U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment

Enterprise Software Services

PTOI-020-00

July 8, 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

EDS

Enterprise Directory Services (EDS) 2.0 is a standards-based authoritative data source for user credentials that provides authorized USPTO personnel with single sign-on access to automated information systems (AISs) throughout USPTO. EDS ensures information consistency and provides a capability for role-based access control (RBAC). EDS supports USPTO employee domain authentication, data access, and connectivity to e-mail as well as other internal applications.

EDS 2.0 defines a structured framework for mapping user roles to security attributes within the internal directory service. EDS also provides extensible communications and identity management by synchronizing with a variety of platforms, and publishing the synchronized information to the internal directory through a meta-directory service. The identity management directory service manages users' digital identities, credentials and groupings throughout the lifecycle of their membership of an enterprise computer system, and it facilitates identity synchronization, certificate management, user password resets and user account provisioning from a single interface.

RBAC

The Role Based Access Control (RBAC) system provides the capability, in both development and production, for integration of newly deployed next generation (NG) systems, through an authentication and authorization framework that will allow secure, on-demand access to its managed applications. This solution will process access requests both from users inside the PTONet, as well as from users anywhere in the world via the Internet. In addition, RBAC will enable USPTO and its partners, with the predetermined role based authorization, to access each other’s systems within this construct.

The key to this authentication and authorization methodology is the integration of the SSO capability that allows a user to log on securely and seamlessly to many applications, without having to authenticate multiple times. In addition, the overlay of RBAC – the means to control to what and where a user has access within an application based on an assigned role – will allow the functions and data within applications to be very specific and focused based on the needs of the individual user.

PTOES

The PTO E-mail System is integrated with the EDS infrastructure, and provides electronic mail, calendar, contacts and tasks, office chat and messaging, support for mobile and web-based access to information; and support for data storage. This is a legacy subsystem that remains in production for redundancy, although all mailboxes have been migrated to the cloud-based Email as a Service (EaaS) subsystem.

EaaS

Email as a Service (EaaS) leverages a FedRAMP-authorized cloud-based platform to provide electronic mail, calendar, contacts and tasks; support for mobile and web-based access to information; and support for data storage. All USPTO mailboxes are now hosted in the cloud.

SEP

SEP provides the functionality to detect and eradicate known viruses from hard drives. The software manually or automatically scans for viruses and downloads updated virus pattern files.

ESPS

Enterprise Share Point Services (ESPS) is an application information system that facilitates collaboration, provides full content management, implements business processes, and provides access to information essential organizational goals and processes. It provides an integrated platform to plan, deploy, and manage intranet, extranet, and Internet applications across and beyond the enterprise.
USPTO is currently in the process of migrating SharePoint sites to a cloud based solution, to improve application performance, document retrieval response time, enhance access control and separation of duties, increase system redundancy, improve backup and recovery capabilities, and facilitate integration with other USPTO systems.

PTOFAX provides external (non-USPTO) users the ability to send fax documents to the USPTO and USPTO personnel the ability to send fax documents to external users from their USPTO Enterprise Desktop Platform (EDP) computers using the PTOFAX client software and via the Enterprise Remote Access (ERA) Secure External Access System (SEAS) by launching the PTOFAX client application. The PTOFAX system provides this service by utilizing standard hardware and a commercial off-the-shelf (COTS) product.
The PTOFAX system consists of several hardware and software components. The current solution is a high-availability design that provides server redundancy and offers 24 hours a day, 7 days a week (24 x 7) operation for USPTO “Official” and “Non-official” fax requests. PTOFAX can also maintain an 18-month data repository for online search and retrieval for the USPTO “Official Fax” account.

QUESTIONNAIRE

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

a) EDS – The following pieces of user data are captured from internal USPTO employees and contractors and stored in EDS: First name, last name, middle name, organization (department), work telephone number(s), USPTO e-mail address and physical addresses of USPTO work locations.

b) RBAC – For internal USPTO users, the following attributes are propagated to and stored in RBAC from EDS for internal users: First name, last name, middle name, organization, work telephone number(s), and e-mail address.

