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

Privacy Impact Assessment
for the
MicroPact Equal Employment System / Reasonable Accommodation Case Management System (EES/RACMS)

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

Jennifer Goode   06/24/2021
Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer   Date

U.S. Department of Commerce Privacy Impact Assessment
USPTO MicroPact Equal Employment System / Reasonable Accommodation Case Management System (EES/RACMS)

Unique Project Identifier: PTOC-026-00

Introduction: System Description

The EES/RACMS 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/RACMS supports all activities associated with the recruitment and management of USPTO personnel.

(a) Whether it is a general support system, major application, or other type of system
EES/RACMS is a major application system.

(b) System location
EES/RACMS system is located at 44470 Chilum Place Bldg. 1, Ashburn, VA 20147. EES/RACMS has an alternate hot site located at 180 Peachtree Street, Atlanta, GA at an Equinox Atlanta Data Center.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
The EES/RACMS applications are hosted by the MicroPact Software as a Service (SaaS). Network and Security Infrastructure (NSI) and Enterprise Software Services (ESS) – Role Based Access Control (RBAC) facilitate the communication between USPTO and MicroPact.

(d) The way the system operates to achieve the purpose(s) identified in Section 4
EES administrators, managers and specialists access the application through a web-based portal to create, update, collect, capture, assign, generate and close complaints and cases. RACMS administrators, managers, specialists, reviewers, business leads and officials access the application through a web-based portal to process and manage requests. This is done by collecting and maintaining accommodation requests, and cost of accommodation.

(e) How information in the system is retrieved by the user
USPTO OEEOD staff access the system via the USPTO intranet and web-based portal. Users are able to retrieve and transmit information from the systems after being authenticated.

(f) How information is transmitted to and from the system:
Users access the EES and RACMS systems via the USPTO intranet and a web-based portal hosted by the MicroPact SaaS. The transmission of information between USPTO and MicroPact is encrypted.

(g) Any information sharing conducted by the system
    Information is shared within the bureau based on business needs.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
    5 U.S.C. 301; 42 U.S.C. 2000e et seq.; 29 U.S.C. 206; 29 U.S.C. 621 et seq.; 29 U.S.C. 701 et seq.; 29 U.S.C. 791 et seq.; 42 U.S.C. 2000ff et seq.; E.O. 13164, E.O. 11478; 41 U.S.C. 433(d); 29 CFR Part 1614; AAO 214-01, and AAO 214-02.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system
    The 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.)

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):					

☐   This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

☒   This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017).

☐   This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later).

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*	☐	f. Driver's License	☐	j. Financial Account	☐
b. Taxpayer ID	☐	g. Passport	☐	k. Financial Transaction	☐
c. Employer ID	☐	h. Alien Registration	☐	l. Vehicle Identifier	☐
d. Employee ID	☒	i. Credit Card	☐	m. Medical Record	☐
e. File/Case ID	☒				

n. Other identifying numbers (specify):

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

General Personal Data (GPD)

a. Name	☒	h. Date of Birth	☒	o. Financial Information	☐
b. Maiden Name	☐	i. Place of Birth	☒	p. Medical Information	☒
c. Alias	☐	j. Home Address	☒	q. Military Service	☐
d. Gender	☒	k. Telephone Number	☒	r. Criminal Record	☐
e. Age	☒	l. Email Address	☒	s. Physical Characteristics	☒
f. Race/Ethnicity	☒	m. Education	☐	t. Mother's Maiden Name	☐
g. Citizenship	☐	n. Religion	☒		

u. Other general personal data (specify):

Work-Related Data (WRD)

a. Occupation	☒	e. Work Email Address	☒	i. Business Associates	☐
b. Job Title	☒	f. Salary	☐	j. Proprietary or Business Information	☐
c. Work Address	☒	g. Work History	☐	k. Procurement/contracting records	☐
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	☐		

l. Other work-related data (specify):

Distinguishing Features/Biometrics (DFB)

a. Fingerprints	☐	f. Scars, Marks, Tattoos	☐	k. Signatures	☐
b. Palm Prints	☐	g. Hair Color	☐	l. Vascular Scans	☐
c. Voice/Audio Recording	☐	h. Eye Color	☐	m. DNA Sample or Profile	☐
d. Video Recording	☐	i. Height	☐	n. Retina/Iris Scans	☐
e. Photographs	☐	j. Weight	☐	o. Dental Profile	☐

p.	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	☒	f. 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   Describe how the accuracy of the information in the system is ensured.

