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-020-00

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 Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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 is comprised of multiple on premise and in-the-cloud software services, which support the USPTO in carrying out its daily tasks. Within this system, the services are broken up into several subsystems. These subsystems are Enterprise Active Directory Services (EDS), MyUSPTO, Role Based Access Control (RBAC), Email as a Service (EaaS), Enterprise Share Point Services (ESPS), Symantec Endpoint Protection, and PTOFAX.

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 at 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) -The NSI is an Infrastructure information system, and provides an aggregate of subsystems that facilitates the communications, secure access, protective services, and network infrastructure support for all United States Patent and Trademark Office (USPTO) IT applications.

Enterprise UNIX Services (EUS) - EUS consists of assorted UNIX operating system variants (OS), each comprised of many utilities along with the master control program, the kernel.

Service Orientated Infrastructure (SOI) - The SOI provides a feature-rich and stable platform upon which USPTO applications can be deployed.

Agency Administrative Support System (AASS) - AASS consists of several applications that provide consolidation of document imaging services, enables management and tracking of hardware/software assets, and enables Under Secretary of Commerce for Intellectual Property and USPTO Director to receive and respond to a wide range of official correspondences.

Corporate Administrative Office System (CAOS) - The CAOS is an application information system composed of four Automated Information Systems (AISs) that supports all activities associated with the recruitment and management of USPTO personnel.

Consolidated Financial System (CFS) - The CFS is a Master System composed of the following subsystems: Momentum, Concur Integration, E-Acquisition (ACQ), and VendorPortal.

Data Storage Management System (DSMS) - DSMS is an infrastructure system that provides archival and storage capabilities securely to the USPTO. The information system is considered an essential component of USPTO's Business Continuity and Disaster Recovery program.

Enterprise Desktop Platform (EDP) - EDP is an infrastructure information system, which provides a standard enterprise-wide environment that manages desktops and laptops running on the Windows 10 operating system (OS), providing United States Government Configuration Baseline (USGCB) compliant workstations. The USGCB security mandate by the Office of Management and Budget (OMB) requires all Federal Agencies, including the United States Patent and Trademark Office (USPTO), to use the directed desktop configuration

Information Delivery Product (IDP) - Information Delivery Product (IDP) is a master system that provides access to integrate USPTO data through various tools in support of not only reporting and visualizing but also analytics used in decision-making across USPTO.

Enterprise Monitoring and Security Operations (EMSO) - EMSO provides a centralized command and control console with integrated enterprise log management, security information and event management, network behavior analysis, and reporting through the collection of events, network/application flow data, vulnerability data, and identity information.

Enterprise Record Management and Data Quality System (ERMDQS) – ERMDQS is Major Application (MA) consisting of two Automated Information Systems (AIS): Data Architecture Tool – Metadata (DAT-Metadata) and Records Management Tracking System (RMTS). In support of the USPTO mission, ERMDQS provides a standard-based approach to managing

digital records electronically by storing metadata about a record but leaving that record in its native repository, tracking for inactive records that are being transferred to an off-site approved records center, and a metadata management solution used for creating a centralized repository of USPTO metadata information.

Enterprise Virtual Events Services (EVES) - The EVES is an application information system consisting of five subsystems: Cisco Telepresence (CT)/ Tandberg, WebEx (WebEx), vBrick, Adobe (ACS), and LiveStream. It enables business units to share vital knowledge through collaboration capabilities that incorporate data, voice, and video communication technologies.

Enterprise Windows Servers (EWS) - EWS is an Infrastructure information system, and provides a hosting platform for major applications that support various USPTO missions. FPNG Fee Processing Next Generation (FPNG) - FPNG provides a modern payment system to the public and internal facing functionality that enables USPTO employees to support customers Personal Identity Verification System Card Management System (HSPD-12/PIVS/CMS)

Information Dissemination Support System (IDSS) – IDSS supports the Trademark and Electronic Government Business Division, the Corporate Systems Division (CSD), the Patent Search System Division, the Office of Electronic Information Products, and the Office of Public Information Services by providing automated support for the timely search and retrieval of electronic text and images concerning patent applications and patents by USPTO internal and external users.

Intellectual Property Leadership Management System (IPLMSS) - IPLMSS is a master Automated Information System (AIS) which facilitates grouping and managing 12 general support and separately boundaried AISs that collectively support the United States Patent and Trademark Office's (USPTO) Director; Deputy Director; Office of the General Counsel (OGC), including OGC's components the Office of General Law (OGL), Office of the Solicitor, and Office of Enrollment and Discipline (OED); Trademark Trial and Appeal Board (TTAB); Patent Trial and Appeal Board (PTAB); Office of Patent Training (OPT); and Office of Policy and International Affairs (OPIA).

Microsoft Office 365 MT (O365 MT) - A line of subscription services offered by Microsoft as part of the Microsoft Office product line.

OCIO Program Support System (OCIO-PSS) – OCIO-PSS helps authorized USPTO personnel and contractor employees obtain the information and data needed for contract related, system requirements, test plans, test requirements, and other documents important to the OCIO-PSS personnel.

