

**U.S. Department of Commerce
U.S. Patent and Trademark Office**



**Privacy Threshold Analysis
for the
Enterprise Software Services (ESS)**

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Enterprise Software Services (ESS)

Unique Project Identifier: PTOI-020-000

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Senior Agency Official for Privacy (SAOP).

Description of the information system and its purpose: *Provide a general description of the information system and its purpose in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44 U.S.C. § 3502(8).

ESS comprises of multiple on premise and in the cloud software services which support the USPTO in carrying out their daily task. Within this system, the services are broken up into several subsystems. These subsystems are identified as Enterprise Active Directory Services (EDS), MyUSPTO, Role Based Access Control (RBAC), Email as a Service (EaaS), Enterprise Share Point Services (ESPS), PTO Exchange Services (PTOES) and PTOFAX.

Enterprise Directory Services (EDS)

EDS is comprised of software products that are used for identity and access management that govern user's profile within the organization. These tools provide single sign-on access for authorized users, and serve as a standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other systems and services. User attributes such as First Name, Last Name, Middle Name and Telephone Number are populated in the system.

MyUSPTO – MyUSPTO is an external facing web site that provides a single location where customers can register and maintain a central account to do business with multiple USPTO services. The registration process consist of customers going through an account creation process that requires the following actions;

1. Email address used for signing in;
 - a. as well as other necessary account information;
 - i. Title
 - ii. Name
 - iii. Suffix
2. Verify the ReCaptcha.
3. Agree to the terms of service and privacy policy
4. An email is sent to one provided for account activation.

5. After account is activated;
 - a. Customers will be able to create a password
 - b. Select and answer security questions for password reset

MyUSPTO provides customers the capability to access and manage their own contact information, track patent applications, grants, trademark registrations, and post-registration statuses. MyUSPTO currently does not share any information with other systems or other agencies. This information is to be used only by USPTO for the purpose of identity proofing and verification. The information (including PII) is used only by USPTO for the purpose of identity proofing and verification.

Role-Based Access Control System (RBAC) – The RBAC system provides an authentication and authorization framework that allows secure, on-demand access to its managed applications by assigning system access to users based on their roles in an organization. For internal USPTO users, the organizational attributes that identify each user, their roles and groups are contained in RBAC. Roles are defined according to job competency, authority, and responsibility within the enterprise. The attributes include First Name, Middle Name, Last Name and Phone Number. For external (non-USPTO) users, no Personally Identifiable Information (PII) is collected within RBAC. To support the authentication and authorization process of external applications, RBAC collects, stores and maintains account login information, passwords, account activity, roles, and/or security question/answers for password resetting.

Email as a Service (EaaS) – The EaaS system is provided by Microsoft Office 365 (O365) and is FedRAMP approved. This Commercial off-the-shelf (COTS) product manages, maintains and distributes USPTO electronic mail, calendar, contacts and tasks that are on premise and/or in the cloud. Emails transmitted to and stored in the cloud leverage FIPS 140-2 compliant encryption mechanisms. EaaS does not collect any PII. However, there is a potential the usage of the service may introduce PII into the system. EaaS is not responsible for the collection and sharing of PII within the system.

Enterprise Sharepoint Services (ESPS) – The ESPS information system is provided by O365 Multi-Tenant & Supporting Services SaaS platform, which facilitates collaboration, provides full content management, implements business processes, and provides access to certain information that is essential to organizational goals and processes. It provides an integrated platform to plan, deploy, and manage intranet, extranet, and Internet applications across USPTO. As ESPS acts as a central repository, there is potential that ESPS may contain documents with PII or other sensitive information used by other applications and information systems throughout the organization. The PII uploaded by those systems, document their use and abide by USPTO policy, federal laws, executive orders, directives, policies, regulations, standards, and guidance. ESPS is not responsible for the collection and sharing of PII within the system.

PTO Exchange Servers (PTOES) - PTOES is an integrated system of COTS products that provides remote, secure access and data transmission for collaborative communication between USPTO resources and the internet through the use of laptops, desktops, and other mobile devices, such as Blackberry, Android and Apple devices. All communications between these devices and USPTO use FIPS 140-2 approved encryption modules. PTOES does not collect any PII.

PTO Enterprise Fax System (PTOFAX) – PTOFAX is an information system which manages and maintains all aspects of the USPTO fax services. This includes authenticating and authorizing users for fax services, receiving and sending faxes, converting electronic mail into faxes, exporting and maintaining fax records. This PTOFAX system does not collect, maintain, or disseminate any PII.

Questionnaire:

1. What is the status of this information system?

- ☐ This is a new information system. *Continue to answer questions and complete certification.*
- ☐ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>	g. New Interagency Uses	<input type="checkbox"/>
b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input type="checkbox"/>	h. Internal Flow or Collection	<input type="checkbox"/>
c. Significant System Management Changes	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character of Data	<input type="checkbox"/>
j. Other changes that create new privacy risks (specify):					

- ☒ This is an existing information system in which changes do not create new privacy risks. *Continue to answer questions, and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

- ☒ Yes. *Please describe the activities which may raise privacy concerns.*

The collection of certain PII when customers are registering for an account with MyUSPTO and/or other USPTO registration information that is uploaded to SharePoint, are activities which could raise privacy concerns.

- ☐ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C. 552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

- ☒ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*
- ☒ Companies
- ☐ Other business entities
- ☐ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

- ☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*
- ☒ DOC employees
- ☒ Contractors working on behalf of DOC
- ☐ Members of the public
- ☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

- ☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

- ☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

- ☐ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.
- ☒ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PIA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ I certify the criteria implied by one or more of the questions above **apply** to the Enterprise Software Services (ESS) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

☐ I certify the criteria implied by the questions above **do not apply** to the Enterprise Software Services (ESS) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Jimmy Orona III

Signature of SO: Users, Orona, Jimmy III
Digitally signed by Users, Orona, Jimmy III
Date: 2019.06.05 09:37:10 -04'00'

Date: _____

Name of Senior Information Security Officer (SISO): Don Watson

Signature of SISO:  Date: 6/14/19

Name of Authorizing Official (AO) & Bureau Chief Privacy Officer (BCPO): Henry J. Holcombe

Signature of AO & BCPO:  Date: 19 JUN '19