Version Number: 01-2017

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

**Privacy Threshold Analysis**
**for the**
**MicroPact Background Investigation Tracking System/ Employee Relations & Labor Relations (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: [2396] 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 of the information system in a way that a non-technical person can understand.*

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 system.
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. NSI and ESS – RBAC facilitates the communication between USPTO and MicroPact.
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 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 received authorization.

*f) A general description of the type of information collected, maintained, use, or disseminated by the system*
BITS tracks a number of candidate types (employees, contractors, volunteers 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 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. 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 later). *Skip questions and complete certification.*

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. *Please describe the activities which may raise privacy concerns.*

☒ 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 about: *(Check all that apply.)*

☐ Companies

☐ Other business entities

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

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or

trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

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

- ☒ DOC employees
- ☒ Contractors working on behalf of DOC
- ☐ 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 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.

4c. 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, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the 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.

Name of System Owner (SO): Colleen Sheehan

Signature of SO: Users, Sheehan, Colleen Digitally signed by Users, Sheehan, Colleen Date: 2020.02.18 16:22:18 -05'00' Date: _____

Name of Chief Information Security Officer (CISO): Don Watson

Signature of CISO: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2020.03.13 08:12:46 -04'00' Date: _____

Name of Authorizing Official (AO) & Bureau Chief Privacy Officer (BCPO): Henry J. Holcombe

Signature of AO & BCPO: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2020.03.19 16:35:27 -04'00' Date: _____

Name of Authorizing Official (AO) or Designated Representative: Frederick W. Steckler

Signature of AO: Users, Steckler, Frederick W. Digitally signed by Users, Steckler, Frederick W. Date: 2020.04.10 14:50:37 -04'00' Date: _____