U.S. PATENT AND TRADEMARK OFFICE

Patent eGov

Unique Investment Identifier: 006510103018004001050 12

USPTO Privacy Impact Assessment Statement

Prepared by: Brooks Hunt, Director, Office of Technical Plans and Policy
Reviewed by: Ron Hack, Acting Chief Information Officer

U.S. Patent and Trademark Office

USPTO Office of the Chief Information Officer (OCIO)

Patent e-Government Privacy Impact Assessment (PIA)

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

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 is collected from the applicant or applicant's legal representative.

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 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 inside of the USPTO system firewalls.

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

During the Pre-Grant or processing period 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 are shared with the

Department of Energy (DOE) and the Department of Defense (DOD) as part of a statutorily mandated process. Also, in the course of prosecution, a small number of applications may be reviewed by the Department of Justice (DOJ) or judicial court personnel.

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 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 electronicically 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)?

According to 35 U.S.C. Section 122 USPTO must maintain patent applications in confidence. In order to comply with this law, the USPTO distributes software that supports secure communication among the USPTO, 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 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.

When filing a new utility or provisional patent application, users may use the low-level digital certificate that is built in to ePAVE, the tool used 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.

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

A system of records has been created: Patent Application Files--COMMERCE/PAT-TM-7. This system is broken down into three subsystems relating to the status of the files: Pending, Abandoned, and Patented. Individuals covered by the system include: Applicants for patent, including inventors, legal representatives for deceased or incapacitated inventors, and other persons authorized by law to make applications for patent. Categories of records in the system include: Oath or declaration of applicant including name, citizenship, residence, post office address and other information pertaining to the applicant's activities in connection with the invention for which a patent is sought. Routine uses of records maintained in the system, including categories of users and the purposes of such uses: a.) Information concerning these records is provided outside the Office only upon authorization of the applicant or owner of the application or when necessary to carry out the provisions of any act of Congress or in such special circumstances as may be determined by the Commissioner, e.g. files referred for secrecy order determination under 35 U.S.C. 181. b.) Same as a., except where application is referred to in a U.S. Patent, in which case the record is open to public inspection. c.) Records are open to public inspection. Retrievability: Pending and Abandoned applications are filed by serial number, cross-indexed to name of applicant. Patented applications are filed by patent number, cross-indexed to name of applicant. The information is stored on various media: paper files, microfilm reels, index card files, and magnetic storage media, such as various internal USPTO Automated Information systems (i.e., Patent Application Location and Monitoring (PALM) system, Image File Wrapper (IFW) system, and Revenue and Accounting Management (RAM) system).