U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment

Equal Employment System (EES)

PTOC-026-00

July 14th 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

The EES system is an Application information system, and provides support to the Office of Equal Employment Opportunity and Diversity business functions within the United States Patent and Trademark Office (USPTO). The EES supports all activities associated with the recruitment and management of USPTO personnel. The EES is composed of two (2) Information Systems that provide the following capabilities:

- Track and manage Equal Employment Opportunity (EEO) claims through the USPTO.
- The RA (Reasonable Accommodations) program housed in OEEOD includes processing requests and ensuring that RA requests are addressed promptly, thoroughly, and in strict compliance with the Equal Employment Opportunity Commission's (EEOC) regulations.

EES/RACMS is hosted externally outside of the USPTO network at the at the MicroPact, Inc., facilities at 44470 Chilum Place Bldg 1 Ashburn, VA 20147.
Following section describes the information systems/components that comprise the EES:

The Reasonable Accommodation Case Management System (RACMS)
The United States Patent and Trademark Office's (USPTO) policy is to fully comply with the reasonable accommodation requirements of the Rehabilitation Act of 1973, as amended, 29 U.S.C. sec. 791 et seq. (Act); 29 C.F.R. pts. 1614, 1630. The USPTO is committed to provide reasonable accommodations to employees and job applicants who are qualified individuals with disabilities, in order to ensure that they enjoy access to all employment opportunities at the USPTO. Reasonable accommodation is a cooperative, interactive process between the individual with a disability and the USPTO. The USPTO processes requests for reasonable accommodation and, where required by law, provides reasonable accommodations in a prompt, fair, and efficient manner.

The users of the *Reasonable Accommodation Case Management System (RACMS)* are USPTO employees and job applicants who are qualified individuals with disabilities, in order to ensure that they enjoy access to all employment opportunities at the USPTO. The system customer base consist of Office of Equal Employment Opportunity and Diversity Division (OEEOD) staff and Reasonable Accommodation (RA) deciding officials throughout the Agency's business units in the USPTO headquarters. The OEEOD staff, in particular members of the RA team, are the primary users of the electronic RA case management system. RACMS is designed to help the Office of Civil Rights staff to process requests for reasonable accommodation by collecting and maintaining data on accommodations requested and provided, and costs of each accommodation, for annual reporting purposes. The Reasonable Accommodation Case Management System is using the MicroPact COTS product entellitrak. The entellitrack RA Edition and entellitrack efile COTS software is an electronic case management and tracking system to track the RA requests. The USPTO requires a software package to track and manage the flow of RA requests through the RA process from the initial filing of a new RA request to the final resolution of the request.
The RACMS design uses entellitrak as a Web-based interface for the client side, and provides access to an Oracle 11G database.
The new system provides the following enhancements:
Specifically, the RACMS information system includes the following functionalities:

- Windows 7 Support

- Section 508 Web Accessibility Compliance
- Vendor Support
- Standard Reports
- Internal Controls
- Improve Security
- Electronic Filing
- One System for All Data

The Equal Employment Opportunity Case Management and Reporting System (EEOCMRS)

Equal Employment Opportunity Case Management and Reporting System (EEOCMRS) is an Information System that supports the Office of Equal Employment Opportunity and Diversity (OEEOD) of the United States Patent and Trademark Office. The mission of the EEOCMRS is to provide automated information support to the OEEOD in tracing and managing the flow of Equal Employment Opportunity (EEO) claims through the USPTO process. The EEOCMRS customer base consists of EEO staff in USPSTO Headquarters. OEEOD staff is the primary users of the system. The EEOCMRS system is using the MicroPact COTS product icomplaints.

QUESTIONNAIRE

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

   EEOCMRS:
   EEOCMRS manages and tracks Equal Employment Opportunity (EEO) cases. In order to process EEO cases EEOCMRS collects and maintains the contact's name, address, date of birth, social security number, telephone number, email address, and employment information.

   RACMS:
   The purpose of RACMS is to provide reasonable accommodations to employees and job applicants who are qualified individuals with disabilities, in order to ensure that they enjoy access to all employment opportunities at the USPTO. RACMS will be collecting personally identifiable information (PII) including names, date of birth, addresses, social security numbers, along with medical information associated with individuals with disabilities.

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

   EEOCMRS:
   This information is used by the EEOCMRS to manage and track EEO cases as well as to generate ad hoc and periodic reports.

