Template Version Number: 01-2020

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

Privacy Threshold Analysis
for the
USPTO MicroPact Background Investigation Tracking System / Employee Relations & Labor Relations System (BITS/ERLR)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO MicroPact Background Investigation Tracking System / Employee Relations & Labor Relations System (BITS/ERLR)

Unique Project Identifier: PTOC-009-00

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 and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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).

The MicroPact Background Investigation Tracking System / Employee Relations & Labor Relations (BITS/ERLR) are suites of web-based applications hosted by the MicroPact FedRAMP Software as a Service (SaaS) which includes: supporting hardware and software, secure computing facilities, Internet gateway communications security, system administration, and system and application security services.

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

BITS/ERLR is a major application.

b) System location

BITS/ERLR system is located at 44470 Chilum Place Bldg 1, Ashburn, VA 20147. BITS/ERLR has an alternate hot site located at data center located at 180 Peachtree Street, Atlanta, GA at an Equinox Atlanta Data Center.

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

The BITS/ERLR applications are hosted by the MicroPact SaaS. BITS-ERLR interconnects with the following systems:

- **Network and Security Infrastructure (NSI)**: The NSI is an Infrastructure information system, and 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)

- **Enterprise Software Services (ESS)** - ESS provides Enterprise Directory Services, Role-Based Access Control System, Email as a Service, PTO Exchange Services, Symantec Endpoint Protection, Enterprise SharePoint Services, etc. IT applications ESS – RBAC facilitates the communication between USPTO and MicroPact.

- **Information Delivery Product (IDP)** - IDP is a Master System composed of the following three subsystems: 1) Enterprise Data Warehouse; 2) Electronic Library for Financial Management System (EL4FMS); and 3) Financial Enterprise Data Management Tools (FEDMT).
- **Enterprise Data Warehouse (EDW):** 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.

- **Office of Personnel Management-National Background and Investigations Bureau (OPM/NBIB):** NBIB will be the primary provider of effective, efficient, and secure background investigations for the Federal Government. NBIB is designed with an enhanced focus on national security, customer service, and continuous process improvement to meet this critical government-wide need now and in the future.

- **National Finance Center (NFC):** NFC data is fed to the USPTO's Enterprise Data Warehouse. – USPTO System administrators then upload a flat file from the Enterprise Data Warehouse into the Employee Relations / Labor Relations system. There is no direct connection between the two systems – it requires human intervention to upload this data.

d) The purpose that the system is designed to serve

BITS is an application information system, and provides a personnel background investigation security tracking system for the USPTO.
ERLR is used by the USPTO Office of Human Resources (OHR) to manage and share records\documents between Employee Relation (ER) and Labor Relation (LR).

e) The way the system operates to achieve the purpose

BITS USPTO adjudicators, contractor and employee specialist access the application through a web-based portal to create, update, track and monitor the status of personnel background investigations. Access to the web portal is restricted to USPTO personnel within the intranet and who have received authorization.
ERLR administrators, managers, specialists and employees are able to access the application through a web-based portal to input case data, events and dates. Manage the sharing of records and documents between assigned staff and internal organizations using business rule workflow. Access to the web portal is restricted to USPTO personnel within the intranet and who have received authorization.

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

BITS tracks a number of candidate types (employees, contractors etc.) and their current personnel security details. The BITS acts as an electronic personnel security folder for each person, tracking data related, but not limited to, investigations, clearances and adjudications.
The ER group uses the system to manage employee relation issues, to include disciplinary actions, conduct actions, and administrative grievances (for non-union employees).
The LR group uses the system to manage the negotiated grievance processes and management initiatives.

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

BITS: USPTO OHR staff, which includes administrators, contractor specialists, employee specialists, report writers, security specialists, security service managers and adjudicators.
ERLR: USPTO OHR staff, which include ER and LR administrators, managers and specialists.

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 systems after authenticating.

i) How information is transmitted to and from the system

Users access the BITS and ERLR systems via the USPTO intranet and a web-based portal hosted by the MicroPact SaaS. The transmission of information is facilitated by an encrypted communication between USPTO and MicroPact.

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 (version 01-2015 or 01-2017). *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 (version 01-2019 or later). *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; 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.

☐ 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

☒ I certify the criteria implied by one or more of the questions above **apply** to the MicroPact Background Investigation Tracking System / Employee Relations & Labor Relations (BITS/ERLR) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

☐ I certify the criteria implied by the questions above **do not apply** to the MicroPact Background Investigation Tracking System / Employee Relations & Labor Relations (BITS/ERLR) 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 Human Resources (C/OHR) Phone: (571) 272-8246 Email: Colleen.Sheehan@uspto.gov Signature: Users, Sheehan, Colleen Digitally signed by Users, Sheehan, Colleen Date: 2021.05.11 14:30:44 -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: DON R Watson Digitally signed by DON R Watson Date: 2021.05.12 07:36:11 -04'00' Date signed: _____
Privacy Act Officer Name: John Heaton Office: Office of General Law (O/GL) Phone: (571) 270-7420 Email: Ricou.Heaton@upsto.gov Signature: Users, Heaton, John (Ricou) Digitally signed by Users, Heaton, John (Ricou) Date: 2021.04.19 15:22:47 -04'00' Date signed: _____	**Bureau Chief Privacy Officer and Co-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: 2021.05.12 13:23:39 -04'00' Date signed: _____
Co-Authorizing Official Name: Frederick Steckler Office: Office of the Chief Administrative Officer (C/CAO) Phone: (571) 272-9600 Email: Frederick.Steckler@upsto.gov Signature: Users, Steckler, Frederick W. Digitally signed by Users, Steckler, Frederick W. Date: 2021.05.14 18:15:13 -04'00' Date signed: _____	