Version Number: 09-2016

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

Privacy Impact Assessment
for the
Enterprise Software Services (ESS)

Reviewed by: John B. Owens II, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Catrina D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2017.08.04 10:32:53 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
USPTO Enterprise Software Services (ESS)

Unique Project Identifier: PTOI-020-00

Introduction: System Description

Provide a description of the system that addresses the following elements:

The response must be written in plain language and be as comprehensive as necessary to describe the system.
[Guidance: When completing this section, be sure to include only information suitable for public viewing since this is to be posted online. Do not include system information such as IP addresses, architecture diagrams, et.]

(a) A general description of the information in the system

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), PTOFAX, and Symantec Endpoint Protection (SEP).

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.

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.

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. 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.

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.

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.

Symantec Endpoint Protection (SEP) – SEP is an information system that maintains and manages the protection mechanism used to safeguard USPTO system components from today's most known and malicious threats. The SEP system does not collect, maintain, or disseminate any PII.

(b) a description of a typical transaction conducted on the system
The typical transactions of USPTO Enterprise Software Services (ESS) consist mostly of identity and account management functions of USPTO staffs, contractors and external users to include; requesting, creating, issuing, modifying and disabling user accounts; enabling and disabling access to resources and applications; establishing conditions for group and role membership; tracking accounts and their respective access authorizations; and managing these functions.

In addition, ESS provides the capability for transmitting and communicating USPTO resources (emails, messaging, and collaborative documents) both on premise and remotely, through the use of various software.

(c) any information sharing conducted by the system

No, ESS does not conduct information sharing.

(d) a citation of the legal authority to collect PII and/or BII

The citation of the legal authority to collect PII and/or BII is 5 U.S.C. 301, 35 U.S.C. 2, and E.O.12862.

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system

ESS is considered a business-essential system with a Federal Information Processing Standard (FIPS) 199 security categorization of ***Moderate***.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

☐ This is a new information system.
☒ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*
☐ This is an existing information system in which changes do not create new privacy risks. *Continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	☐	d. Significant Merging	☐	g. New Interagency Uses	☐
b. Anonymous to Non-Anonymous	☐	e. New Public Access	☐	h. Internal Flow or Collection	☒
c. Significant System Management Changes	☐	f. Commercial Sources	☐	i. Alteration in Character of Data	☐
j. Other changes that create new privacy risks (specify): ESPS provides an online shared repository that is used throughout USPTO. Users are capable of uploading and downloading information from their designated Share Folders. From these Share Folders, users can obtain system documents, manuals, SOP, templates, diagrams, user/account records, sensitive information,					

etc. Users also have the ability to create folders and configure their repositories specifically for their department for ease of account management and data archiving. ESPS does not manage or maintain the data being uploaded/downloaded to the online shared repositories. However, there is a new privacy risk for this system due to the change in the ***USPTO ENTERPRISE SHAREPOINT*** policy. Users will now have the capability to upload sensitive data if needed.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	☐	e. File/Case ID	☒	i. Credit Card	☐
b. Taxpayer ID	☐	f. Driver's License	☐	j. Financial Account	☐
c. Employer ID	☐	g. Passport	☐	k. Financial Transaction	☐
d. Employee ID	☒	h. Alien Registration	☐	l. Vehicle Identifier	☐
m.Other identifying numbers (specify): Law Registration Number and state Bar number.					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: ESS does not collect, store or process Social Security Numbers (SSNs).					
*If SSNs are collected, stored, or processed by the system, please explain if there is a way to avoid such collection in the future and how this could be accomplished: N/A					

General Personal Data (GPD)					
a. Name	☒	g. Date of Birth	☒	m. Religion	☐
b. Maiden Name	☐	h. Place of Birth	☒	n. Financial Information	☐
c. Alias	☐	i. Home Address	☒	o. Medical Information	☐
d. Gender	☐	j. Telephone Number	☒	p. Military Service	☐
e. Age	☐	k. Email Address	☒	q. Physical Characteristics	☐
f. Race/Ethnicity	☐	l. Education	☐	r. Mother's Maiden Name	☐
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	☒	d. Telephone Number	☒	g. Salary	☒
b. Job Title	☒	e. Email Address	☒	h. Work History	☒
c. Work Address	☒	f. Business Associates	☒		
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	d. Photographs	☐	g. DNA Profiles	☐
b. Palm Prints	☐	e. Scars, Marks, Tattoos	☐	h. Retina/Iris Scans	☐
c. Voice Recording/Signatures	☐	f. Vascular Scan	☐	i. Dental Profile	☐
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	☒	c. Date/Time of Access	☒	e. ID Files Accessed	☐
b. IP Address	☐	d. Queries Run	☐	f. Contents of Files	☐
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	☐	Hard Copy: Mail/Fax	☐	Online	☒
Telephone	☐	Email	☐		
Other (specify):					