   RACMS:
   This information is being collected to determine eligibility for claims for reasonable accommodations. This information is also used to manage and track claims including generating actions, tracking the status of actions, recording data, and issuing reports.

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

   EEOCMRS:
   The intended use of information is to support EEOCMRS role and mission.
   The information is used to manage and track EEO cases as well as to generate ad hoc and periodic reports. OEEOD staff members are allowed to search and verify EEO case records by complaint's first and last name, social security number, date of birth, case number etc.

   RACMS:
   The information will be used to track and manage the flow of reasonable accommodation requests through the RA process from the initial filing of a new RA request to the final resolution of the request. The information will also be used to process requests for reasonable accommodation by collecting and maintaining data on accommodations requested and provided, and costs of each accommodation, for annual reporting purposes.

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

EEOCMRS:
The information is shared within USPTO with authorized parties only. Some information obtained from the EEOCMRS is shared with the Equal Employment Opportunity Commission as required by regulation.

RACMS:
The information is shared within USPTO with authorized parties only. There is no other agency involved.

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?

EEOCMRS:
Contacts must submit essential information in order to ensure their cases can be processed in accordance with the governing regulations. Contacts can always refuse to provide information, but they risk their cases not being processed correctly or timely. Submission functions as consent for use of the information for the intended purpose. This information is necessary for the EEOCMRS to manage and track EEO cases. This information is shared within USPTO with authorized parties only.

RACMS:
All information requested is provided on a voluntary basis. Applicants must submit essential information to ensure that their qualifications for employment can be examined and verified during initial employment application. Applicants can always refuse to provide information, but their applications will not be screened further. Submission functions as consent for use of the information for the intended purpose. This information is further necessary and it is used by the EES (EEOCMRS) and Reasonable Accommodation (RA) deciding officials throughout the Agency's business units in the USPTO headquarters to process, manage, and track reasonable accommodation claims. This information is not shared with anyone outside the hiring process.

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

EEOCMRS/RACMS:
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 Micropact USPTO EES 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. Additional management controls include performing national agency check on all personnel, including contractor staff.*

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 EES in the Equinix 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.*

   Physical access authorizations at the entry and exit points to the facility where the Micropact systems reside are enforced. The main facility entry door is protected by the biometric hand scanner and panel for 5 digit pin associated with each individual with the access to the building. Once inside the building there is a security guard protected station. Equinix is a 24/7 guarded facility, before entering the Equinix lobby all authorized MicroPact team members and visitors must present valid government issued ID and sign in prior to being granted access into the facility past the lobby. Visitors need to be escorted by the authorized individuals. Once this is done all authorized users and visitors need to go through the second physical access included man door traps. Once individual go through man traps there are two additional doors that require biometric hand scanner and a 5 digit oit before reaching actual MicroPact cage that also requires biometric hand scans and 5 digit PIN assigned to each authorized individual. Equinix logs all entry and exit from the facility. All points of access and exit require biometric hand scan and pin or assistance of Equinix guards.

   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?

   EEOCMRS/RACMS:
   The Micropact USPTO EEOCMR/RACMS S system includes databases that store PII data related to USPTO EEO cases. 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 EEOCMRS 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?

EEOCMRS:
The existing system of records covers the information residing in the database. These include: COMMERCE/DEPT-18, Employee Personnel Files Not Covered by Notices of Other Agencies.

RACMS:
SORN exists "Employees Personnel Files not covered by Notices of Other Agencies-COMMERCE/DEPT-18"

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

EEOCMRS:
No. GRC 20 allows agency determination that certain electronic records are authorized for erasure of deletion when they are no longer needed for administrative, legal, audit, or other operational purposes. Electronic records that represent hard copy records can be deleted after expiration of the retention period authorized for the hard copy records.

RACMS:
Yes. RACMS files that relate to reasonable accommodation request are covered by the NARA GRS Schedule 1. Civilian Personnel Records, Item 24, Reasonable Accommodation Request Records.

SIGNATORY AUTHORITY

Agreed: _____ 7/15/15

Tamika Beverly — Date

Information System Owner

Agreed: _____ 7/21/15

John Pardun — Date

Senior Information Security Officer

Agreed: _____ 7/24/15

Tony Chiles for John B. Owens II — Date

Co-Authorizing Official

Agreed: _____ 7/24/15

Bismarck Myrick — Date

Co-Authorizing Official