Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Case Management System (CMS)

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: 2024.01.02 13:35:00 -05'00' 12/13/2022

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Case Management System (CMS)

Unique Project Identifier: EBPL-PM-01-00

Introduction: System Description

Provide a brief description of the information system.

Case Management System (CMS) is a suite of SaaS applications hosted by Tyler Federal, which is a Federal Risk and Assessment Management Program (FedRAMP)-authorized Software as a Service (SaaS). Case Management System is composed of several applications that enable USPTO to perform Office of Human Resources (OHR) functions. The applications contained in Case Management System include the following:

- Background Investigation Tracking System, (BITS) is an application information system, and provides a personnel background investigation security tracking system for the USPTO.
- Employee Relations & Labor Relations (ERLR) is used by USPTO to manage Employee Relation (ER) and Labor Relation (LR) cases.
- The Equal Employment System (EES) is an application information system that provides support to the Office of Equal Employment Opportunity and Diversity business functions.
- Reasonable Accommodation Case Management System (RACMS) supports all activities associated with reasonable accommodations.

Address the following elements:

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

(b) System location
Case Management System is located in Ashburn, Virginia, with an alternate host site in Atlanta, Georgia.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
Case Management System interconnects with the following systems:

- **Network and Security Infrastructure (NSI):** The NSI is an Infrastructure information system which provides an aggregate of subsystems that facilitates the communications, secure access, protective services, and network infrastructure support for all United States Patent and Trademark Office (USPTO)

- **PTO-EBPL-IDP-EDW Enterprise Data Warehouse (PTO-003-02);** EDW system is an automated information system (AIS) that provides access to integrated United States Patent and Trademark Office (USPTO) data to support the decision-making activities of managers and analysts in the USPTO's business areas as needed to achieve business goals. It helps USPTO managers and analysts to answer a variety of strategic and tactical business questions using quantitative enterprise business information. Specifically, EDW provides a tool that allows managers and analysts to analyze business processes, resource use and needs, and other facets of the business.

- **Identity Credential Access Management Identity as a Service (ICAM-IdaaS)):** ICAM-IDaaS is an infrastructure information system that provides authentication and authorization service to secure all USPTO enterprise applications and provides audit ability to user activity.

- **PTO-CISO Common Controls (CISO-CC)**, the Common Control Provider for the USPTO CISO Common Controls. The USPTO CISO Common Controls maximize the use of common controls at the organization level to promote standardized, consistent, security and privacy policy inheritance by individual system owners and are available for inheritance by all USPTO information systems at the low, moderate, and high impact level.

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

Authorized users access the applications which comprise the Case Management System through a web-based portal to create, update, track and monitor the status of employee cases.

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

USPTO OHR staff access the system via the USPTO intranet and web-based portal. Users are able to retrieve and transmit information from the applications after authentication.

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

Users access Case Management System via the USPTO intranet and a web-based portal hosted by Tyler Federal. The transmission of information is facilitated by an encrypted communication between USPTO and Tyler Federal.

(g) Any information sharing

BITS: Information is shared within the bureau

ERLR: Information is shared within the bureau

EES: Information is shared within the bureau, DOC bureaus and other federal agencies based on business need and requests. Information is shared with supporting federal agencies and DOC when requested.

RACMS: Information is shared within the bureau

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

BITS: Executive Orders 10450, 13526, 13764; 5 U.S.C. 301; 15 U.S.C. 1501 et seq.; 28 U.S.C. 533–535; 44 U.S.C. 3101; Executive Orders 9397, as amended by 13478, 10577, 10865, 12968, and 13470; Section 2, Civil Service Act of 1883; Public Laws 82–298 and 92– 261; Title 5, U.S.C., sections 1303, 1304, 3301, 7301, and 9101; Title 22, U.S.C., section 2519; Title 42 U.S.C. sections 1874(b)(3), 2165, and 2201; Title 50 U.S.C. section 435b; Title 51, U.S.C., section 20132; Title 5 CFR sections 731, 732 and 736; Homeland Security Presidential Directive 12 (HSPD 12), Policy for a Common Identification Standard for Fed. Employees and Contractors 6 (Aug. 5, 2005); OMB Circular No. A–130; 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202–957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210–110; Executive Order 12564; Public Law 100–71, dated July 11, 1987.

ERLR: 5 U.S.C. 301; Title V Chapter 71, FLRA Statute; 5 U.S.C. 7531-7533; 5 CFR 2411-2473; E.O. 12107, Relating to the Civil Service Commission and Labor Management in the Federal Service.

