Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Patent End to End (PE2E) System

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

Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry
Date: 2022.03.14 09:30:04 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Patent End to End (PE2E) System

Unique Project Identifier: PTOP-003-000

Introduction: System Description

Provide a brief description of the information system.

Patents End-to-End (PE2E) is a Master system portfolio consisting of next generation Patents Automated Information Systems (AIS). The goal of PE2E is to make the interaction of USPTO's users as simple and efficient as possible in order to accomplish user goals. PE2E will be a single web-based examination tool providing users with a unified and robust set of tools. PE2E will overhaul the current patents examination baseline through the development of a new system that replaces the existing tools used in the examination process. The project stakeholders desire a simple, unified interface that does not require launching of separate applications in separate windows, and that supports new and improved IT advances. There are 14 sub-systems under PE2E: DAV, OPD, CPC-DB, P-GD-PAD, P-OA2XML, P-ELP, PE2E-Search, OC, Patent Center, CEDR INFRA, S-DWP, S-OPSG, SLIC and P-STAR.

- **PE2E Docket Application Viewer (DAV)**

Patents End to End (PE2E) Docket Application Viewer (DAV) is an automated information system (AIS) that provides a set of useful tools for the Patent examiners to manage and process the patent application in USPTO. The purpose of PE2E DAV is to provide examination tools for patent examiners to track and manage the cases in their docket and view documents in image and text format.

- **Cooperative Patent Classification (CPC-DB)**

CPC is an International Patent Classification (IPC) based bilateral classification system that is jointly managed and maintained by the European Patent Office (EPO) and USPTO. The conversion from European Classification to Cooperative Patent Classification ensures IPC compliance and eliminates EPO requirement to classify U.S. patent documents. The USPTO conversion provides an up-to-date internationally compatible classification system. CPC periodically receives non-sensitive PII files from USPTO contractors from SERCO Patent Processing System (PPS). Also, CPC receives non-sensitive PII (i.e., USPTO and EPO Employee names, job titles and email address from CEDR-INFRA (formerly PALM-INFRA).

- **One Portal Dossier (OPD)**

OPD is an IP5 collaborative platform initiative based on the international agreement between the IP5 Offices (Japan Patent Office [JPO], Korean Intellectual Property Office [KIPO], EPO, Chinese Patent Office [SIPO], and USPTO), to share non-sensitive patent data search and examination results held by each office for the purpose of facilitating inter-office collaboration amongst IP5 and USPTO Examiners/Officers only.

- **Patent Global Dossier Public Access Dossier (P-GD-PAD)**

P-GD-PAD is a set of business services aimed at modernizing the global patent system and delivering benefits to all stakeholders through a single portal/user interface to all stakeholders with a secure one-stop USPTO-hosted User Interface that accesses related applications across the IP5 offices. The current users of P-GD-PAD are USPTO and IP5patent examiners/officers. P-GD-PAD receives non-sensitive PII (i.e., name, correspondence address, and telephone number) from CEDR-INFRA (formerly PALM- INFRA).

- **Patents Office Action to XML (P-OA2XML)**

P-OA2XML performs continuous automated conversion of previous Office Actions (Microsoft Word format) into Extended Markup Language (XML) format and captures/converts newly submitted official office actions into XML format as well. P-OA2XML processes and stores non-sensitive PII (i.e., applicant/examiner name, phone number, correspondence address) for public correspondence.

- **Patents - Electronic Library for Patents (P-ELP)**

The P-ELP system maintains a content repository for USPTO's patent application images and patent-related text files and provides a means to store a variety of content forms. P-ELP also serves as a back-end service provider with no user interface.

- **Patent End to End Search (PE2E- search)**

The Search for Patents (Search4P) system is a patent examiner search tool that replaces legacy search tools (Examiners Automated Search Tool (EAST) and the Web-based Examiners Search Tool (WEST)). Search4P contains patent published applications (US and foreign) and published nonpatent literature (i.e., books, articles, published research).

