

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



**Privacy Impact Assessment
for the
Building, Asset, & Property Management (BAPM)**

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

CHARLES CUTSHALL

Digitally signed by CHARLES CUTSHALL
Date: 2025.06.04 10:50:15 -04'00'

6/4/2025

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

Date

U.S. Department of Commerce Privacy Impact Assessment USPTO Building, Asset, & Property Management (BAPM)

Unique Project Identifier: EBPL-PFM-04-00

Introduction: System Description

Provide a brief description of the information system.

The Building, Asset, & Property Management (BAPM) is a United States Patent and Trademark System (USPTO) master system that is composed of four (4) Property & Facility Management (P&FM) components that operate independently:

Radio Frequency Identification (RFID) – is an Enterprise-Level asset tracking solution that aims to reduce the inventory management burden of asset management while increasing asset visibility of critical assets and improved inventory accuracy;

Property & Facility Scheduling (PFS) – consist of two schedulers, FLU Shot and RoomRez are applications used for booking meeting rooms and scheduling flu shot appointments at United States Patent and Trademark Office (USPTO);

Emergency Notification System (ENS) – is a network-based emergency notification system which provides rapid dissemination of emergency messages to USPTO personnel; and

Warehouse File Tracking System (WFTS) – is a tracking program used by USPTO to track the location of each patent and trademark file as it is transported.

Address the following elements:

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

General Support System

(b) System location

Alexandria, VA

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

Enterprise Software Services (ESS): is a major application and provides an architecture capable of supporting current software services at USPTO. ESS includes USPTOs Active Directory (AD) which hosts USPTO employee and contractor data.

Enterprise Unix Services (EUS): is a General Support System with a purpose of providing a LINUX base hosting platform to support other information systems at USPTO. The system supports the underlying operating system (OS), OS patching and updates, and OS level baseline compliance.

Enterprise Windows Servers (EWS): is an Infrastructure Information System, and provides a basic hosting platform for major applications that support various USPTO missions. Data is generally owned by the application not the platform. The USPTO facilities are leased by the General Services Administration (GSA) from LCOR, Incorporated. The facility that houses the EWS components is equipped with physical and environmental protective measures that ensure ongoing operation.

Information Delivery Product (IDP): is a master system composed of the following three subsystems: Enterprise Data Warehouse (EDW), Electronic Library for Financial Management System (EL4FMS), and Financial Enterprise Data Management Tools (FEDMT). EDW provides tool that allows managers and analysts to analyze business processes, resource use and needs, and other facets of the business. EL4FMS provides access to USPTO financial-related documents to support the decision-making activities of managers and analysts. FEDMT is a database/user interface solution utilizing the Oracle APEX product to build small applications to support Financial Reference data.

Security and Compliance Services (SCS): provides Security Incident and Event Management, Enterprise Forensic, Enterprise Management System, Security and Defense, Enterprise Scanner, Enterprise Cybersecurity Monitoring Operations, Performance Monitoring Tools, Dynamic Operational Support Plan, & Situational Awareness and Incident Response.

Network and Security Infrastructure (NSI): facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO applications.

Service Management Platform (SMP): is a Software as a Service (SaaS) cloud-based Information Technology Services Management (ITSM) Major Application that provides a single system of record for IT services, operations, and business management by automating IT service applications and processes.

Identity Management Authenticator (ID-AUTH): supports the physical protection of an organization's personnel, assets, and facilities. ID-Auth is automated control physical access systems that support security management processes and access to the USPTO facility.

Patent Capture and Application Processing System - Examination Support (PCAPS-ES):

provides processing, transmitting, and the storing of data and images to support the data-capture and conversion requirements of the USPTO patent application process.

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

BAPM is for federal employees and contractors to help with administrative matters by creating platforms where employees are notified of emergencies, track business-related schedules, and track business continuity for updates as necessary. The way each component operates to achieve its purpose is described below:

RFID: Select USPTO employees and contractor have access to the RFID system. The employee goes to the web application and log in via username and password. The users are then able to navigate the site to upload scan data from handheld scanners and then can move it to the USPTO integration of ServiceNow. The USPTO employees are able to view their account information and update their passwords as required or needed.

PFS: All USPTO employees and contractors can access PFS via the USPTO website. The employee can submit a request to schedule a flu shot or request a room reservation. The user's information is managed via ESS and active directory.

ENS: Select USPTO employees and contractors are able to access the ENS ad-hoc site through username and password. The employees are able to navigate the site where they can send out notification regarding emergencies that may impact all USPTO employees or select employees based on their duty station.

