



UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

USPTO Privacy Impact Assessment Statement
Human Resources Management Support System

Unique Investment Identifier: 00651010801800900403251

Prepared by: Robert Rathbun, Office of the Executive for System Development and
Maintenance Services, OCIO

Reviewed by: David J. Freeland, Chief Information Officer



UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

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

Information collected from the public includes that under OMB collection number 0651-0042, Electronic Application for Patent Examiners-Job Application Rating System (JARS).

The information to be collected by the system includes personnel information about potential employees to include personal information about educational attainment, background and work history. USPTO employee payroll transactions; awards information, employee relations information, labor relations information, position description and management information are also collected.

The data sources are applicants for enlistment and scoring comments made by screeners and managers.

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

The collection of the information facilitates the hiring of entry-level patent examiners and is essential to begin the evaluation and interview process.

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

The information is used to perform initial evaluations of the fitness of applicants for employment at the USPTO and for supporting the decision-making activities of managers and analysts in the USPTO business areas.

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

The information is shared within USPTO with authorized parties only, specifically those performing evaluation, interviewing and hiring. 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 individuals can grant consent?

Applicants must submit essential information to ensure that their qualifications for employment can be examined and verified. Applicants can always deign to provide information, but their applications will not be screened further. Submission is consent for use of the information for the intended purpose. This information is not shared with anyone outside the hiring process.



UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

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

Management Controls:

The USPTO uses the Life Cycle review process to ensure that management controls are in place. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the Security Plan, which is a document prepared during the Concept Phase of the project's life cycle. The Security Plan specifically addresses 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.

Operational Controls:

Operational controls include securing all hardware associated with this investment in the USPTO Data Center. The Data Center is controlled by access card entry, and is manned by a uniformed guard service to restrict access to the servers, their operating systems and databases. Contingency planning has been prepared for the data center. Backups are performed on the processing databases. Backups are stored on tape and are secured off-site. Additional operation controls include: (1) Logical edit checks to ensure proper sequence of actions; (2) Physical terminal identification; (3) Database UserID; (4) Restricted data display, as required; and (5) Restricted access.

Technical Controls:

Technical Controls include password authentication (userid and passwords). At the client PCs, access is managed through a password authentication (userid and password) based on certification. The security form must be signed by a supervisor, and requires additional approval from Human Resources based on a justification of need.

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

No, there is no new system of records being created. Existing system of records cover the information residing in the data base. These include: COMMERCE/DEPT-18, Employee Personnel Files Not Covered by Notices of Other Agencies.



UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

Human Resources Management Support System

UII: 00651010801800900403251

[Signature] /s/
RW Rathbun 2-14-2006
Prepared by _____ Date

[Signature] /s/
Joyce English 3-23-06
Approved _____ Date
Joyce English
Director, Systems Development and Maintenance

I have reviewed and approve the attached Privacy Impact Assessment document(s).

[Signature] /s/
David J. Freeland 6-29-06
David J. Freeland _____ Date
Chief Information Officer

cc:

Griffin Macy, Deputy Chief Information Officer
David Larsen, Acting Director, Enterprise IT and Security Management