



UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

USPTO Privacy Impact Assessment Statement

Patent Automation System

Unique Investment Identifier: 00651010301800400105012

Prepared by: Will Atkinson, Director, Patent Reengineering Systems Division, 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 numbers 0651-0016, Rules for Patent Maintenance Fees; 0651-0030, Patent Processing (Updating); and 0651-0031, Initial Patent Applications.

Application filing: Bibliographic data (Inventor name, Inventor address, Citizenship, and Correspondence address) are collected from the applicant or applicant's legal representative.

Payment related data (Credit Card and Deposit Account information) are collected to cover application fees. (Payment related data is covered under the Revenue and Accounting Management (RAM) Privacy Impact Assessment available under separate cover.)

Application access: Name and correspondence address of individuals who desire access from external sources to their own data is collected from the applicant or applicant's legal representative. Once publication has occurred, some of the data is publicly available.

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

Information is required to obtain or retain benefits.

Application filing: Name and address of Inventor is collected to uniquely identify the inventor and is required as part of Patent Rights determination under the Patent statutes. Correspondence address is collected to facilitate communications with the applicant or applicant's legal representative.

Application access: Name and correspondence address of individuals who desire access from external sources to their own data is collected to implement authentication and verification of access (via PKI High-level digital certificate) with the applicant or applicant's legal representative.

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

Application filing: The information becomes part of the official record of the application and is used to document Inventor location and nationality and for communications.

Application access: To implement authentication and verification of an individual's access rights to his own data from outside of the USPTO system firewalls.



UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

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

During processing the information is passed through to various internal Automated Information Systems for processing at the USPTO. The information is not routinely shared with other agencies before publication. During National Security Interest review, a subset of applications is shared with the Department of Energy (DOE) and the Department of Defense (DOD) as part of a statutorily mandated process. In addition, in the course of prosecution, the Department of Justice (DOJ) or judicial court personnel may review a small number of applications.

After the application has been published, the information is part of the public record. A member of the public may request a copy of the application file. The Office file containing the application and all correspondence leading up to issuance of the patent is made available in the Files Information Unit for inspection by anyone, and copies of these files may be purchased from the Office.

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?

Application filing: The information must be provided in order for the USPTO to process the patent application. The information becomes part of the official record of the application. See 35 U.S.C. 131

After filing an application, applicants may choose to electronically submit address changes to the Electronic Business Center (EBC) for Patents. Electronic address changes however, are voluntary, and may also be submitted via certified mail.

Application access: The election of on-line access functionality is voluntary.

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

Management Controls:

According to 35 U.S.C. Section 122 USPTO must maintain patent applications in confidence. In order to comply with this law, the USPTO requires secure communication between the USPTO and applicants and practitioners.

As a result, the USPTO has implemented several electronic commerce projects that promote secure communications, including instituting rules to protect applicants when they file patent applications electronically and providing electronic access to pending patent applications to



UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

authorized persons via the Patent Application Information Retrieval (PAIR) system. USPTO has implemented public key infrastructure technology to provide the security of these systems. A PKI digital certificate is necessary to ensure the security of the electronic transmission of patent applications and is used to establish a Secure Socket Layer connection with the USPTO server for secure transmission of patent application information.

Technical Controls:

When filing a new utility or provisional patent application, users may use the low-level digital certificate to submit a new patent application to the Electronic Filing System (EFS). The low-level digital certificate is compatible with the public key infrastructure that is implemented by the USPTO and allows secure communications between applicants and the USPTO. Low-level digital certificates may only be used to file new utility and provisional submissions.

High-level digital certificates issued by the USPTO require an approval process. USPTO will also provide a version of Entrust Direct security software that is custom-made for the USPTO and is used to create the high-level digital certificate. Entrust Direct is compatible with the public key infrastructure that is implemented by the USPTO and enables secure communications among individual applicants, practitioners, and the USPTO.

A high level PKI certificate is recommended and allows the applicant to access their application information in private PAIR and also allows all six filing types to be submitted. PKI digital certificates may be obtained by contacting the Electronic Business Center (EBC) for Patents.

Operational Controls:

All USPTO Automated Information Systems (AISs), which process unpublished patent application data, have undergone a formal IT Security Certification & Authorization process and have been approved for operation with the requisite and appropriate security controls in place in conformance with Federal IT Security Policy.

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 Systems of Records cover the information residing in the data bases. These include the COMMERCE/PAT-TM-7, Patent Application Files.



UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

Patent Automation System UII: 00651010301800400105012

/s/ William R. Atkinson
Prepared by William R. Atkinson Date 2/14/06

/s/ Joyce English
Approved Joyce English Date 3/23/06
Joyce English
Director, Systems Development and Maintenance

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

/s/ David J. Freeland
David J. Freeland Date 6-29-06
David J. Freeland
Chief Information Officer

cc:

Griffin Macy, Deputy Chief Information Officer

David Larsen, Acting Director, Enterprise IT and Security Management