- **Official Correspondence (OC)**

OC is a workflow tool which enables patent examiners and automation specialists to create and manage official office action text and forms as outgoing patent correspondence to patent applicants and their attorneys. OC receives non-sensitive PII pertaining to USPTO employees (examiners) and applicants (i.e., name, examiner employee ID correspondence address, telephone number, fax, location, worker type code, and job class code) from CEDR-INFRA (formerly PALM-INFRA) for correspondence purposes; however, only employee IDs (examiner) are stored within the OC database.

- **Patent Center (PCTR)**

PC is a web-based patent application and document submission tool to enable external users to file and manage their patent application.

- **Central Enterprise Data Repository Infrastructure (CEDR INFRA)**

CEDR INFRA is transitioning as the replacement of the legacy PALM INFRA and is a next generation back-end database. CEDR INFRA maintains USPTO employee and contractor information such as names, date and place of birth, social security numbers (SSN) (all 9-digits for federal employee and the last 2-digits for contractor employees), employee ID, worker number, locations, organization, and correspondence address. It also provides functionalities to capture site, building, floor, classifications and search rooms. This information is required for

subsequent Patent subsystems that track patent application prosecution, the location of the application, and Group Art Unit and Examiner productivity. CEDR INFRA synchronizes USPTO (federal) employee's information from the National Finance Center's (NFC) personnel/payroll system for pay purposes only.

- **Services – Document Wrapper for Patents (S-DWP)**

S-DWP is a collection of business layer services that provides Patent next generation applications with backwards compatibility access to unpublished and published patent application images which are currently maintained on the legacy IFW system.

- **One Patent Service Gateway (S-OPSG)**

The One Patent Services Gateway (S-OPSG) is the next-generation data services hub for USPTO Patent Applications. S-OPSG is unifying and replacing a plethora of legacy PALM and PALM-EXPO Enterprise Java Bean (EJB) and Simple Object Access Protocol (SOAP) web services with secure, high-performance RESTful services. These RESTful services will present as a set of unified interfaces defined by the Patent Common Domain Model (PCDM) and with improved auditing by the Patent History Service (PHS).

- **Patent -Service for time and Application Routing_(P-STAR)**

P-STARS is an application information system that provides the organization with a better understanding of factors that impact examination times and helps the agency to make more informed decisions about examination time. By using CPC and historical PALM data, the P-STAR system will determine each examiner's proficiency with a given subject matter and attempt to use that data to assign future work to their docket, freeing Supervisors from performing that step manually.

- **Sequence Listing Information Control (SLIC)**

SLIC (Sequence Listing Information Control) is the processing system for DNA, RNA & Protein Sequence Listings following ST.23, ST.25 and ST.26 international standards, and in accordance with 37 CFR §§ 1.821 – 1.825 "Application Disclosures Containing Nucleotide and/or Amino Acid Sequences". SLIC performs compliance verification of sequence listings in ST.23, ST.25 and ST.26 formats, and provides a workflow for review and data transformation for downstream intake components including Patents Content Management and Patent Search repositories.

Address the following elements:

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

PE2E is a major application.

(b) System location

Madison building 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)

PE2E interconnects with the following:

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

Enterprise Desktop Platform (EDP): is an infrastructure information system, which provides a standard enterprise-wide environment that manages desktops and laptops running on the Windows 7 and 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.

Security and Compliance Services (SCS): SCS 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 Windows Services (EWS): is an Infrastructure information system, and provides a hosting platform for major applications that support various USPTO missions.

Network and Security Infrastructure (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.

Enterprise Software Services (ESS): is an Infrastructure information system and provides a variety of services to support USPTO missions.

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

Trilateral Network (TRINET): is an Infrastructure information system, and provides secure network connectivity for electronic exchange and dissemination of sensitive patent data between authenticated endpoints at the Trilateral Offices and TRINET members.

Serco Patent Processing System (Serco-PPS): is a contractor system that receives information from USPTO so that inventory, identification and classification activities can be performed on patent applications.

Patent Capture and Application Processing System – Examination Support (PCAPS ES): is a master system that provides a comprehensive prior art search capability and the retrieval of patent and related information, which comprise text and images of United States (US), European Patent Office (EPO) and Japan Patent Office (JPO patents), US pre-grant publications, Derwent data and IBM Technical Disclosure Bulletins.

