

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



**Privacy Impact Assessment
for the
MicroPact Employee Relations & Labor Relations Case
Management System (ERLRCMS)**

Reviewed by: John B. Owens II, 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

Catrina D. Purvis

Digitally signed by Katrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open
Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2017.06.06 10:44:15 -04'00'

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

Date

**U.S. Department of Commerce Privacy Impact Assessment
USPTO MicroPact Employee Relations & Labor Relations Case Management
System (ERLRCMS)**

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

Introduction: System Description

Provide a description of the system that addresses the following elements:

The response must be written in plain language and be as comprehensive as necessary to describe the system.

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

The MicroPact Employee Relation and Labor Relation Case Management System (ERLRCMS) 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 ER & LR divisions in accordance with the business rules defined in relevant workflows. The ERLRCMS is an application information system, and provides a business need to have one case management system that has business process flows built into it for both Employee Relations (ER) and Labor Relations (LR) organizations.

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

MicroPact Entellitrak software is used as the 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

Information will be shared internally with OHR and in some cases the USPTO Office of General Council (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

The legal authority to collect PII for this system comes from the Department of Commerce SORN: *Employees Personnel Files not covered by Notices of Other Agencies – COMMERCE/DEPT-18*.

Legal authority citations include the following, with all revisions and amendments: 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	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>	g. New Interagency Uses	<input type="checkbox"/>
b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input type="checkbox"/>	h. Internal Flow or Collection	<input type="checkbox"/>
c. Significant System Management Changes	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character of Data	<input type="checkbox"/>
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*	<input type="checkbox"/>	e. File/Case ID	<input checked="" type="checkbox"/>	i. Credit Card	<input type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input type="checkbox"/>
d. Employee ID	<input type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					
*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:					

General Personal Data (GPD)					
a. Name	<input checked="" type="checkbox"/>	g. Date of Birth	<input type="checkbox"/>	m. Religion	<input type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	h. Place of Birth	<input type="checkbox"/>	n. Financial Information	<input type="checkbox"/>
c. Alias	<input type="checkbox"/>	i. Home Address	<input type="checkbox"/>	o. Medical Information	<input type="checkbox"/>
d. Gender	<input type="checkbox"/>	j. Telephone Number	<input type="checkbox"/>	p. Military Service	<input type="checkbox"/>
e. Age	<input type="checkbox"/>	k. Email Address	<input checked="" type="checkbox"/>	q. Physical Characteristics	<input type="checkbox"/>
f. Race/Ethnicity	<input type="checkbox"/>	l. Education	<input type="checkbox"/>	r. Mother's Maiden Name	<input type="checkbox"/>

s. Other general personal data (specify):

Work-Related Data (WRD)			
a. Occupation	<input checked="" type="checkbox"/>	d. Telephone Number	<input checked="" type="checkbox"/>
b. Job Title	<input checked="" type="checkbox"/>	e. Email Address	<input checked="" type="checkbox"/>
c. Work Address	<input checked="" type="checkbox"/>	f. Business Associates	<input type="checkbox"/>
g. Salary <input type="checkbox"/>			
h. Work History <input type="checkbox"/>			
i. Other work-related data (specify):			

Distinguishing Features/Biometrics (DFB)			
a. Fingerprints	<input type="checkbox"/>	d. Photographs	<input type="checkbox"/>
b. Palm Prints	<input type="checkbox"/>	e. Scars, Marks, Tattoos	<input type="checkbox"/>
c. Voice Recording/Signatures	<input type="checkbox"/>	f. Vascular Scan	<input type="checkbox"/>
g. DNA Profiles <input type="checkbox"/>		h. Retina/Iris Scans <input type="checkbox"/>	
i. Dental Profile <input type="checkbox"/>		j. Other distinguishing features/biometrics (specify):	

System Administration/Audit Data (SAAD)			
a. User ID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>
b. IP Address	<input checked="" type="checkbox"/>	d. Queries Run	<input checked="" type="checkbox"/>
e. ID Files Accessed <input checked="" type="checkbox"/>		f. Contents of Files <input checked="" type="checkbox"/>	
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	<input checked="" type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>
Telephone	<input checked="" type="checkbox"/>	Email	<input checked="" type="checkbox"/>
Online <input type="checkbox"/>			
Other (specify):			

Government Sources			
Within the Bureau	<input checked="" type="checkbox"/>	Other DOC Bureaus	<input checked="" type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>
Other Federal Agencies <input checked="" type="checkbox"/>			
Other (specify):			

Non-government Sources			
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>
Third Party Website or Application		<input type="checkbox"/>	Commercial Data Brokers <input type="checkbox"/>
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	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	For administering human resources programs	<input type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input type="checkbox"/>
For litigation	<input checked="" type="checkbox"/>	For criminal law enforcement activities	<input checked="" type="checkbox"/>
For civil enforcement activities	<input checked="" type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input type="checkbox"/>	For employee or customer satisfaction	<input type="checkbox"/>
For web measurement and customization technologies (single-session)	<input type="checkbox"/>	For web measurement and customization technologies (multi-session)	<input type="checkbox"/>
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).

The information will be used to document, track and manage the flow 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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private sector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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:

<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input type="checkbox"/>		
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.*)

<input checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input checked="" type="checkbox"/>	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	
<input type="checkbox"/>	Yes, notice is provided by other means.	Specify how:
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

<input type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: 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.

<input type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: PII that is processed or stored by ERLR is pulled from internal USPTO personnel records. This information is needed for cases to be processed, and individuals cannot consent to any particular use of that information within the ERLR system.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Users can request to update information through a formal process through the USPTO OHR.
<input type="checkbox"/>	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.*)

<input type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: The ERLRCMS 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.
<input checked="" type="checkbox"/>	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>May 23, 2016</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	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).
<input type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input type="checkbox"/>	Contracts with customers establish ownership rights over data including PII/BII.
<input type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input type="checkbox"/>	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

<p>Operational Controls:</p> <p>1. Automated operational controls include securing all hardware associated with ER/LR 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 is controlled by physical locking mechanism including separate door locks, an alarm control contact monitored twenty-four (24) hours a day, a motion detector at each door and hallway and a video camera at each hallway.</p> <p>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.</p> <p>Technical controls:</p> <p>1. 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.</p>

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."

<input checked="" type="checkbox"/>	<p>Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i>:</p> <p>Employees Personnel Files not covered by Notices of Other Agencies – COMMERCE/DEPT-18.</p>
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input type="checkbox"/>	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.)*

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule: Yes. ERLRCMS files that relate to employee relation and labor relations are covered by the NARA GRS Schedule 1- Civilian Personnel Records, Item 30, Administrative Grievances, Disciplinary, and Adverse Action Files; Item 28, Labor Management Relations Records.
<input type="checkbox"/>	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:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	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	<input type="checkbox"/>	Overwriting	<input checked="" type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
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.

<input type="checkbox"/>	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input checked="" type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	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.)

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: Details information of employee work related data and system administration and audit data.
<input type="checkbox"/>	Quantity of PII	Provide explanation:
<input type="checkbox"/>	Data Field Sensitivity	Provide explanation:
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: Use of PII and work / system audit data in combination for tracking and reporting of employee and labor relations cases.
<input type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation:
<input checked="" type="checkbox"/>	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.
<input type="checkbox"/>	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required business process changes. Explanation:
<input checked="" type="checkbox"/>	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.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required technology changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.