For external (non-USPTO) users, the following information is collected via MyUSPTO and stored in RBAC: First name, last name, telephone number (work, cell, or home), e-mail address, physical address, and security question answers to at least three of the following questions:

- Father's middle name,
- First pet's name,
- All-time favorite sports team,
- High school mascot,
- Name of first school,
- City/town of birth,
- Favorite comic book hero,
- Favorite hobby,
- Mother's middle name,
- Color of first pet
- Year the individual met his/her spouse/partner, and
- Number of bedrooms in the individual's house/apartment.

c) EaaS - Personally Identifiable Information (PII) is not collected. This system provides USPTO email services stored in the cloud. Electronic messages might contain sensitive information or documentation. Emails transmitted to and stored in the cloud leverage FIPS 140-2 compliant encryption mechanisms.

d) ESPS - This system does not collect any PII. However, SharePoint serves as a repository that is utilized throughout the entire USPTO organization and may contain documents with sensitive information.

e) PTOES - This system does not collect any PII. This system provides USPTO email services managed on-premise. E-mails sent through the USPTO Exchange System might contain sensitive information or documentation. While in transmission and stored on premise, emails are protected with FIPS 140-2 approved encryption algorithms.

f) PTOFAX - Not applicable. This system does not collect any PII.

g) SEP - Not applicable. This system does not collect any PII.

2. **Why is this information being collected (e.g., to determine eligibility)?** The information is collected to identify the users and partners when authenticating through the network. User credentials are managed through EDS for internal users and through MyUSPTO for external users, and integrated with RBAC. This information is being collected to verify the identity of the users leveraging the USPTO services with which EDS and/or RBAC are integrated.

3. **What is the intended use of information (e.g., to verify existing data)?** The information is intended to identify the users and partners when authenticating through the network. While being identified, EDS (integrated with the RBAC system) will allow users to access USPTO's network and various systems through Single Sign-On. The security questions collected by MyUSPTO and stored in RBAC are to be used by the USPTO Service Desk to verify the identity of customers interacting with MyUSPTO.

4. **With whom will the information be shared (e.g., another agency for a specified programmatic purpose)?** This information is only to be used by the USPTO for the purpose of identity verification, to allow authorized users to authenticate to USPTO systems and/or applications. The information will not be shared with any other government agencies. PII will only be shared externally if authorized by the individual or mandated by law.

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?** Sensitive personal information is required for the processing of the USPTO PTONet accounts managed through the EDS and RBAC systems. As part of USPTO's onboarding process, internal employees and contractors consent to providing the above referenced information, for the primary purpose of acquiring network privileges that will allow them to access their business email inboxes, repositories, application systems according to their business needs and to obtain physical access by assigning badge or PIV card access to their accounts. Applicants are notified that if the information is not provided to USPTO, they will not be able to access the USPTO network to perform their job duties.

   In order to use MyUSPTO, external customers must create accounts via an online self-registration process. As part of the first step in the registration process, external users must click on a checkbox that explicitly states, "I understand and agree with USPTO's Terms of Use and Privacy Policy." Links are provided to the Terms of Use and Privacy Policy detailing the authorized uses of collected information. After this initial consent, users must complete the registration process by filling out their account profiles. At this stage in the process, users can refuse to provide the required information, but will not be able to complete the self-registration process. Successful submission functions as consent for use of the information for the intended purpose.

6. **How will the information be secured (e.g., administrative and technological controls)?** The information within the EDS and RBAC databases will be secured in accordance with USPTO policies, Federal laws, and NIST guidance (e.g. Risk Management Framework).

   In accordance with NIST 800-18 Rev. 1 and NIST 800-53 Rev. 4 the ESS System Security Plan (SSP) addresses the extent to which the security controls are implemented correctly, operating as intended, and

producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment. The SSP is reviewed on an annual basis.