Patent Capture and Application Processing System – Initial Processing (PCAPS IP): is an Application information system, and provides support to the USPTO for the purposes of capturing patent applications and related metadata in electronic form; processing applications electronically; reporting patent application processing and prosecution status; and retrieving and displaying patent applications.

Patent Search System – Primary Search and Retrieval (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): is made up of multiple applications that allow Patents examiners and applicants to effectively search the USPTO Patent data repositories.

Service Orientated Infrastructure (SOI): is an infrastructure system that provides a feature-rich and stable platform upon which USPTO applications can be deployed.

Data Storage Management System (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

Cooperative Patent Classification (CPC): is an information system deployed within the AWS East Region IaaS, and is a shared repository for all patents schemes approved by the United States Patent and Trademark Office (USPTO) and the European Patent Office (EPO). The intent is to provide another resource for the patent examiners in their work.

Patent Automation Application to Docket Worker Management - Examination and Post-Examination (PALM-EXPO): supports the production of reports related to examination and publication processes. PALM-EXPO interfaces with Revenue Accounting and Management (RAM), Patent Application Security System (PASS), and other PALM subsystems. PALM-EXPO also provides external services for PASS, and eDAN to enable these components to access PALM data.

Storage Infrastructure Management (SIMS): provides access to consolidated, block level data storage and files system storage.

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

Patent End to End (PE2E) is a Master system portfolio consisting of next generation Patents Automated Information Systems (AISs) which process applications for the issuance and granting of U.S. Patents. The goal of PE2E is to make the interaction of USPTO's users as simple and efficient as possible in order to accomplish user goals.

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

Registered patent applicants are provided with unique user accounts to facilitate subsequent secure logins for their application status and update submissions. Patent examiners are granted access to only the patent applications that have been assigned to them.

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

Hypertext Transfer Protocol Secure (HTTPS) is used for all data transmissions to and from the Internet, USPTO DMZ, and PTOnet.

(g) Any information sharing

PE2E receives information from USPTO authorized contractor facilities SERCO PPS to support the USPTO patent application process (no PII is shared with SERCO PPS). OPD and CPC systems enable patent data searches and ensure that examination results are available to be shared between the International Intellectual Property Offices under an international agreement and applicable legal authorities to promote work-sharing and redundancy reduction. Information is shared within the bureau, with the public, with the private sector, and with foreign governments.

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

- Leahy-Smith America Invents Act, 2011
- 37 C.F.R. 1, United States Patent and Trademark Office, Department of Commerce
- 5 U.S.C. 301, Departmental Regulations
- 35 U.S.C.

(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: The SSNs for USPTO employees are cross-referenced to a USPTO HR assigned employee ID. Federal employee SSNs are 9-digits and contractors are the last 2-digits of the SSN. Federal employee SSNs are mandatory key identifiers that facilitate federal personnel data synchronization between USPTO HR payroll and the National Finance Center (NFC) only. The contractor's last two digits of the SSN are minimum administrative requirements for unique employee ID assignment.					

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): Fax Number, Organization Name, Job Class Code, Supervisor Indicator, Worker Type Code.					

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.

PE2E is secured using appropriate administrative, physical, and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, and auditing). Mandatory IT awareness and role-based training is required for staff who have access to the system and address how to handle, retain, and dispose of data. All access has role-based restrictions and individuals with privileges have undergone vetting and suitability screen. The USPTO maintains an audit trail and performs random, periodic reviews (quarterly) to identify unauthorized access and changes as part of verifying the integrity of administrative account holder data and roles.

PE2E employs system checks to ensure accuracy, completeness, validity, and authenticity. Each PE2E component has established specific rules or conditions for checking the syntax of information input to the system such as numbers or text; numerical ranges and acceptable values are utilized to verify that inputs match specified definitions for format and content.

