Version Number: 01-2015

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

Privacy Impact Assessment
For the
Equal Employment System (EES)

Reviewed by: John B. Owens II, Senior Agency Official for Privacy

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

____

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

Version Number: 01-2015

U.S. Department of Commerce Privacy Impact Assessment
USPTO EES

Unique Project Identifier: PTOC-026-00

<u>Introduction</u>: 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 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.

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

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.

(c) any information sharing conducted by the system

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

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system.

Confidentiality	**- Moderated**
Integrity	**- Moderated**
Availability	**- Moderated**

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 privacy risks do not change.

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): **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.					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: **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.

*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: **N/A**

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).

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.

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:
☒	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: ______________________________.	
☐	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:

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:

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:
☒	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.)*

☐	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:
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): __________________ ☐ 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.

Operational Controls: 1. Automated operational controls include securing all hardware associated with BITS 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.

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)*:
☐	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: 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.* 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.
☐	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:
☒	Quantity of PII	Provide explanation:
☒	Data Field Sensitivity	Provide explanation:
☒	Context of Use	Provide explanation:
☒	Obligation to Protect Confidentiality	Provide explanation:
☒	Access to and Location of PII	Provide explanation:
☐	Other:	Provide explanation:

<u>Section 12</u>: 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.