USPTO OEEOD administrators and specialists have the ability to modify user information and work with employees, contractors and applicants to validate the accuracy of the information. The data is stored within a database and data is backed-up continually.

2.4   Is the information covered by the Paperwork Reduction Act?

☐	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.

☒	No, the information is not covered by the Paperwork Reduction Act.

2.5 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			
For a Computer Matching Program	☐	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): Used to determine reasonable accommodation eligibility.			

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).

> EES: PII used by the system will support USPTO compliance with Equal Employment Opportunity (EEO) laws for employees, contractors and applicants.
>
> RACMS: PII used by the system will support USPTO compliance with reasonable accommodation requirements for employees, contractors, members of the public such as applicants and medical providers.

5.2   Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

> Foreign governments and insider threats are the predominant threat to the systems privacy and data leakage. USPTO has implemented National Institute of Standards and Technology (NIST) security controls (encryption, access control, auditing) and selected a Federal Risk Authorization Management Program (FedRAMP) authorized cloud provider to reduce the risk. Mandatory IT Awareness and role-based training are required for staff that have access to the system and address how to handle, retain and dispose of data. Contract terms between the cloud provider and USPTO provide guidance on how data should be handled, retained and disposed.

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 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

☐	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☒	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☐	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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 systems connect with ESS – RBAC; encryption, auditing, physical and logical access controls are in place to prevent leakage.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 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): • Applicants applying for position			

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: http://www.uspto.gov/privacy-policy	
☒	Yes, notice is provided by other means.	Specify how: • Employees are requested to complete the Request for Reasonable Accommodation Medical Provider Statement form
☐	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: • Information is provided voluntarily; however, not providing the information would result in case not being able to be processed or delayed.
☐	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: • Information is provided voluntarily; however, not providing the information would result in case not being able to be processed or delayed.
☐	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: • 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:

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 EES/RACMS MicroPact and USPTO Administrator conduct monthly audits of the system, to include when and by whom the system was accessed and what info was updated, changed corrected, etc.
☒	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): ___7/25/2020_____ ☐ 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 (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish DOC 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. *(Include data encryption in transit and/or at rest, if applicable).*

Automated operational controls include securing all hardware associated with EES/RACMS 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   Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

☒   Yes, the PII/BII is searchable by a personal identifier.

☐   No, the PII/BII is not searchable by a personal identifier.

9.2   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, number, and link. *(list all that apply)*: Employees Personnel Files not covered by Notices of Other Agencies – COMMERCE/DEPT-18. Equal Employment Opportunity in the Federal Government Complaint and Appeal Records-- EEOC/GOVT-1
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, this system is not a system of records and a SORN is not applicable.

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: NARA GRS Schedule 2.3, Item 20. Reasonable Accommodation Case Files. EES: NARA GRS Schedule 2.3 Items 110 & 111 EEO discrimination complaint case files, 120 Records documenting contractor compliance with EEO regulations
☐	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 Level

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. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

☐	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 level. *(Check all that apply.)*

☒	Identifiability	Provide explanation: • Detailed information of employee work related data and system administration and audit data separately or in combination may provide a detailed private individual profile.
☒	Quantity of PII	Provide explanation: • Approximately ten years of PII data reside on the system with about 100 cases per year. There is a need to ensure the confidentiality of the approximate 1,000 PII data residing on the system.
☒	Data Field Sensitivity	Provide explanation: • The presence of medical information along with sensitive PII could result in potential harm to individuals if not used in accordance with its intended use.
☒	Context of Use	Provide explanation: • Use of PII and work/system audit data in combination for tracking and reporting of equal employment or accommodations cases may provide a detailed private individual profile.
☒	Obligation to Protect Confidentiality	Provide explanation: • Based on the data fields input in to the 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   Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Foreign entities and insider threats are the predominant threats to the information collected and its privacy. Security controls following FedRAMP and NIST guidance were implemented to deter and prevent threats to privacy.

12.2   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.

12.3   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.