Version Number: 01-2017

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

Privacy Impact Assessment
for the
MicroPact Background Investigation Tracking System / Employee Relations & Labor Relations System (BITS/ERLR)

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

for Dr. Catrina D. Purvis LISA MARTIN Digitally signed by LISA MARTIN Date: 2019.06.14 11:35:36 -04'00' 05/17/2019

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO MicroPact Background Investigation Tracking System / Employee Relations & Labor Relations System (BITS/ERLR)

Unique Project Identifier: [2396] PTOC-009-00

Introduction: System Description

(a) a general description of the information in the system

The MicroPact Background Investigation and Tracking System (BITS) is a suite of Web-based applications. MicroPact provides a fully managed support infrastructure service including: supporting hardware and software, secure computing facilities, Internet gateway communications security, system administration, and system and application security services.

The MicroPact Employee Relation and Labor Relations System (ERLR) is a web application suite used by the USPTO Office of Human Resources (OHR). Both OHR divisions use the same system, but logical access controls are employed to manage the sharing of records and documents between the Employee Relations (ER) & Labor Relations (LR) divisions in accordance with the business rules defined in relevant workflows. The ERLR is an application information system, and satisfies a business need to have one case management system that has business process flows built into it for both the ER and LR organizations.

(b) a description of a typical transaction conducted on the system

BITS is an Application information system, and provides a personnel background investigation security tracking system for the USPTO. The system 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.

ERLR uses MicroPact Entellitrak software as a Case Management tool with automatic workflow functions using business rules to route work to the proper person and/or organization and to define the steps to be taken. A graphical user interface is used for inputting case data, events, and dates associated with a case. A dashboard displays all of the cases, the status of the cases, and all of the up-coming events associated with the cases assigned to an ER or LR staff member. The system automatically generates template letters, and reports for upcoming and past events based upon business rules and the division workflows. 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. Managing management initiatives is similar to managing an information system's project.

(c) any information sharing conducted by the system

The information for BITS will primarily stay within the USPTO Office of Security and Safety and is shared with properly credentialed background investigators who are conducting the background investigation and employees from the OHR's Employee Relations Division who conduct suitability adjudication on USPTO employees. It will also be shared with other federal agency security offices that require the 'passing' of USPTO background investigative data for USPTO personnel visiting or attending meetings, conferences, and/or briefings at other federal agencies.

Information for ERLR will be shared internally with OHR and in some cases the USPTO Office of General Counsel (OGC). Information will not be shared with external customers and business areas.

(d) a citation of the legal authority to collect PII and/or BII

Executive Orders 10450, 12065; 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) and OMB Circular No. A–130.

5 U.S.C. 301; 44 U.S.C. 3101; 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.

(e) the Federal Information Processing Standard (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.)*

☒ This is an existing information system in which changes do not create new privacy risks. *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):					

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*	☒	e. File/Case ID	☒	i. Credit Card	☐
b. Taxpayer ID	☐	f. Driver's License	☐	j. Financial Account	☐
c. Employer ID	☐	g. Passport	☐	k. Financial Transaction	☐
d. Employee ID	☒	h. Alien Registration	☐	l. Vehicle Identifier	☐
m. Other identifying numbers (specify): Last, First and Middle initial, DOB, POB, Dual Citizenship, Position Title, Position Designation, Employee/Contractor, Name of Contracting Co., if applicable, type of background investigation (BI), status of BI, BI Case Number, OPM Issue Code and adjudicative determination					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: The system 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.					
*If SSNs are collected, stored, or processed by the system, please explain if there is a way to avoid such collection in the future and how this could be accomplished: At this time, there is no way for avoiding the collection and processing of SSNs by the system. This IN is necessary for the system users to conduct the background investigation tracking.					