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. 0651-0031 Patent Processing 0651-0032 Initial Patent Processing 0651-0033 Post Allowance and Refilling 0651-0035 Representative and Address Provisions 0651-0071 Matters Related to First Inventor to File
☐	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):			

☒	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): Non-sensitive PII (correspondence information) is collected to facilitate processing and/or patent application examination submissions and issuance of U.S. patent to a patent applicant. Sensitive PII (i.e., SSN) is captured in order for HR to assign a unique employee ID number for federal and contractor employees. The employee ID is used instead of the SSN for identifying employees internally. CEDR INFRA captures federal employees' 9-digit SSNs and for contractor employees the last 2-digits of their SSNs and is not shared publicly			

but is used by USPTO HR and National Finance Center for synchronizing federal employee identification and validation for pay purposes only.

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).

Federal employee: PE2E collects and maintains USPTO federal employees' PII (name, date of birth, SSN (9-digit), place of birth, employee ID, home and email address, and telephone number) for internal use only. This information is not shared with the public. Specifically, federal employee's SSN facilitates USPTO HR and National Finance Center employee data synchronization and payroll validation only. Payroll data is not collected within PE2E system boundary. PE2E also collects and maintains federal employee's work-related information (occupation, job title, work address, telephone number, email address, fax, organization name, job class code, worker type code etc.) for employee management (i.e., employee work assignment, crediting work to employees, and organizing employees (e.g. I work for this supervisory patent examiner in Art Unit 1234 in Tech Center 000 for Director overseeing those Art Units – organizational management). Only the examiner's name, fax, telephone number, job title, email address is publicly shared for correspondence.

Patent applicant: Patent applicants or representatives provide name, mailing and/or email address, and phone number to facilitate correspondence. The minimum information for publication, patent grants and pre-grant publication are name and residence; however, once a patent is granted the patent applicant's name and residence (city, state) is included with the patent for public record.

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.)

The threats to privacy are insider threats, and foreign governments. USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees. The annual training has made all employees aware of the possibility of insider threats and threats from adversarial or foreign entities and how these bad actors can affect USPTO's reputation. The following are USPTO's current policies that are adhered to: IT Privacy Policy (OCIO-POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), and USPTO Rules of the Road (OCIO-POL36). The combination of USPTO trainings and policies will help USPTO employees to recognize insider threats and threats from adversarial or foreign entities. 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.

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: DSMS SCS SIMS TRINET PCAPS-ES PCAPS-IP PSS-SS SERCO-PPS PSS-PS ESS PE2E has put certain security controls 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. The following are current USPTO policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy (OCIO- POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), USPTO Rules of the Road (OCIO-POL- 36). 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: ___http://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: Individuals grant consent by completing and submitting a patent application for processing/examination. They are notified that if a patent is granted, the information that they submitted will become public information. Individuals may decline to provide PII by not submitting an application for processing.
☐	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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: Submitting personal information is voluntary. When you voluntarily submit information, it constitutes your consent to the use of the information for the purpose(s) stated at the time of collection. Should there ever be a need to use information for a purpose other than one already provided for under the Privacy Act, we will give you specific instructions on how you may consent to such use. You are never required to give such consent.
☐	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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

☒	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals will need to work with USPTO to update their records if contact information changes.
☐	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

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

☐	All users signed a confidentiality agreement or non-disclosure agreement.

☒	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: By reviewing 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): _____6/4/2021_____ ☐ 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 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).
☒	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): All sensitive-PII at-rest and in-transit are protected in accordance with NIST recommended encryption.

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).*

Adversarial entities, foreign governments, insider threats and inadvertent private information exposure are all risks and 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. The following are current USPTO policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy (OCIOPOL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), USPTO Rules of the Road (OCIO-POL- 36). 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.

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 authorize personnel. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access.

Additionally, PE2E 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. All sensitive-PII at-rest and in-transit is protected in accordance with NIST recommended encryption.