EES and RACMS: 5 U.S.C. 301; Rehabilitation Act of 1973, 29 U.S.C. 701, 791, 794; Title VII of the Civil Rights Act of 1964, 42 U.S.C. 2000e; 9 U.S.C. 621 et seq.; 29 U.S.C. 701 et seq.; 29 U.S.C. 791 et seq.; 29 CFR 1605 (Guidelines on Discrimination Because of Religion); 29 CFR 1614 (Federal Sector Equal Employment Opportunity); 29 CFR 1614.203 (Regulations to Implement the Equal Employment Provisions of the Americans With Disabilities Act); 5 U.S.C. 302, 1103; Executive Order 13164, Requiring Federal Agencies to Establish Procedures to Facilitate the Provision of Reasonable Accommodation (July 26, 2000); Americans with Disabilities Act Amendments Act (ADAAA) of 2008; and Executive Order 13548, Increasing Federal Employment of Individuals with Disabilities (July 26, 2010); AAO 214-01, and AAO 214-02.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The FIPS 199 security impact category for the system is 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):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: For BITS, the collection of SSN is necessary for the system users to conduct the background investigation tracking.					

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):					

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 (specify):					

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): Account logon events, Account management, Directory Service Access, Object Access, Policy Change, Privileged Use, Process Tracking, System Events					

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.

The system 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 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. Inactive accounts will be deactivated and roles will be deleted from the application.

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. • #3206-005, Questionnaires for National Security Positions, Standard Form 86 (SF 86) • #3206-0261, SF 85 Questionnaire for Non-Sensitive Positions
☐	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).

BITS	BITS is used to perform a background investigation as authorized by Executive Order 10450 and 5 C.F.R. Parts 731, 732, and 736. Periodic investigations are conducted at least once every 5 years on individuals who occupy Public Trust Positions as well as those individuals who have access to classified (national security positions). The background investigation is not an evaluation of the subject's character, but is instead a determination of the likelihood that a particular person will adhere to all security requirements in the future. In addition, Homeland Security Presidential Directive 12 (hereinafter HSPD-12) requires a standardized form of official identification for both government employees and contractors. The directive establishes minimum government-wide background investigation requirements for entry on duty and states that official identification cards should be issued only to those individuals with certain pre-employment background checks completed and that the validity of these checks must be updated or verified every five (5) years for employees, other federal government personnel and contractors. The HSPD12 directive will expand the USPTO's oversight responsibilities to include monitoring identification card recertification for all employees and contractors, and checking hiring practices for contractors who are investigated and hired locally.
ERLR	The information will be used to document, track and manage the flow of ER and LR cases more efficiently. Both organizations will use the same system, and they will be able to control the sharing of records and documents among them in accordance with the business rules defined in relevant workflows. The system will automatically generate template letters, and reports for upcoming events, and reports can be shared between ER to LR as approved by the relevant Human Resource (HR) business area or Human Resource Senior Management. The systems pull PII from the database to automatically generate these files and reports.

EES	PII is used by the system to support USPTO's compliance with Equal Employment Opportunity (EEO) laws for employees, contractors and applicants.
RACMS	PII used by the system will support USPTO comply with reasonable accommodation requirements for employees and USPTO job applicants.

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 the system by adversarial or foreign entities, any potential PII data stored within the system could be exposed. To avoid a breach, the system 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.

Case Management System interconnect with NSI, CISO-CC, IDP, and ICAM-IDaaS.

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. Encryption and access controls are used to prevent PII/BII leakage

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. (BITS/ERLR)
☒	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: Case Management System interconnect with NSI, CISO-CC, IDP, and ICAM-IDaaS. 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. Encryption and access controls are used to prevent PII/BII leakage
☐	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: Employees are requested to complete the Request for Reasonable Accommodation Medical Provider Statement form.
☐	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: individuals have the opportunity to decline to provide PII/BII however declining to provide the information would result in not being considered for employment or a case not being able to be processed or delayed. BITS: All information requested is provided on a voluntary basis. USPTO as part of the U.S Government is authorized to ask for this information under Executive Orders 10450 and 10577. As such the information is required in order to conduct adequate background investigation to be considered for employment with the USPTO. Declining to provide the information would result in not being considered for employment. EES/RACMS: Information is provided voluntarily; however, not providing the information would result in case not being able to be processed or delayed.
☒	No, individuals do not have an opportunity to decline to provide	Specify why not: ERLR: PII that is processed or stored by ERLR is pulled from

	PII/BII.	internal USPTO personnel records. This information is needed for case management, and individuals cannot decline having this information input in to the system.