General Personal Data (GPD)					
a. Name	☒	g. Date of Birth	☒	m. Religion	☐
b. Maiden Name	☒	h. Place of Birth	☒	n. Financial Information	☐
c. Alias	☒	i. Home Address	☐	o. Medical Information	☐

d. Gender	☒	j. Telephone Number	☐	p. Military Service	☐
e. Age	☒	k. Email Address	☒	q. Physical Characteristics	☐
f. Race/Ethnicity	☒	l. Education	☐	r. Mother's Maiden Name	☐
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	☒	d. Telephone Number	☒	g. Salary	☐
b. Job Title	☒	e. Email Address	☒	h. Work History	☐
c. Work Address	☒	f. Business Associates	☐		
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	d. Photographs	☐	g. DNA Profiles	☐
b. Palm Prints	☐	e. Scars, Marks, Tattoos	☐	h. Retina/Iris Scans	☐
c. Voice Recording/Signatures	☐	f. Vascular Scan	☐	i. Dental Profile	☐
j. 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	☒	d. Queries Run	☒	f. Contents of Files	☒
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	☒	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 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):			

☒	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			
To determine eligibility	☐	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).

For BITS - The U.S. Patent & Trademark Office (USPTO) must ensure that only trustworthy individuals are hired to work in national security or public trust positions. The primary means for determining whether an individual is trustworthy is the background investigation, 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 and contractors. The HSPD-12 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.

For 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.

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 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: The BITS system is connected with OPM/NBIB. For ERLR - HR data is resident within the 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.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 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:// https://www.uspto.gov/privacy-policy	
☐	Yes, notice is provided by other means.	Specify how:
☐	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:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: 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. PII that is processed or stored by ERLR is pulled from 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:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Information requested is provided voluntarily. USPTO is authorized to ask for this information under Executive Orders (EO) 10450 and 10577. SSN is needed in order to keep records accurate because other people may have the same name and birth date. EO 9397 also asks Federal Agencies to use SSN to help identify individuals in agency records. Information is required in order to conduct adequate background investigations to be considered for employment. 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 ERLR - 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: For BITS - Individuals do not have access to review their PII information. They can however, reach out to the security office to review to update any PII/BII information.

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 has audit features built into the application. The ERLR Administrator conducts monthly audits of the system, to include when and by whom the system was accessed and what info was updated, changed, or corrected.
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): May 23, 2018_____ ☐ 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 (POAM).
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☐	Contracts with customers establish 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.

Automated operational controls include securing all hardware associated with BITS/ERLR in the MicroPact Data Center. The Data Center is controlled by access card entry and all use of the card is audited through the access system to restrict access to the servers, their Operating Systems and databases. In addition, physical access points to the MicroPact Data Center are controlled by physical locking mechanisms including separate door locks, an alarm control contact monitored twenty-four (24) hours a day by ADT, a motion detector at each door and hallway and a video camera at each hallway. Contingency planning has been prepared for the data. Backups are performed on the processing databases. All backup tapes that contain PII or information covered under the Privacy Act are encrypted with FIPS 140-2 compliant algorithms by the MicroPact Database Administration Team. Technical controls: Information is also secured through the application itself, by only allowing authorized users access to the application and to data to which they have access and privilege. Also the information system controls attacks and unauthorized attempts on the application and database through strict logins, AV protection, and through firewalls.

Section 9: Privacy Act

9.1 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 and number *(list all that apply)*: "COMMERCE/PAT-TM-24: Background Investigations" Employees Personnel Files not covered by Notices of Other Agencies – COMMERCE/DEPT-18.
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, a SORN is not being created.

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: Yes. ERLR files that relate to employee relation and labor relations are covered by the "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."
☐	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 Levels

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.

☐	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 levels. *(Check all that apply.)*

☒	Identifiability	Provide explanation: BITS - Name, SSN, DOB, POB. ERLR - Employee work related data and system administration/audit data.
☐	Quantity of PII	Provide explanation:
☒	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.

☒	Context of Use	Provide explanation: The BITS acts as an electronic personnel security folder for each person, tracking data related, but not limited to, investigations, clearances and adjudications. For ERLR - Use of PII and work / system audit data in combination for tracking and reporting of employee and labor relations cases.
☒	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 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.

12.2 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.