U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment

Global Patent Solutions (GPS) System

PTOC-024-00

September 2015

Privacy Impact Assessment

This Privacy Impact Assessment (PIA) is a requirement of the Privacy Act of 1987 and OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.* A PIA documents the due diligence and oversight placed upon information associated with the project or system in question. Written from the System Owner's perspective for the American public, the PIA discloses what information is being collected, and how that information is protected. The intent is to build confidence that privacy information is secure, processes that utilize this information comply with Federal requirements, and more importantly, inform the privacy expectations of the American public.

The Privacy Threshold Analysis (PTA) is a separate artifact that must be completed prior to beginning this PIA. In many cases, the PTA will be the only required artifact to satisfy DOC privacy considerations.

SYSTEM DESCRIPTION

The Global Patent Solutions (GPS) Automated Information Management System (GPS) is located at GPS headquarters in Scottsdale, AZ and is comprised of a Local Area Network (LAN), network devices, web, application, workstations, and additional network support devices. GPS is a major system that provides the following functions: anti-virus, domain controller, DNS, web, application, Remote Desktop Services and file/print services.

GPS includes HP thin-client workstations that operate on Windows 7 Professional operating systems. There is also a single Windows 8 tablet deployed, with more deployments to GPS management possible in the future. Applications available on the workstations include Abacus Law, Microsoft Office Suite, Adobe Acrobat Standard, Microsoft Internet Explorer, Google Chrome, and Mozilla Firefox. Network devices include application and file servers, firewalls, routers, switches, and storage devices. The network server operates on Microsoft Windows 2008 R2 and Windows 2012 Server Standard in the virtual environment on VMWare ESX server 5.1.0.

USPTO data is received through a secured file transfer using Tumbleweed and stored on a file server in GPS. This connection is encrypted using Secured Socket Layer (SSL). The data is transmitted to and stored at the Research Analysts' workstations. The Research Analysts perform work with the data at their workstations. When the work is completed, work deliverables are transmitted back and stored on the same file server. When the work deliverables are finally approved by a Search Approval Official, the Search Manager transmits the work deliverables via the same secured file transfer back to the USPTO. Data is backed up Monday through Thursday, with full backups running on Friday using Commvault backup software. Copies of data are also made with VSS snapshots that are taken every two hours from 4 AM until 10 PM daily. Files are also replicated with DFS between two servers located at GPS.

USPTO data is received from the USPTO and stored on a separate drive directory on a file server. Windows Active Directory controls access to the drive with user privileges.

The communication link from GPS to USPTO is managed by USPTO. Inbound and outbound data on the GPS network is limited only to the resources, protocols, and ports that are required to support the mission of the GPS system under the terms specified in the USPTO contract. Per the GPS IT Security Policy and Security Control Procedures document, connection to any internal GPS network or system must be approved by the Information System Security Officer. All such connections must be limited only to the resources and services required to perform the stated requirements of the connection.

GPS office space is located in Scottsdale, AZ. The facility includes the following physical protection mechanisms: locks and electronic card access. All network equipment besides the workstations is stored in a locked communication room. Research Analysts perform PCT searches and write opinions from this facility or remotely through an SSL VPN connection. The work deliverables are received from the USPTO via the Internet and through a workstation equipped with Tumbleweed and saved to a file server located in this facility. The facility has computer workstations for each of the Research Analysts. The workstations at this location are connected to the SCDDC-01 server which functions as the GC, DNS, and DHCP server. The MGMT-01 server functions as the DNS, DC, and print server, and also hosts PhoneFactor. The PCT searches and written opinions are submitted to the USPTO through a workstation equipped with Tumbleweed and then via the Internet.

Remote Users

Research Analysts who work remotely will connect to the GPS system using a secure link using SSL and/or a VPN connection and the users will have to authenticate themselves with the system using their Window Active Directory username and password. They will then gain access the GPS system using Remote Desktop Services (RDS) that run on our server located in Scottsdale, AZ. When working in the RDS environment the remote user is presented with a virtual desktop that is actually running on the GPS server in Scottsdale, AZ and not running

on their local machine. The RDS environment will provide the users with various applications to perform the PCT search and examination procedures such as Microsoft Office Suite, Adobe Acrobat and Microsoft Internet Explorer. The RDS will also provide access to the file server where the user can view PCT applications and complete the various forms to be submitted to the USPTO. With this environment the USPTO PCT files are never actually sent or stored on the remote user's local machine but instead they always reside on the GPS server. Some restrictions on RDS remote users include not allowing any files to be downloaded, printed or store to any internal or external storage device of the remote workstation. If the remote user's workstation is ever lost, stolen or damaged, no confidential files will be located on that remote workstation. All files reside on GPS servers in Scottsdale, AZ.

QUESTIONNAIRE

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

   Patent applications could include applicants' names and addresses. GPS receives patent applications directly from the United States Patent and Trademark Office (USPTO).

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

   This PII data is collected by the USPTO and provided to authorized contractors to enable identification of the inventor throughout the patent application process.

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

   The PII data contained in the patent application uniquely identifies the inventor.

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

   Global Patent Solutions (GPS) does not share any information with other agencies, individuals, or organizations. The information provided by USPTO is used by GPS to conduct searches under the PCT by internal personnel only.

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 can individuals grant consent?

   The patent application documents received by GPS are obtained directly from USPTO. This process does not provide opportunity for individuals to decline to provide their names, addresses, or any other PII data that might be provided on the patent application received from USPTO. Individuals are not able to decline or consent to any particular use of the patent application PII data.

   Under the terms and conditions of the PCT, USPTO serves as a Receiving Office, an International Searching Authority, and an International Preliminary Examination Authority for international patent applications filed in accordance with the PCT. A single filing of an international application is accompanied with a search report and a written opinion regarding the patentability of the invention which is the subject of the application. Applicants are required to provide the information to the Receiving Office, in this case the USPTO, as part of the application process.

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

   The information received from and sent to the USPTO is transmitted using a secure protocol. Patent applications are stored on servers configured to limit access to data to authorized, internal users only.

7. How will the data extract log and verify requirement be met?

No individually identifiable payment-related information or other PII is processed by GPS. The address and other contact information are collected by the system for correspondence purposes. This would not be considered a data extract and therefore the data extract log and verify requirement is not applicable to the system.

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

   No.

9. Are these records covered by a record control schedule approved by the National Archives and Records Administration (NARA)?

   Not Applicable. USPTO is in the process of identifying the General Records Schedules (GRS). The COTR will be responsible for determining the correct GRS for this system.

SIGNATORY AUTHORITY

Agreed: _____ 9/3/2015

Blaine Copenheaver — Date

Information System Owner

Agreed: _____ 9/9/2015

John Pardun — Date

Senior Information Security Officer

Agreed: _____ 9/14/15

John B. Owens II — Date

Co-Authorizing Official

Agreed: _____ 10/20/15

Drew Hirshfeld — Date

Co-Authorizing Official