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: Individuals have an opportunity to consent to particular uses of their PII/BII since all information requested is provided on a voluntary basis. USPTO as part of the U.S Government is authorized to ask for this information under Executive Orders 10450 and 10577. Social Security Number (SSN) is needed in order to keep records accurate, because other people may have the same name and birth date. The executive Order 9397 also asks Federal Agencies to use SSN to help identify individuals in agency records. The information is required in order to conduct adequate background investigation to be considered for employment with the USPTO. Declining to provide all PII/BII requested may result in not being considered for employment. EES/RACMS: Information is provided voluntarily; however, not providing the information would result in case not being able to be processed or delayed.
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: ERLR: PII processed or stored by ERLR is pulled from internal USPTO personnel records and individuals cannot consent to a particular use within ERLR.

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: For BITS - Individuals do not have access to review their PII. They can however, reach out to the security office to review to update any PII/BII information. For ERLR - Employees cannot view or update information but the information that is updated within EDW will be synced to ERLR. For EES-RACMS - Users can request to update information through a formal process through the USPTO OHR.
☐	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: BITS/ERLR: Application, System and Security logs are used to track and record access to PII/BII. The EES/RACMS Tyler Federal and USPTO Administrator conduct monthly audits of the system, to include when and by whom the system was accessed and what info was updated, changed, corrected, etc.
☐	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 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 (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):

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 the system 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."

☒	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/OIG-1: Investigative Records • COMMERCE/DEPT-14: Litigation, Claims, and Administrative Proceeding Records • COMMERCE/PAT-TM-24: Background Investigations • COMMERCE/DEPT-18: Employees Personnel Files not covered by Notices of Other Agencies. • EEOC/GOVT-1: Equal Employment Opportunity in the Federal Government Complaint and Appeal Records • MSPB/Govt-1: Appeals and Case Records • OPM/GOVT-2: Employee Performance File System Records • OPM/GOVT-3: Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers • OPM Central-9: Personnel Investigations Records • OPM/Govt-9: File on Position Classification Appeals, Job Grading Appeals, and Retained Grade of Pay Appeals and FLSA Claims and Complaints
☐	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: • BITS: Personnel Security Investigative Reports (GRS 5.6, 170); Personnel Security and Access Clearance Records (GRS 5.6, 180-181) Index to the Personnel Security Case Files (GRS 5.6, 190) • ERLR: NARA GRS Schedule 2.3: Employee Relations Records, Item 060, Administrative

	Grievances; Disciplinary, and Adverse Action Files; Item 050, Labor Management Relations Agreement Negotiations Records. • EES: NARA GRS Schedule 2.3 Items 110 & 111 EEO discrimination complaint case files, 120 Records documenting contractor compliance with EEO regulations • RACMS: NARA GRS Schedule 2.3, Item 20. Reasonable Accommodation Case Files.
☐	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 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, SSN, DOB, POB and Alias can be easily used to identify an individual.
☒	Quantity of PII	Provide explanation: Collectively, the number of records collected generate a large amount of PII and a breach in such large numbers of individual PII must be considered in the determination of the impact level.

☒	Data Field Sensitivity	Provide explanation: The presence of employee SSNs, DOB, POB, and Name in the BITS system alone are sensitive PII, and in combination, could result in potential harm to individuals if not used in accordance with their intended use. For ERLR, the use of PII and work / system audit data in combination for tracking and reporting of employee and labor relations cases. EES/RACMS includes medical information.
☒	Context of Use	Provide explanation: BITS acts as an electronic personnel security folder for each person, tracking data related, but not limited to, investigations, clearances and adjudications. For ERLR, because the information containing PII must be transmitted outside of the USPTO environment, there is an added need to ensure the confidentiality of information during transmission. For EES/RACMS, use of PII and work / system audit data in combination for tracking and reporting of equal employment or accommodations cases may provide a detailed private individual profile.
☒	Obligation to Protect Confidentiality	Provide explanation: Based on the data fields input in to the BITS system, USPTO must protect the PII of each individual in accordance with the Privacy Act of 1974.
☒	Access to and Location of PII	Provide explanation: Because the information containing PII must be transmitted outside of the USPTO environment, there is an added need to ensure the confidentiality of information during transmission.
☐	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 poses 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.

☐	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.