WFTS: Select USPTO employees are able to access this program file. The individuals access the program to track warehouse file locations.

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

RFID: The subcomponent is available to USPTO employees and contractors users after authentication into the assets. Data is pushed collected from the ItemAware application servers, database servers, and internal web server and pushed to ServiceNow.

.

PFS: PFS is only accessible internally within USPTO intranet. USPTO employees and contractors can navigate to the PFS scheduling site to book appoints or view and manage previous bookings.

ENS: The subcomponent can only be accessed by assigned ENS AtHoc privileged users. The forty (40) privileged users also known as ENS AtHoc operators navigate to the Blackberry AtHoc site to send emergency notifications to all USPTO employees and contractors when needed. ENS AtHoc End-users can only receive notifications. End-users cannot access the ENS AtHoc site.

WFTS: This subcomponent can be accessed by the USPTO Warehouse Supervisor's GFE as a program file that requires installation from the service desk. WFTS users do not have the capability to view content of these scanned physical files or locations of the physical files within the application itself. The transmitted data is only seen within Patents system, PALM-FOS; PALM-FOS storage functions are outside of the WFTS assessment scope.

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

Information is transmitted to and from BAPM's components via the internal USPTO network. All BAPM component applications and respective servers exist on the enterprise internal network. The personally identifiable information (PII) within BAPM, is transmitted from ESS component Active Directory (AD) and the IDP's subsystem Enterprise Data Warehouse (EDW). This information is gathered from employee's when they onboard with the agency.

(g) Any information sharing

ENS: The information collected is shared internally among agency emergency management personnel.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

35 USC Part I; Federal Continuity Directive-1 (FCD-1)

(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	<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, 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*	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
d. Employee ID	<input checked="" type="checkbox"/>	i. Credit Card	<input type="checkbox"/>	m. Medical Record	<input type="checkbox"/>
e. File/Case ID	<input type="checkbox"/>				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

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

Work-Related Data (WRD)					
a. Occupation	<input type="checkbox"/>	e. Work Email Address	<input checked="" type="checkbox"/>	i. Business Associates	<input type="checkbox"/>
b. Job Title	<input type="checkbox"/>	f. Salary	<input type="checkbox"/>	j. Proprietary or Business Information	<input type="checkbox"/>
c. Work Address	<input type="checkbox"/>	g. Work History	<input type="checkbox"/>	k. Procurement/contracting records	<input type="checkbox"/>
d. Work Telephone Number	<input checked="" type="checkbox"/>	h. Employment Performance Ratings or other Performance Information	<input type="checkbox"/>		
l. Other work-related data (specify):					

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

System Administration/Audit Data (SAAD)					
a. User ID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input type="checkbox"/>	e. ID Files Accessed	<input type="checkbox"/>
b. IP Address	<input type="checkbox"/>	f. 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 type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input checked="" type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input checked="" type="checkbox"/>		
Other (specify):					

Government Sources					
Within the Bureau	<input checked="" 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 Describe how the accuracy of the information in the system is ensured.

The BAPM system is secured by only providing access to authorized users with specific role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. For ENS USPTO employees can contractors can optionally provide a personal phone and email to receive emergency notifications. The employees are able to directly go into ENS and make this update. All system related generic error messages are presented to users while detailed debugging error messages are provided to administrators. Error conditions are handled so as not to provide information that could be exploited by adversaries. 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 screening. 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. USPTO employees and contractors are able to review and update the optional PII that is within the BAPM component ENS. All other PII data points in BAPM may be reviewed and updated via the Employee Personal Page or HR Connect. Inactive accounts will be deactivated and roles will be deleted from the application during the quarterly review or upon request.

2.4 Is the information covered by the Paperwork Reduction Act?

<input type="checkbox"/>	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
<input checked="" type="checkbox"/>	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 (TUCPBNDP)
--

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): Click or tap here to enter text.			

<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			
For a Computer Matching Program	<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 PII in BAPM is about federal employees and contractors to help with administrative matters that have to do with employee and business satisfaction by creating platforms where employees are notified of emergencies, and track business-related schedules as necessary.

- 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.)

In the event of computer failure, insider threats, or attack against BAPM by adversarial or foreign entities, any potential PII data stored within the system could be exposed. To avoid a breach, BAPM has certain security controls in place to ensure the information is handled, retained, and disposed of appropriately. 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. These audit trails are based on application server out-of-the-box logging reports reviewed by the Information System Security Officer (ISSO) and System Auditor and any suspicious indicators such as browsing will be immediately investigated and appropriate action taken. Also, system users undergo annual mandatory training regarding appropriate handling of information.

