐
d. Video Recording	☐	i. Height	☐	n. Retina/Iris Scans	☐
e. Photographs	☐	j. Weight	☐	o. Dental Profile	☐
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	☒	c. Date/Time of Access	☒	e. ID Files Accessed	☒
b. IP Address	☒	f. 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 Describe how the accuracy of the information in the system is ensured.

PBMI employs system checks to ensure accuracy, completeness, validity, and authenticity. Each PBMI component has established specific rules or conditions for checking the syntax of information input to the system such as numbers or text; numerical ranges and acceptable values are utilized to verify that inputs match specified definitions for format and content. The Data Reform's Query Team & Validation Team perform statistical validation and code reviews to confirm data accuracy.

PBMI is secured using appropriate administrative, physical, and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, and auditing). Mandatory IT awareness and role-based training is required for staff who have access to the system and address how to handle, retain, and dispose of data. All access has role-based restrictions and individuals with privileges have undergone vetting and suitability screen. The USPTO maintains an audit trail and performs random, periodic reviews (quarterly) to identify unauthorized access and changes as part of verifying the integrity of administrative account holder data and roles.

2.4 Is the information covered by the Paperwork Reduction Act?

☒	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0651-0031 Patent Processing 0651-0032 Initial Patent Processing

☐	No, the information is not covered by the Paperwork Reduction Act.

2.5 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): Click or tap here to enter text.			

☒	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			
For a Computer Matching Program	☐	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).

PBMI collects and maintains USPTO federal employees' and USPTO contractors' PII for internal use only; with the exception of indirectly publishing basic employee information, such as name and work phone number(s), for the "employee search" functionality on www.uspto.gov. Payroll data is not collected within PBMI system boundary. Patent applicants or representatives provide name, mailing and/or email address, and phone number to facilitate correspondence. The minimum information for publication, patent grants and pre-grant publication are name and residence; however, once a patent is granted the patent applicant's name and residence (city, state) is publicly disseminated with the Patent for public record. DOC employees and DOC contractors.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

PBMI has put certain security controls in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed.

The threats to privacy are insider threats, and foreign governments. USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees. The annual training has made all employees aware of the possibility of insider threats and threats from adversarial or foreign entities and how these bad actors can affect USPTO's reputation. The following are USPTO's current policies that are adhered to: IT Privacy Policy (OCIO-POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), and USPTO Rules of the Road (OCIO-POL36). The combination of USPTO trainings and policies will help USPTO employees to recognize insider threats and threats from adversarial or foreign entities. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

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 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

☐	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☐	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☒	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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: PE2E FPNG EDW PBMI has put certain security controls in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees. The following are current USPTO policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy (OCIO- POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), USPTO Rules of the Road (OCIO-POL- 36). All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 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: https://www.uspto.gov/privacy-policy.	
☒	Yes, notice is provided by other means.	Specify how: Access to the system requires a USPTO laptop, which displays a privacy message before logging in. Each access to internal systems requires following the OCIO's Rules of the Road, which provide the Privacy Act notice.
☐	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: Individuals do not have an opportunity to decline to provide the PII/BII as the information is required for an USPTO employee or contractor and for the submission of patent applications.

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: Individuals do not have the opportunity to consent to particular uses of their PII because the system only collects the minimum required information to fulfil its intended purposes. The system has no other way to fulfil its purpose

		without the requested PII/BII.

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:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Individuals are not able to directly update their information within PBMI or its subsystems. Individuals are able to update their information by working with USPTO HR to update their records.

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: Audit logs, administrative monitoring
☒	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): ☒ 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 5 recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish DOC ownership rights over data including PII/BII.
☒	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☒	Other (specify): All sensitive-PII at-rest and in-transit are protected in accordance with NIST recommended encryption.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Adversarial entities, foreign governments, insider threats and inadvertent private information exposure are all risks and USPTO has policies, procedures and training to ensure that employees are aware of their responsibility of protecting sensitive information and the negative impact on the agency if there is a loss, misuse, or unauthorized access to or modification of sensitive private information. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. The following are current USPTO policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy (OCIO-POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), USPTO Rules of the Road (OCIO-POL- 36). All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation. 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 authorize personnel. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access. Additionally, PBMI 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. All sensitive-PII at-rest and in-transit is protected in accordance with NIST recommended encryption.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

☒ Yes, the PII/BII is searchable by a personal identifier.

☐ No, the PII/BII is not searchable by a personal identifier.

9.2 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, number, and link. *(list all that apply)*: COMMERCE/DEPT-1 Attendance, Leave, and Payroll Records of Employees and Certain Other Persons COMMERCE/PAT-TM-3 Employee Production Records
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, this system is not a system of records and a SORN is not applicable.

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:
☒	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: USPTO is working with NARA and with be submitting a records schedule for approval. USPTO will update this section to include the NARA issued disposition authority, once the schedule is approved.
☒	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 Level

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. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

☐	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 level. *(Check all that apply.)*

☒	Identifiability	Provide explanation: Name, age, date of birth, email address and place of birth can be used to identify an individual.
☒	Quantity of PII	Provide explanation: Approximately 47K rows of data associated with the following PII columns "Birth Date, Birth Country, Birth City and Birth State".
☒	Data Field Sensitivity	Provide explanation:

		PII stored in the system is data collected from USTPO employees and contractor personnel in which the information is confidential and unique to those individuals. Any unauthorized access, modification, and/or disclosure of sensitive data would have a Moderate impact on the organization and its operations.
☒	Context of Use	Provide explanation: PBMI collects and maintains USPTO federal employees' PII for internal use only; with the exception of indirectly publishing basic employee information, such as name and work phone number(s), for the "employee search" functionality on www.uspto.gov.
☒	Obligation to Protect Confidentiality	Provide explanation: USPTO examiners are obligated to protect applicants' identity and application while the application is undergoing patent prosecution.
☒	Access to and Location of PII	Provide explanation: The information captured, stored, and transmitted by the PBMI system is accessed within USPTO on-campus systems.
☐	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Nation states, adversarial entities, and insider threats are the predominant threats to the information collected and its privacy. Security controls following FedRAMP and NIST guidance were implemented to deter and prevent threats to privacy. USPTO has identified and evaluated potential threats to PII such as loss of confidentiality and integrity of information. Based upon USPTO's threat assessment policies, procedures, and training has been implemented to ensure that employees are aware of their responsibility to protect PII and to be aware of insider threats. Our employees are aware of the negative impact to the agency if there is a loss, misuse, or unauthorized access to or modification of PII.

12.2 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.

12.3 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.