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	☐	Other Federal Agencies	☐
State, Local, Tribal	☐	Foreign	☐		
Other (specify):					

Non-government Sources					
Public Organizations	☐	Private Sector	☐	Commercial Data Brokers	☐
Third Party Website or Application			☐		
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	☐	Biometrics	☐
Caller-ID	☐	Personal Identity Verification (PIV) Cards	☐
Other (specify):			

☒	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify):			

☒	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility	☒	For administering human resources programs	☐
For administrative matters	☒	To promote information sharing initiatives	☐
For litigation	☒	For criminal law enforcement activities	☐
For civil enforcement activities	☐	For intelligence activities	☐
To improve Federal services online	☒	For employee or customer satisfaction	☐
For web measurement and customization technologies (single-session)	☐	For web measurement and customization technologies (multi-session)	☐
Other (specify): PII is collected to process and/or examine STEPP registration submissions and troubleshoot issues with U.S. patent applicants.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The information is collected to identify the users and partners when authenticating through the network. User credentials are managed through Active Directory and will integrate with RBAC. This will allow users to access USPTO's network and various systems through Single Sign-On.
Also the collected information is intended to be used by the USPTO Service Desk for verifying the identity of customers interacting with MyUSPTO. If a customer forgets the password to their USPTO account, the PII collected would be used to verify a customer.

ESPS does not manage or maintain the data being uploaded/downloaded to the online shared repositories. However, the shared repositories are used throughout USPTO, which may contain PII. Currently, Patents will be using the SharePoint folder to store STEPP registration data. This data includes the following; First and Last Name, Company name, Home Address, E-mail address, telephone number, citizenship, and Law Registration and Bar number.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	☒	☒	☒
DOC bureaus	☐	☒	☐
Federal agencies	☐	☒	☐
State, local, tribal gov't agencies	☐	☒	☐
Public	☐	☐	☐
Private sector	☐	☐	☐
Foreign governments	☐	☐	☐
Foreign entities	☐	☐	☐
Other (specify):	☐	☐	☐

☒	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

☒	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: Patents system will want to upload PII information collected during the STEPP registration process. Information is protected through a layered security approach which incorporates the use of secure authentication, access control, mandatory configuration settings, firewalls, Virtual

	Private Network (VPN), and encryption, where required. Internally within USPTO, data transmission confidentiality controls are provided by PTOnet.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	☐	Government Employees	☒
Contractors	☒		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

☒	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
☒	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: http://www.uspto.gov/privact.jsp	
☐	Yes, notice is provided by other means.	Specify how:
☐	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

☐	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: PII is collected as part of the registration process, account creation, to keep track of work location of internal users, and is also used to verify external users' identity for authentication and security purposes.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

☒	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Individuals consent to providing information for the primary purpose of acquiring access to applications, network or to sign

		up for programs.
☐	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

☒	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals may login to MyUSPTO and update their PII held in their Account Profile.
☐	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

☐	All users signed a confidentiality agreement or non-disclosure agreement.
☐	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Unauthorized access, suspicious system log behavior and log failures are audited in real time and reported to the appropriate personnel to troubleshoot and remediate any potential issues.
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): ___8/7/2016_____ ☐ This is a new system.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☐	Contracts with customers establish ownership rights over data including PII/BII.
☐	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☒	Other (specify): Database-Level FIPS 140-2 encryption is applied

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

The information system is 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. In addition, annual assessments and Continuous Monitoring reviews are conducted on the ESS data. The USPTO Office of Policy and Governance/Cybersecurity Division (OPG/CD) conducts these assessments and reviews based on NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations and NIST SP 800-53A Revision 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations. The results of these assessments and reviews are documented in the ESS Security Assessment Package as part of the system's Security Authorization process.

