Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Enterprise Software Services (ESS)

Reviewed by: Deborah Stephens, 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

NICHOLAS CORMIER Digitally signed by NICHOLAS CORMIER
Date: 2025.09.24 07:55:40 -04'00' 9/24/2025

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 brief description of the information system.

Enterprise Software Services (ESS) is comprised of multiple software services, which support the United States Patent and Trademark Office (USPTO) in carrying out its daily tasks. Within this system, the services are broken up into several subsystems. These subsystems are Delivery Services-NIFI-API (NIFI), which moves information between vital operations services and components. Enterprise Active Directory Services (EDS), which provides a unique identifier for the user, computer or group and to provide access to network resources, used by multiple systems. USPTO Exchange Servers (PTOES), which allows emails to be relayed from the internet instead of from USPTO systems. Global Enterprise Architecture Repository System (GEARS), which keeps an inventory of all technologies and assets of all USPTO systems. Adobe Experience Manager (AEM) – On Premises (OnPrem) (AEM-OnPrem) provides a system to sign documents such as Patents and Trademarks.

Address the following elements:

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

Major application.

(b) System location

ESS is hosted in Alexandria, VA

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

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 USPTO IT applications.

Identity, Credential, and Access Management Identity as a Service (ICAM IDaaS) - The ICAM IDaaS is an Infrastructure information system, and provides authentication and authorization service to secure all enterprise applications/ Automated Information Systems (AIS's), provide audit ability to user activity. The system provides following services to the enterprise: User Provisioning and Life Cycle Management, User Roles and Entitlement Management,

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.

HRConnect – ESS ingest its PII from HRConnect. HRConnect is the Treasury's Government-wide Human Resources Line of Business (HRLoB) Shared Services Center (SSC) online personnel management system that provides managers, supervisors, employees, and personnel specialists with desktop access to personnel and payroll data.

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

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

Consolidate d 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 USPTO to use the directed desktop configuration.

Information Delivery Product (IDP) - 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.

Security and Compliance Services (SCS) - SCS provides Security Incident and Event Management, Enterprise Forensic, Enterprise Management System, Security and Defense, Enterprise Scanner, Enterprise Cybersecurity Monitoring Operations, Performance Monitoring Tools, Dynamic Operational Support Plan, & Situational Awareness and Incident Response.

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.

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.

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 AIS which facilitates grouping and managing 12 general support and separate boundary AISs that collectively support the 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 Internal (M365 Internal) - A line of subscription services offered by Microsoft as part of the Microsoft Office product line.

Private Branch Exchange-Voice Over Internet Protocol (PBX-VOIP) – The PBX-VOIP is an infrastructure information system, consisting of the Cisco VOIP, ECC and CRS that provides the following services in support of analog voice, digital voice, collaborative services and data communications for business units across the entire USPTO.

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, images, 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 – 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 way the system operates to achieve the purpose(s) identified in Section 4

ESS is comprised of multiple 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 NIFI, EDS, PTOES, GEARS, and AEM-OnPrem.

AEM-OnPrem – provides electronic signature functionality for USPTO Product Lines. Provides compliance with Paper Reduction Act.

NIFI – is an orchestration helper tool for automating sending data exchanges between various applications by connecting to each system and putting and pulling data to and from it.

EDS – a database containing all users, computers and groups in order to help identify said users, computers and groups and grant access to network resources.

GEARS – An enterprise architecture tool that displays all PTO technologies broken out by applications and components of those applications

PTOES – is an on-premise Email System that provides resources like Mailboxes, Calendars, Contacts, and other services for email communications. Exchange Servers allows both send and receive connectors for secure internal and external mail flows thru SMTP relays. End-users are able to view the PTOES resources thru other Microsoft products like Outlook, SharePoint, Web browsers, or other 3rd party systems thru API calls.

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

EDS – users can view their personal data within the network at http://ars.uspto.gov/ARWebAdmin/, only admins can change application data.

GEARS – all authorized USPTO users can access information in the system which is retrieved through intranet access and a registered account.
AEM-OnPrem – no user access, only admins can see application data
PTOES – no user access, only admins can see application data
NIFI – no user access, only admins can see application data

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

Information is transmitted to and from ESS via the internet and internal USPTO network. All communication is encrypted over TLS 1.2 higher using HTTPS protocols.

(g) Any information sharing

Information about employees may be shared or accessed by other USPTO systems via the EDS.

(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

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	☐	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.

☐ This is an existing information system in which changes do not create new privacy risks, and there is 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*	☐	f. Driver's License	☐	j. Financial Account	☐
b. Taxpayer ID	☐	g. Passport	☐	k. Financial Transaction	☐
c. Employer ID	☐	h. Alien Registration	☐	l. Vehicle Identifier	☐
d. Employee ID	☒	i. Credit Card	☐	m. Medical Record	☐
e. File/Case ID	☒				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	☒	h. Date of Birth	☐	o. Financial Information	☐
b. Maiden Name	☐	i. Place of Birth	☐	p. Medical Information	☐
c. Alias	☐	j. Home Address	☐	q. Military Service	☐
d. Gender	☐	k. Telephone Number	☐	r. Criminal Record	☐
e. Age	☐	l. Email Address	☐	s. Marital Status	☐
f. Race/Ethnicity	☐	m. Education	☐	t. Mother's Maiden Name	☐
g. Citizenship	☐	n. Religion	☐		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	☒	e. Work Email Address	☒	i. Business Associates	☒
b. Job Title	☒	f. Salary	☐	j. Proprietary or Business Information	☐
c. Work Address	☒	g. Work History	☐	k. Procurement/contracting records	☐
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	☐		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	f. Scars, Marks, Tattoos	☐	k. Signatures	☐
b. Palm Prints	☐	g. Hair Color	☐	l. Vascular Scans	☐
c. Voice/Audio Recording	☐	h. Eye Color	☐	m. DNA Sample or Profile	☐
d. Video Recording	☐	i. Height	☐	n. Retina/Iris Scans	☐
e. Photographs	☐	j. Weight	☐	o. Dental Profile	☐
p. 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	☒	f. 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 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 individuals 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?