The USPTO uses the SDLC and ORR processes to ensure that the security controls are in place for ESS. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the Security Plan. The Security Plans specifically address the management, operational and technical controls that are in place, and planned, during the operation of the enhanced system.

In addition, Continuous Monitoring reviews and annual assessments are conducted on the control implementations for ESS. The USPTO ITSMG conducts these assessments and reviews based on NIST SP 800-53 Revision 4, Recommended Security Controls for Federal Information Systems and NIST SP 800-53A, Final Guide for Assessing the Security Controls in Federal Information Systems. The results of these assessments and reviews are documented in the ESS Security Assessment Package, as part of the system's Authorization & Accreditation (A&A) process.

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

The USPTO has established OCIO-POL-23, "Personally Identifiable Data Removal Policy." Per USPTO policy, the data extra log and verify requirement will be met by the following:

USPTO PII Data Removal Policy (OCIO-POL-23):
(http://usptoocio/opg/psd/pol/Documents/Forms/All%20Approved%20Documents.aspx)

a) Maintain a centralized office log for extracted datasets that contain sensitive PII. This log must include the date the data was extracted and removed from the facilities, a description of the data extracted, the purpose of the extract, the expected date of disposal or return, and the actual date of return or deletion.
b) Ensure that any extract which is no longer needed is returned to USPTO premises or securely erased, and that this activity is recorded on the log.
c) Obtain management concurrence in the log, if an extract aged over 90 days is still required.
d) Store all PII data extracts maintained on an USPTO laptop in the encrypted My Documents directory. This includes any sensitive PII data extracts downloaded via the USPTO VPN.
e) Encrypt and password-protect all sensitive PII data extracts maintained on a portable storage device (such as CD, memory key, flash drive, etc.). Exceptions due to technical limitations must have the approval of the Office Director and alternative protective measures must be in place prior to removal from USPTO premises.
f) Encrypt and password-protect prior to transmission any sensitive PII data extracts that are sent to an external e-mail address via the Internet. The password key should be forwarded to the recipient in a separate e-mail from the attached file.

ESS data is monitored through the use of Audit Logs. These logs are sent to the SIEM and monitored on a near-real time basis by the CIO Command Center (C3). The information is restricted and managed in the backend by authorized personnel. The automatic on-line remote back-up of network servers is excluded from the extract logging requirement.

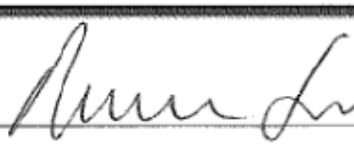
8. **Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?** A system of records exists for "USPTO Identification and Security Access Control and Certificate Systems" and the "USPTO PKI Registration and Maintenance System".

   Source: http://www.uspto.gov/sorn/privacy_sorn.jsp#

   Are these records covered by a record control schedule approved by the National Archives and Records Administration (NARA)? Yes. The OCIO IT Management of Records Policy (OCIO-POL-33) provides the requirements applicable for the creation, maintenance, use, and disposition of all records and other documentary materials in compliance with established Federal Records Management requirements.

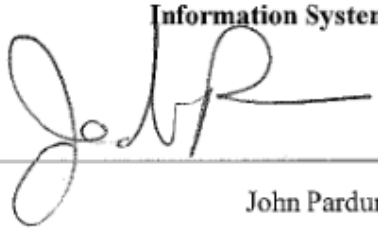
   The USPTO's Comprehensive Records Schedule is updated every year and lists the NARA-approved record series and dispositions for Agency documents, both from the unique agency schedules and from the federal-wide General Records Schedules.

SIGNATORY AUTHORITY

Agreed:  07/16/2015

Bob Simms — Date

Information System Owner

Agreed:  7/21/2015

John Pardun — Date

Senior Information Security Officer

Agreed:  7/24/15

Tony Chiles for John B. Owens II — Date

Authorizing Official