

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



**Privacy Impact Assessment
for the
Enterprise Software Services (ESS)**

Reviewed by: Henry J. Holcombe, 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 PURVIS Digitally signed by CATRINA PURVIS
Date: 2019.08.15 18:12:22 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer 7/6/2019
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:

(a) Whether it is a general support system, major application, or other type of system

Enterprise Software Services (ESS) is a Major Application.

(b) System location

ESS is located 600 Dulany Street, Alexandria Va. 22314

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

ESS interconnects with the following other systems:

Network and Security Infrastructure System (NSI)
Enterprise Unix Services (EUS)
Service Orientated Infrastructure (SOI)
Agency Administrative Support System (AASS)
Corporate Administrative Office System (CAOS)
Consolidated Financial System (CFS)
Cornerstone on Demand Unified Talent Management Solution (CUTMS)
Data Storage Management System (DSMS)
Enterprise Desktop Platform (EDP)
Information Delivery Product (IDP)
Enterprise Monitoring and Security Operations (EMSO)
Enterprise Record Management and Data Quality System (ERMDQS)
Enterprise Virtual Events Services (EVES)
Enterprise Windows Servers (EWS)
FPNG Fee Processing Next Generation (FPNG)
Personal Identity Verification System Card Management System (HSPD-12/PIVS/CMS)
Information Dissemination Support System (IDSS)
Intellectual Property Leadership Management System (IPLMSS)
Microsoft Office 365 MT (O365 MT)
OCIO Program Support System (OCIO PSS)
PBX-VOIP
Patent Capture and Application Processing System – Examination Support (PCAPS ES)

Patent Capture and Application Processing System – Capture and Initial Processing (PCAPS IP)
Patent Search System – Primary Search and Retrieval (PSS PS)
Patent Search System – Specialized Search and Retrieval (PSS SS)
Public and Enterprise Wireless LAN (PEWLAN)
Revenue Accounting and Management System (RAM)
Trademark Processing System – External System (TPS ES)
Trademark Processing System – Internal System (TPS IS)
Trademark Next Generation (TMNG)
Database Services (DBS)

(d) The way the system operates to achieve the purpose(s) identified in Section 4

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. **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. To the extent PII is uploaded by those other systems, they document its use and abide by USPTO policy, federal laws, executive orders, directives, policies, regulations, standards, and guidance. **EaaS 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 that 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.**

(e) *How information in the system is retrieved by the user*

Information in the system is retrieved through internet access and a registered account.

(f) *How information is transmitted to and from the system*

Information is transmitted to and from ESS via the internet and internal USPTO network.

(g) Any information sharing conducted by the system

ESS does conduct public information sharing of search and retrieval of electronic texts, and images concerning Patent and Trademark Applications, Patents, and Trademarks by USPTO internal and external users within MyUSPTO. MyUSPTO provides public users the ability to register and maintain an account to do business with multiple USPTO services.

(h) *The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*

The citation of the legal authority to collect PII and/or BII is 5 U.S.C 301, 15 U.S.C. 1051 et seq., 35 U.S.C. 2, and E.O. 12862.

(i) *The Federal Information Processing Standards (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.)

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, and there is not a SAOP approved Privacy Impact Assessment.

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*	<input type="checkbox"/>	e. File/Case ID	<input checked="" type="checkbox"/>	i. Credit Card	<input type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input type="checkbox"/>
d. Employee ID	<input checked="" type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: N/A – ESS does not collect, store or process Social Security Numbers (SSNs)					

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

Work-Related Data (WRD)					
a. Occupation	<input checked="" type="checkbox"/>	d. Telephone Number	<input checked="" type="checkbox"/>	g. Salary	<input checked="" type="checkbox"/>
b. Job Title	<input checked="" type="checkbox"/>	e. Email Address	<input checked="" type="checkbox"/>	h. Work History	<input checked="" type="checkbox"/>
c. Work Address	<input checked="" type="checkbox"/>	f. Business Associates	<input checked="" type="checkbox"/>		
i. Other work-related data (specify):					

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

System Administration/Audit Data (SAAD)					
a. User ID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>	e. ID Files Accessed	<input type="checkbox"/>

b. IP Address	<input type="checkbox"/>	d. Queries Run	<input type="checkbox"/>	f. Contents of Files	<input type="checkbox"/>
g. Other system administration/audit data (specify):					

Other Information (specify)
MyUPTO is a conduit for users to access other systems, which manage the transference of financial data captured by other systems. MyUSPTO does not collect, maintain or disseminate financial data or any other data not selected in the GPD/WPD tables.

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	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input checked="" type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		
Other (specify):					

Government Sources					
Within the Bureau	<input checked="" type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		
Other (specify):					

Non-government Sources					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application	<input type="checkbox"/>				
Other (specify): N/A					

2.3 Describe how the accuracy of the information in the system is ensured.

Personally, Identifiable Information in ESS is secured using appropriate administrative, physical and technical safeguards in accordance with the applicable federal laws, Executive Orders, directives, policies, and standards.