☐	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
☒	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	☐	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): Click or tap here to enter text.			

☒	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			
For a Computer Matching Program	☐	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):			

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).

All PII used in ESS is in reference to a Federal Employee/ Contractor. AEM-OnPrem does not process PII, NIFI transfers POC names between SMP, GEARS and COMET. PTOES allows access to user names and email addresses to the various systems that use email. GEARS relays POC names through a user interface for authenticated PTO users. EDS provides user names, work email addresses and work phone numbers, user work locations, employee numbers, business associations as well as an org chart.

5.2 Describe any potential threats to privacy, such as insider threat, 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. The potential threats to the system are insider threats and adversarial entities that may pose a threat to the confidentiality, access and integrity of the system. 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 SCS 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	☒	☒	☒
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 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

☐	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☒	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☐	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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: HRConnect M365 Internal ICAM IDaaS NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 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: https://www.uspto.gov/privacy-policy	
☐	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: Individuals do not have an opportunity to decline to provide PII/BII as it is a requirement to have network access.

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:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Individuals do not have the opportunity to consent to particular uses of their PII/BII as the information is required to ensure the security of the system.

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:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Individuals do not have the opportunity to review or update their PII/BII within ESS. The individual can contact the Office of Human Resources to review or update their PII/BII.

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: audit logs
☒	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 6/6/2024

	☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	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 5 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).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish DOC 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. *(Include data encryption in transit and/or at rest, if applicable).*

The information system provides protection of resources in accordance with NIST 800-18 Rev. 1 and NIST 800-53 Rev. 5; 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 Cybersecurity Division CD) conducts these assessments and reviews based on NIST SP 80053 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 1.2 over HTTPS or HSTS. Dedicated interconnections offer protection through IP Sec VPN tunnels.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

☒ Yes, the PII/BII is searchable by a personal identifier.

☐ No, the PII/BII is not searchable by a personal identifier.

9.2 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, number, and link. *(list all that apply)*: System of Records Notices - COMMERCE-DEPT-18 | U.S. Department of Commerce
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	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.)*

General Records Schedules (GRS) | National Archives

☒	There is an approved record control schedule. Provide the name of the record control schedule: Information technology operations and maintenance records – GRS 3.1 (excluding 050) General Technology Management Records – GRS 3.1: 012 - Special purpose computer programs and applications. Information Systems Security Records - GRS 3.2 IT Development Project records – GRS 3.1:010 System and data security records - GRS 3.2:010
☐	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 Level

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, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

☒	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 level. *(Check all that apply.)*

☒	Identifiability	Provide explanation: The information in section 2.1 collected for user PII information are collected and managed in the EDS system as part of the authentication process.
☒	Quantity of PII	Provide explanation: 10 PII data points per individual. ESS has PII for all USPTO employees and contractors which is about 15000 people
☒	Data Field Sensitivity	Provide explanation: The data includes limited personal and work-related elements for identifying and authenticating users and does not include social security numbers of individuals.
☒	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
☒	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.

☐	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 insider threats and adversarial entities which may cause a loss of confidentiality and integrity of information. Based upon USPTO's threat assessment the Agency has implemented baseline of security controls to mitigate these risks to sensitive information to an acceptable level. USPTO has policies, procedures and training to ensure that employees are aware of their responsibility of protecting sensitive information and the negative impact on the agency if there is a loss, misuse, or unauthorized access to or modification of sensitive private information. USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees.

12.2 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.

12.3 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.

Points of Contact and Signatures

Approval Number: 09082513409082

System Owner Name: Jimmy Orona III Office: Branch Chief – Software Services Branch 2 (I/SSB2) Phone: (571) 272-0673 Email: Jimmy.Orona@uspto.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Orona, Jimmy III approved on 2025-09-19T08:48:52.1052429 Date signed: 9/19/2025 8:48:00 AM	**Chief Information Security Officer** Name: Timothy S. Goodwin Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-0653 Email: Timothy.Goodwin@uspto.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Goodwin, Timothy approved on 2025-09-19T14:56:52.6869299 Date signed: 9/19/2025 2:56:00 PM
Privacy Act Officer Name: Ezequiel Berdichevsky Office: Office of General Law (O/GL) Phone: 571) 270-1557 Email: Ezequiel.Berdichevsky@uspto.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: Berdichevsky, Ezequiel approved on 2025-09-16T08:37:53.2527302 Date signed: 9/16/2025 8:37:00 AM	**Bureau Chief Privacy Officer and Authorizing Official** Name: Deborah Stephens Office: Office of the Deputy Chief Information Officer (I/DCIO) Phone: (571) 272-9410 Email: Deborah.Stephens@uspto.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: Stephens, Deborah approved on 2025-09-23T08:28:58.0911344 Date signed: 9/23/2025 8:28:00 AM