PBX-VOIP - Patent Capture and Application Processing System – Examination Support (PCAPS ES) - PCAPS-ES consists of several applications that enable patent examiners and public users to search and retrieve application data and images and patent examiners and patent applicants to identify individuals and organizations with intellectual property, pre-grant, and published applications. Patent Capture and Application Processing System – Capture and Initial Processing (PCAPS IP) - PCAPS-IP consists of several applications that facilitate the automated processing of patent applications.

Patent Search System – Primary Search and Retrieval (PSS PS) - PSS-PS is a master system that processes, transmits and store data and images to support the data-capture and conversion requirements of the USPTO to support the USPTO patent application process.

Patent Search System – Specialized Search and Retrieval (PSS SS) - PSS-SS is Master system which supports the Patent Cost Center. It is considered a mission critical "system". PSS-SS provides access to highly specialized data that may include annual submissions of nucleic and amino acid sequence or prior-art searching of polynucleotide and polypeptide sequences, other types of information that may be more scientific or technology-based, Patent Linguistic Utility Service (a query by example search system), Chemical Drawing ability, and Foreign Patent Data.

Public and Enterprise Wireless LAN (PEWLAN) - PEWLAN provides wireless internet connection for USPTO staff, contractors, and guests as a productivity enhancer. It is designed to facilitate a secure network connectivity from anywhere within USPTO's Alexandria and Shillington campuses.

Trademark Processing System – External System (TPS ES) - TPS-ES is Major Application information system, and provides customer support for processing Trademark applications for USPTO.

Trademark Processing System – Internal System (TPS IS) - TPS-IS consists of several applications that are used in the automated processing of trademark applications. The applications that are used to support USPTO staff through the trademark review process.

Trademark Next Generation (TMNG) - The TMNG is a Major Application, and provides support for the automated processing of trademark applications for the USPTO.

Database Services (DBS) - DBS is an Infrastructure information system, and provides a Database Infrastructure to support the mission of USPTO database needs.

d) The purpose that the system is designed to serve

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

e) The way the system operates to achieve the purpose

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

Enterprise Directory Services (EDS) – EDS is comprised of software products that are used for identity and access management that govern users' profiles 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 the email address 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, and to 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 and 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. 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 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. The PTOFAX system does not collect, maintain, or disseminate any PII.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

Enterprise Directory Services (EDS) collects user attributes such as First Name, Last Name, Middle Name and Telephone Number are populated in the system.

MyUSPTO's 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

Role-Based Access Control System (RBAC) collects attributes including 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.

g) Identify individuals who have access to information on the system
Government Employees and Contractors

h) How information in the system is retrieved by the user
Information in the system is retrieved through internet access and a registered account.

i) How information is transmitted to and from the system
Information is transmitted to and from ESS via the internet and internal USPTO network.

Questionnaire:

1. Status of the Information System

1a. 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	☐	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):					

☐   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. *Continue to answer questions and complete certification.*

☐   This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017). *Continue to answer questions and complete certification.*

☒   This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

☐   Yes. This is a new information system.

☐   Yes. This is an existing information system for which an amended contract is needed.

☐   No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

☒   No. This is not a new information system.

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. *(Check all that apply.)*

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

☒ 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.

☐ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)
4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

    ☒ DOC employees
    ☒ Contractors working on behalf of DOC
    ☐ Other Federal Government personnel
    ☒ 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 Social Security numbers (SSNs), including truncated form?

    ☐   Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

    ☒   No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. 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.

4d. 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, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP 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.

System Owner Name: Jimmy Orona Office: Branch Chief – Software Services Branch 2 (I/SSB2) Phone: (571) 272-0673 Email: Jimmy.Orona@uspto.gov Signature: Users, Orona, Jimmy III *Digitally signed by Users, Orona, Jimmy III Date: 2021.04.27 08:47:59 -04'00'* Date signed: _____	**Chief Information Security Officer** Name: Don Watson Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-8130 Email: Don.Watson@uspto.gov Signature: DON R Watson *Digitally signed by DON R Watson Date: 2021.04.28 07:25:40 -04'00'* Date signed: _____
Privacy Act Officer Name: John Heaton Office: Office of General Law (O/GL) Phone: (571) 270-7420 Email: Ricou.Heaton@upsto.gov Signature: Users, Heaton, John (Ricou) *Digitally signed by Users, Heaton, John (Ricou) Date: 2021.04.26 19:44:21 -04'00'* Date signed: _____	**Bureau Chief Privacy Officer and Authorizing Official** Name: Henry J. Holcombe Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-9400 Email: Jamie.Holcombe@uspto.gov Signature: Users, Holcombe, Henry *Digitally signed by Users, Holcombe, Henry Date: 2021.04.28 15:44:59 -04'00'* Date signed: _____
Co-Authorizing Official Name: N/A Office: N/A Phone: N/A Email: N/A Signature: _____ Date signed: _____	