U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment

Employee Relation and Labor Relation Case Management System (ERLRCSMS)

PTOC-031-00

May 11, 2015

Privacy Impact Assessment

This Privacy Impact Assessment (PIA) is a requirement of the Privacy Act of 1987 and OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.* A PIA documents the due diligence and oversight placed upon information associated with the project or system in question. Written from the System Owner's perspective for the American public, the PIA discloses what information is being collected, and how that information is protected. The intent is to build confidence that privacy information is secure, processes that utilize this information comply with Federal requirements, and more importantly, inform the privacy expectations of the American public.

The Privacy Threshold Analysis (PTA) is a separate artifact that must be completed prior to beginning this PIA. In many cases, the PTA will be the only required artifact to satisfy DOC privacy considerations.

SYSTEM DESCRIPTION

MicroPact Employee Relation and Labor Relation Case Management System (ERLRCSMS) system will replace the current Employee Relation(ER) and Labor Relation (LR) access database systems. Both OHR divisions shall use the same system, but they shall be able to control the sharing of records and documents between the ER & LR divisions in accordance with the business rules defined in relevant workflows. A significant design goal is to limit the use of e-mail as a mechanism to share documents.

MicroPact Entellitrack 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 business rules are based first on the Division (Employee Relations or Labor Relations) and then upon the type of action (ER) or upon an employee's labor union affiliation (LR). USPTO's Human Resource staff and managers are not represented by a union organization.

USPTO's non-management personnel are represented by three labor organizations – based upon type of position held within USPTO:

- Patent Office Professional Association (POPA)
- National Treasury Employees Union (NTEU) – 243
- National Treasury Employees Union (NTEU) – 245

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.

QUESTIONNAIRE

1. What information is collected (e.g., nature and source)?

   Employee Relation and Labor Relation Case Management system (ERLRCSMS) collect following PII information associated with USPTO employees: name, home address for letters, and as needed by case financial and medical data but only as it relates to the case items.

2. Why is this information being collected (e.g., to determine eligibility)?

   This information is being collected to provide evidentiary data as needed for ER/LR cases. This information may also be used to track the status of actions, recording data, and issuing reports.

3. What is the intended use of information (e.g., to verify existing data)?

   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.

4. With whom will the information be shared (e.g., another agency for a specified programmatic purpose)?

   Information will be shared internally with OHR and in some cases Office of General Council (OGC). Information will not be shared with external customers and business areas.

5. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent?

   For ER Cases - Information is obtained from the employee manager and NFC system of record as needed to fulfill basic needs of case generation; For LR Employees have to submit essential information in order to ensure that their claims can be processed as required. Employees can always refuse to provide information, but their claims will not be screened further.

6. How will the information be secured (e.g., administrative and technological controls)?

   The information is secured in accordance with the NIST 800-53, Revision 4 security controls. Secured technical architecture is incorporated into the system to prevent any unauthorized access to the personally identifiable data. Data is maintained in areas accessible only to authorized personnel and systems are password protected.

Management Controls:

1. *The ER/LR Application follows the USPTO SDLC review process to ensure that management controls are in place for the system. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the System Security Plan (SSP). The SSP specifically address the management, operational and technical controls that are in place, and planned, during the operation of the enhanced system.*

2. *The USPTO IT Privacy Policy and Personally Identifiable Data Extracts Policy are followed and implemented.*

Operational Controls:

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 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:

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.*

7. How will the data extract log and verify requirement be met?

The MicroPact USPTO ERLRCAMS system includes databases that store PII data related to USPTO Employee Relation and Labor Relations. As a result, MicroPact has implemented security controls to meet the data extract log and verify requirements identified in OMB M-07-16. Refer to the Audit and Accountability Controls (AU) in the latest MicroPact USPTO SSP for specific implementation details.

USPTO also requires following to protect sensitive and PII data:

a. *No extracts of sensitive data may be copied on to portable media without a waiver approved by DOC CIO. The request for a waiver must include specifics as to how the data and device are protected, how long the data will be maintained, and how the data on the device will be deleted when no longer required.*
b. *All laptop computers allowed to store sensitive data must have a full disk encryption*

c. *All remote access to public USPTO systems containing sensitive data must be encrypted. All remote access to internal USPTO systems containing sensitive data must fully comply with DOC Remote Access Policy requirements.*
d. *All flexiplace/telework agreements for working off site require that adequate data protection be in place.*

8. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?

   SORN exists "Employees Personnel Files not covered by Notices of Other Agencies-COMMERCE/DEPT-18" http://www.rdc.noaa.gov/foia/sorns/

9. Are these records covered by a record control schedule approved by the National Archives and Records Administration (NARA)?

   Yes. ERLRCAMS 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.

SIGNATORY AUTHORITY

Agreed: _____ 5 / 11 / 2015

Colleen Sheehan — Date

Information System Owner

Agreed: _____ 5 / 12 / 2015

John Pardun — Date

Senior Information Security Officer

Agreed: _____ 5 / 14 / 15

John B. Owens II — Date

Co-Authorizing Official

Agreed: _____ 5 / 19 / 2015

Frederick W. Steckler — Date

Co- Authorizing Official