Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
Case Management System (CMS)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Case Management System (CMS)

Unique Project Identifier: EBPL-PM-01-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system: *Provide a brief description of the information system.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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 purpose that the system is designed to serve

Case Management System enables the USPTO Office of Human Resources (OHR) to perform several responsibilities, including background investigation tracking, employee and labor relations activities, management of Equal Employment Opportunity (EEO) claims, and managing and tracking requests for reasonable accommodation requirements of the Rehabilitation Act of 1973.

e) *The way the system operates to achieve the purpose*

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.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

Case Management System collect and maintain a range of PII data from USPTO employees, including first name, last name, date of birth, place of birth, gender, age, race, address, phone number and case number email address, employee identification (ID), medical condition, physical/mental impairment, accommodation requested, case number, background investigation details, personnel actions, disciplinary actions, and other details.

g) Identify individuals who have access to information on the system

Access to the applications which are comprised of the Case Management System are restricted to USPTO personnel and contractors with authorized access to support the applications.

h) 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.

i) 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.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

☒ This is a new information system. *Continue to answer questions and complete certification.*

☐ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*

☐ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment. *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

☒ Yes. This is a new information system.

☐ Yes. This is an existing information system for which an amended contract is needed.

☐ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

☐ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

☐ Yes. *(Check all that apply.)*

Activities			
Audio recordings	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify):			

☒ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☒ Yes, the IT system collects, maintains, or disseminates BII.

☐ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

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

☒ DOC employees
☒ Contractors working on behalf of DOC
☒ Other Federal Government personnel
☒ Members of the public

☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

☒ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form. The collection of SSN is necessary for the system users to conduct the background investigation tracking.
Provide the legal authority which permits the collection of SSNs, including truncated form. Executive Orders 10450, 13526; 5 U.S.C. 301 and 7531–7533; 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, 10450, 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(e); Title 51, U.S.C., section 20132; Title 5 CFR sections 731, 732 and 736; Homeland Security Presidential Directive 12 (HSPD 12), OMB Circular No. A–130; E.O. 12107; E.O. 13164; 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; 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). Title V Chapter 71, FLRA Statute; 5 CFR 2411-2473.

☐ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

☒ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☐ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ The criteria implied by one or more of the questions above **apply** to the Case Management System (CMS) and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

☐ The criteria implied by the questions above **do not apply** to the Case Management System (CMS) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Colleen Sheehan Office: Office of the Chief Administrative Officer (OCAO) Phone: (571) 272-8246 Email: Colleen.Sheehan@uspto.gov Signature: Users, Sheehan, Colleen Digitally signed by Users, Sheehan, Colleen Date: 2022.09.13 10:36:44 -04'00' Date signed: _____	**Chief Information Security Officer** Name: Don Watson Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-8130 Email: Don.Watson@uspto.gov Signature: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2022.10.04 09:19:43 -04'00' Date signed: _____
Privacy Act Officer Name: Ezequiel Berdichevsky Office: Office of General Law (O/GL) Phone: (571) 270-1557 Email: Ezequiel.Berdichevsky@uspto.gov Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2022.09.30 15:08:23 -04'00' Date signed: _____	**Bureau Chief Privacy Officer and Authorizing Official** Name: Henry J. Holcombe Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-9400 Email: Jamie.Holcombe@uspto.gov Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2022.10.04 14:48:03 -04'00' Date signed: _____
Co-Authorizing Official Name: Frederick Steckler Office: Office of the Chief Administrative Officer (OCA) Phone: (571) 272-9600 Email: Frederick.Steckler@uspto.gov Signature: Users, Steckler, Frederick W. Digitally signed by Users, Steckler, Frederick W. Date: 2022.10.11 17:43:32 -04'00' Date signed: _____	