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)*: • Patent Application Files-COMMERCE/PAT-TM-7 • Patent Assignment Records-COMMERCE/PAT-TM-9 • Petitioners for License to File for Foreign Patents-COMMERCE/PAT–TM–13 • USPTO PKI Registration and Maintenance System—COMMERCE/PAT—TM—16 • Employee Personnel Files Not Covered by Notices of Other Agencies-COMMERCE/DEPT-18 • Attendance, Leave, and Payroll Records of Employees and Certain Other Persons—COMMERCE/DEPT-1 • Access Control and Identity Management System-COMMERCE/DEPT 25
☐	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.)*

☒	There is an approved record control schedule. Provide the name of the record control schedule: • Evidentiary Patent Applications N1-241-10-1:4.1 • Patent Examination Working Files N1-241-10-1:4.2 • Patent Examination Feeder Records N1-241-10-1:4.4 • Patent Post-Examination Feeder Records N1-241-10-1:4.5 • Patent Case Files, Granted N1-241-10-1:2 • Abandoned Patent Applications, Not Referenced in Granted Case File N1-241-10-1:3
☐	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 SSN and employee name captured by the PE2E (CEDR INFRA) specifically identifies employees. Name, mailing address, phone number, and email address for SLIC.
☒	Quantity of PII	Provide explanation: Approximately 47K rows of data associated with the following PII columns "Birth Date, Birth Country, Birth City, Birth State and SS".
☒	Data Field Sensitivity	Provide explanation: PII stored in the system is data collected from USTPO employees and contractor personnel in which the information is confidential and unique to those individuals. Any unauthorized access, modification, and/or disclosure of sensitive data would have a Moderate impact on the organization and its operations.
☒	Context of Use	Provide explanation: The data captured, stored, or transmitted by the PE2E system is used to process patent applications and may

		include sensitive information from the applicant's application correspondence. The sensitive PII data maintained by CEDR INFRA is restricted for USPTO HR and the National Finance Center payroll administration only. The data traversing SLIC facilitates patent application prosecution and may include non-sensitive information (i.e. applicant/examiner correspondence info).
☒	Obligation to Protect Confidentiality	Provide explanation: USPTO examiners are obligated to protect applicants' identity and application while the application is undergoing patent prosecution.
☒	Access to and Location of PII	Provide explanation: The information captured, stored, and transmitted by the PE2E system is accessed within USPTO on-campus systems. Sensitive PII (SSN) are located only on USPTO on-campus systems.
☐	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.)

Nation states, adversarial entities, and insider threats are the predominant threats to the information collected and its privacy. Security controls following FedRAMP and NIST guidance were implemented to deter and prevent threats to privacy. USPTO has identified and evaluated potential threats to PII such as loss of confidentiality and integrity of information. Based upon USPTO's threat assessment policies, procedures, and training has been implemented to ensure that employees are aware of their responsibility to protect PII and to be aware of insider threats. Our employees are aware of the negative impact to the agency if there is a loss, misuse, or unauthorized access to or modification of PII.

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

System Owner
Name: Huong Esposo
Office: Office of Patent Automation (P/OPA)
Phone: (571) 272-5685
Email: Huong.Esposo@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: Users, Esposo, Huong Digitally signed by Users, Esposo, Huong Date: 2022.03.08 14:35:05 -05'00'

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

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: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2022.03.09 09:34:12 -05'00'

Date signed: _____

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: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2022.03.07 10:02:05 -05'00'

Date signed: _____

Bureau Chief Privacy Officer and Co-Authorizing Official

Name: Henry J. Holcombe
Office: Office of the Chief Information Officer (OCIO)
Phone: (571) 272-9400
Email: Jamie.Holcombe@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: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2022.03.09 10:22:23 -05'00'

Date signed: _____

Co-Authorizing Official
Name: Andrew Faile
Office: Office of the Commissioner for Patents
Phone: (571) 272-8800
Email: Andrew.Faile@uspto.gov

I certify that this PIA accurately reflects the representations made to me herein by the System Owner, the Chief Information Security Officer, and the Chief Privacy Officer regarding security controls in place to protect PII/BII in this PIA.

Signature: Users, Faile, Andrew Digitally signed by Users, Faile, Andrew Date: 2022.03.10 12:56:49 -05'00'

Date signed: _____

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.