Management Controls
USPTO uses the Life Cycle review process to ensure that management controls are in place for ESS. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the System Security Plan. The System Security Plan specifically addresses the management, operational, and technical controls that are in place, and planned, during the operation of the enhanced system. Additional management controls include performing national agency checks on all personnel, including contractor staff. Additionally, USPTO develops privacy and PII-related policies and procedures to ensure safe handling, storing, and processing of sensitive data.

Operational Controls
Automated operational controls include securing all hardware associated with the ESS in the USPTO Data center. The Data Center is controlled by access card entry, and is manned by a uniformed guard service to restrict access to the servers, their Operating Systems and databases.

Technical Controls
ESS is secured by various USPTO infrastructure components, including the Network and Security Infrastructure (NSI) system and other OCIO established technical controls to include password authentication at the server and database levels. Web communications leverages modern encryption technology such as TLS 1.1/1.2 over HTTPS. Dedicated interconnections offer protection through IPSec VPN tunnels.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: *COMMERCE/PAT–TM–23, User Access for Web Portals and Information Requests.* *OMMERCE/PAT–TM–1, Attorneys and Agents Registered or Recognized to Practice Before the Office.*

☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

☒	There is an approved record control schedule. Provide the name of the record control schedule: ESS-MyUSPTO and ESPS follow the NARA guidelines and USPTO document retention policies. Current retention policies are to keep electronic information for two years after an individual has departed the agency. • Assignments on the Web (AOTW) - Non-record; Destroy when no longer needed. • Electronic Patent Assignment System (EPAS) - N1-241-05-2:1d USPTO Non-Core Products and Publications (NARA Copy). • Electronic Trademark Assignment System (ETAS) - N1-241-05-2:1d USPTO Non-Core Products and Publications (NARA Copy). • IT Development Project records – GRS 3.1 • System and data security records - GRS 3.2 • IT Customer Service Files – GRS 24 • Evidentiary Patent Applications N1-241-10-1:4.1 • Patent Examination Working Files N1-241-10-1:4.2 • Patent Examination Feeder Records N1-241-10-1:4.4 • Patent Post-Examination Feeder Records N1-241-10-1:4.5 • Patent Case Files, Granted N1-241-10-1:2 • Abandoned Patent Applications, Not Referenced in Granted Case File N1-241-10-1:3 • File Tracking System (FTS) - N1-241-05-1:7a Administrative Services Correspondence. • Patent and Trademark Assignment System (PTAS) - N1-241-5-2:1d USPTO Non-Core Products and Publications (NARA Copy); N1-241-5-2:4 Preliminary Input Files for Dissemination Products and Publications. • Electronic Data Housing (EDH) – N1-241-05-2:5 Information Dissemination Product Reference.
☐	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
☒	Yes, retention is monitored for compliance to the schedule.
☐	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	☒	Overwriting	☒
Degaussing	☒	Deleting	☐
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

☐	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
☒	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☐	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

☒	Identifiability	Provide explanation: Name, mailing address, phone number, email address collected for Patents registration to STEPP program. For MyUSPTO, the first name, last name, telephone number (work, cell, or home), e-mail address, physical address, and security question answers are collected to access the application.
☐	Quantity of PII	Provide explanation:
☐	Data Field Sensitivity	Provide explanation:
☒	Context of Use	Provide explanation: Information is for identifying, authenticating and tracking of users. Internal authorized user credentials are managed through the EDS system. Also the collected information is intended to be used by the USPTO Service Desk for verifying the identity of customers interacting with the system. If a customer forgets the password to their USPTO account, the PII collected would be used to verify a customer. The data captured, stored, or transmitted by the Patents system is used to process STEPP registrations and may include sensitive information from the applicant's application. More details on the Patents use of PII, can be found within the Patents PTA/PIA worksheets.
☒	Obligation to Protect Confidentiality	Provide explanation: USPTO Privacy Policy requires the PII information collected within the system to be protected accordance to NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information.
☒	Access to and Location of PII	Provide explanation: Access is limited only to the identified and authenticated users and partners. The information collected will not be shared with any other agency. This information is to be used only by the USPTO for the purpose of identity proofing and verification.

☐	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

☐	Yes, the conduct of this PIA results in required business process changes. Explanation:
☒	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

☐	Yes, the conduct of this PIA results in required technology changes. Explanation:
☒	No, the conduct of this PIA does not result in any required technology changes.