All access has role based restrictions, and individual with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access and changes as part of verifying the integrity of data.

2.4 Is the information covered by the Paperwork Reduction Act?

<input checked="" type="checkbox"/>	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. PTO Form 2030 (Rev. 05/12). OMB 0651-0041 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE.
<input type="checkbox"/>	No, the information is not covered by the Paperwork Reduction Act.

2.5 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	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	There are not any IT systems 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	<input type="checkbox"/>	For administering human resources programs	<input type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input type="checkbox"/>
For litigation	<input checked="" type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>
For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input checked="" type="checkbox"/>	For employee or customer satisfaction	<input type="checkbox"/>

For web measurement and customization technologies (single-session)	<input type="checkbox"/>	For web measurement and customization technologies (multi-session)	<input type="checkbox"/>
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 PII 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.

- 5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

ESS implements security and management controls to prevent the inappropriate disclosure of sensitive information. Automated mechanisms are in place to ensure the security of all data collected. Security controls are employed to ensure information is resistant to tampering (Physical and Access Controls), the confidentiality of data in transit (Encryption), and that data is available for authorized users only (Access Control). Management controls are utilized to prevent the inappropriate disclosure of sensitive information. In addition, the Perimeter Network (NSI) and EMSO provide additional automated transmission and monitoring mechanisms to ensure that PII is protected and not breached by any outside entities. In the event of disposal, USPTO uses degaussing to permanently remove data according to government mandate and security policy.

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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private sector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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.

<input checked="" type="checkbox"/>	<p>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:</p> <p>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.</p>
<input type="checkbox"/>	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	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
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.)

<input checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input checked="" type="checkbox"/>	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-policy	
<input type="checkbox"/>	Yes, notice is provided by other means.	Specify how:
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

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

<input type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: PII collection is part of the registration process, account creation, and tracking internal users' work location, and is used to verify external users' identity for authentication/security purposes.

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

<input checked="" type="checkbox"/>	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.
<input type="checkbox"/>	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.

<input checked="" type="checkbox"/>	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.
<input type="checkbox"/>	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.)

<input type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
--------------------------	---

<input type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>08/05/2018</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	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 (POA&M).
<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input type="checkbox"/>	Contracts with customers establish ownership rights over data including PII/BII.
<input type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input checked="" type="checkbox"/>	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. (Include data encryption in transit and/or at rest, if applicable).

<p>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.</p> <p><u>Management Controls</u></p> <p>1. 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.</p> <p><u>Operational Controls</u></p>
--

1. 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

1. 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.”

<input type="checkbox"/>	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number (<i>list all that apply</i>):
<input checked="" type="checkbox"/>	<p><i>COMMERCE/PAT-TM-23, User Access for Web Portals and Information Requests.</i></p> <p><i>COMMERCE/PAT-TM-20, Customer Call Center, Assistance and Satisfaction Survey Records</i></p> <p><i>COMMERCE/PAT-TM-1, Attorneys and Agents Registered or Recognized to Practice Before the Office.</i></p>
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input type="checkbox"/>	No, this system is not a system of records and a SORN is not applicable.

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.)*

	<p>There is an approved record control schedule. Provide the name of the record control schedule:</p>
<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> • Assignments on the Web (AOTW) - Non-record; Destroy when no longer needed. • Electronic Patent Assignment System (EPAS) - <u>N1-241-05-2:1d</u> USPTO Non-Core Products and Publications (NARA Copy). • Electronic Trademark Assignment System (ETAS) - <u>N1-241-05-2:1d</u> USPTO Non-Core Products and Publications (NARA Copy). • IT Development Project records – GRS 3.1:010 • System and data security records - GRS 3.2:010 • IT Customer Service Files – GRS 5.8:010 • 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

	<ul style="list-style-type: none"> • 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.
<input type="checkbox"/>	No, there is not an approved record controls schedule. Provide the stage in which the project is in developing and submitting a records controls schedule:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	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	<input type="checkbox"/>	Overwriting	<input checked="" type="checkbox"/>
Degaussing	<input checked="" type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
Other (specify): N/A.			

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.
(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)

<input type="checkbox"/>	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input checked="" type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	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.)

<input checked="" type="checkbox"/>	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.
<input type="checkbox"/>	Quantity of PII	Provide explanation:
<input type="checkbox"/>	Data Field Sensitivity	Provide explanation:
<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	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.
<input type="checkbox"/>	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

USPTO have identified and evaluated potential threats to PII such as loss of confidentiality and integrity if information. Based upon USPTO's threat assessment the Agency have implemented baseline of security controls to mitigate these risk to sensitive information to an acceptable level.

--

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

<input type="checkbox"/>	Yes, the conduct of this PIA results in required business process changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required business process changes.

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

<input type="checkbox"/>	Yes, the conduct of this PIA results in required technology changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.