NIST security controls are 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. 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	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Federal agencies	<input type="checkbox"/>	<input 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"/>

<input type="checkbox"/>	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?

<input type="checkbox"/>	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input checked="" type="checkbox"/>	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.

<input checked="" type="checkbox"/>	<p>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:</p> <p>ID-AUTH SMP SCS PCAPS-ES NSI</p> <p>NIST security controls are 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</p>
-------------------------------------	---

	accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. 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.
<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.

6.4 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	<input 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 checked="" 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: https://www.uspto.gov/privacy-policy	
<input checked="" type="checkbox"/>	Yes, notice is provided by other means.	Specify how: This PIA provides notice.
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

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: USPTO employees and contractors have the opportunity to decline to provide the PII that is optional in the BAPM component ENS. This is their personal email and personal phone number.
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to decline to provide	Specify why not: Individuals do not have the opportunity to decline to provide PII/BII to BAPM. The information collected

	PII/BII.	is the minimum information required for BAPM's purpose.
--	----------	---

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 opportunity to consent to particular uses of their PII/BII.	Specify why not: Individuals do not have an opportunity to consent to particular uses of their PII/BII. The information is only collected for one purpose and is required for to ensure USPTO business operations.

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: USPTO employees and contractors can update their the optional PII they provide within ENS, this information is the personal email and personal phone number, all other data the individuals do not have the opportunity to review/update directly in the BAPM component ENS.
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: USPTO employees and contractors are not able to update their information directly in BAPM, however they may review and update their PII via their Employee Personal Page or HR Connect.

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: Audit logs
<input checked="" type="checkbox"/>	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): 6/11/2024 <input checked="" 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 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).
<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.

<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 type="checkbox"/>	Contracts with customers establish DOC ownership rights over data including PII/BII.
<input 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. *(Include data encryption in transit and/or at rest, if applicable).*

PII within BAPM is secured using appropriate management, operational, and technical safeguards in accordance with NIST requirements. Such management controls include a review process to ensure that management controls are in place and documented in the System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII/BII data to a small subset of users. 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 system maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity. Data is encrypted in transit and at rest.

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."

<input checked="" type="checkbox"/>	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i> DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input type="checkbox"/>	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.)*

<input checked="" type="checkbox"/>	<p>There is an approved record control schedule. Provide the name of the record control schedule:</p> <p>Facilities Management Division Files - N1-241-05-1:8b - Temporary: Destroy when 5 years old</p> <p>Facility, space, vehicle, equipment, stock, and supply administrative and operational records. -GRS 5.4:010-Temporary. Destroy when 3 years old or 3 years after superseded.</p> <p>Employee Health and Safety Records -GRS 2.7 :010 -Temporary. Destroy when 3 years old,</p> <p>Continuity and Emergency Planning Records -Employee emergency contact information GRS 5.3: 020 - Temporary. Destroy when superseded or obsolete, or upon separation or transfer of employee</p> <p>General Technology Management Records - Information technology operations and maintenance records – GRS 3.1:020 - Including System logs – Temporary: Destroy 3 years after (See GRS for cutoff instructions).</p>
<input type="checkbox"/>	<p>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:</p>
<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 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.)

<input checked="" 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 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 level.
(Check all that apply.)

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: All the PII data points identified in section 2.1, can be used to identify an individual.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: There are about 7 PII data points for about 16,000+ individuals within the system. BAPM leverages and transmit the following PII: Employee Name and ID, Home Address, Work Telephone, and Work Email [LA1] [WJ2] [WJ3]. Personal Telephone and Email are voluntary.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: BAPM data is general contact information of individuals, though the information may include an individual's home address, the information stored within BAPM as a whole including home address is not overtly sensitive information.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: Information is used to track USPTO information system equipment, provide employees with emergency notifications, and for employee facility management transactions.
<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: Necessary measures must be taken to ensure the confidentiality of information during processing, storing and transmission of the data. Access controls are used to ensure only a authorized personnel have access to the system.
<input type="checkbox"/>	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.)

The PII in this system does not pose a risk if exposed. System users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zone within the cloud and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized accounts. USPTO monitors, in real-time, all activities and events within the servers storing the potential PII data and personnel review audit logs received on a regular bases and alert the appropriate personnel when inappropriate or unusual activity is identified.

12.2 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.

12.3 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.