

**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: 2024.05.02 19:24:35 -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-003-00**

### **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. PE2E unifies the interface and does not require launching of separate applications in separate windows, and that supports new and improved IT advances. There are 12 sub-systems under PE2E:

- **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.

- **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).

- **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.

- **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 Center (PCTR)**

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

- **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).

- **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.

- **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.

- **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.
- **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.
- **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.

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*

PE2E is located at USPTO 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)*

PE2E interconnects with the following:

**Cooperative Patent Classification (CPC):** 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.

**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 program.

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

**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.

**Enterprise UNIX Services (EUS):** Consists of assorted UNIX Operating System (OS) variants, each comprised of many utilities along with the master control program, the kernel.

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

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

**Fee Processing Next Generation (FPNG):** Fee management and revenue collection system a for USPTO.

**ICAM Identity as a Service (ICAM-IDaaS):** Provides an enterprise authentication and authorization service to all applications/AIS's.

**MyUSPTO Cloud:** Reduces the number of logins for external USPTO customers and to provide a single location from where they can conduct their business with the USPTO.

**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.

**Patent Business Management Information (PBMI):** Facilitates and supports examiner production, quality assurance, and report dissemination to USPTO employees and contractors.

**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 – Specialized Search and Retrieval (PSS SS):** The PSS-SS system is made up of multiple applications that allow Patents examiners and applicants to effectively search the USPTO Patent data repositories.

**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.

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

**Storage Infrastructure Managed Service (SIMS):** Provides access to consolidated, block level data storage and files system storage.

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

**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.

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

PE2E will be a single web-based examination tool providing users with a unified and robust set of tools.

*(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.)*

<b>Changes That Create New Privacy Risks (CTCNPR)</b>					
a. Conversions	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>	g. New Interagency Uses	<input type="checkbox"/>
b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input type="checkbox"/>	h. Internal Flow or Collection	<input type="checkbox"/>
c. Significant System Management Changes	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character of Data	<input type="checkbox"/>
j. Other changes that create new privacy risks (specify):					

- ☐ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.
- ☒ 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.)*

<b>Identifying Numbers (IN)</b>					
a. Social Security*	<input checked="" type="checkbox"/>	f. Driver's License	<input checked="" type="checkbox"/>	j. Financial Account	<input type="checkbox"/>
b. Taxpayer ID	<input checked="" type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input type="checkbox"/>
c. Employer ID	<input checked="" type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
d. Employee ID	<input checked="" type="checkbox"/>	i. Credit Card	<input type="checkbox"/>	m. Medical Record	<input type="checkbox"/>
e. File/Case ID	<input checked="" type="checkbox"/>				
n. Other identifying numbers (specify):					
<p>*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:</p> <p>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.</p>					

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

<b>Work-Related Data (WRD)</b>					
a. Occupation	<input checked="" type="checkbox"/>	e. Work Email Address	<input checked="" type="checkbox"/>	i. Business Associates	<input type="checkbox"/>
b. Job Title	<input checked="" type="checkbox"/>	f. Salary	<input type="checkbox"/>	j. Proprietary or Business Information	<input type="checkbox"/>



c. Work Address	<input checked="" type="checkbox"/>	g. Work History	<input type="checkbox"/>	k. Procurement/contracting records	<input type="checkbox"/>
d. Work Telephone Number	<input checked="" type="checkbox"/>	h. Employment Performance Ratings or other Performance Information	<input type="checkbox"/>		
l. Other work-related data (specify): Fax Number, Organization Name, Job Class Code, Supervisor Indicator, Worker Type Code.					

<b>Distinguishing Features/Biometrics (DFB)</b>					
a. Fingerprints	<input type="checkbox"/>	f. Scars, Marks, Tattoos	<input type="checkbox"/>	k. Signatures	<input type="checkbox"/>
b. Palm Prints	<input type="checkbox"/>	g. Hair Color	<input type="checkbox"/>	l. Vascular Scans	<input type="checkbox"/>
c. Voice/Audio Recording	<input type="checkbox"/>	h. Eye Color	<input type="checkbox"/>	m. DNA Sample or Profile	<input type="checkbox"/>
d. Video Recording	<input type="checkbox"/>	i. Height	<input type="checkbox"/>	n. Retina/Iris Scans	<input type="checkbox"/>
e. Photographs	<input type="checkbox"/>	j. Weight	<input type="checkbox"/>	o. Dental Profile	<input type="checkbox"/>
p. Other distinguishing features/biometrics (specify):					

<b>System Administration/Audit Data (SAAD)</b>					
a. User ID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>	e. ID Files Accessed	<input checked="" type="checkbox"/>
b. IP Address	<input checked="" type="checkbox"/>	f. Queries Run	<input checked="" type="checkbox"/>	f. Contents of Files	<input checked="" type="checkbox"/>
g. Other system administration/audit data (specify):					

<b>Other Information (specify)</b>

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

<b>Directly from Individual about Whom the Information Pertains</b>					
In Person	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input checked="" type="checkbox"/>	Online	<input checked="" type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		
Other (specify):					

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

<b>Non-government Sources</b>					
Public Organizations	<input checked="" type="checkbox"/>	Private Sector	<input checked="" type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input checked="" type="checkbox"/>		

Other(specify):
-----------------

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

<p>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.</p>
--

<p>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.</p>
--

### 2.4 Is the information covered by the Paperwork Reduction Act?

<input checked="" type="checkbox"/>	<p>Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.</p> <p>0651-0031 Patent Processing 0651-0032 Initial Patent Processing 0651-0033 Post Allowance and Refiling 0651-0035 Representative and Address Provisions 0651-0071 Matters Related to First Inventor to File</p>
<input type="checkbox"/>	No, the information is not covered by the Paperwork Reduction Act.

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

Technologies Used Containing PII/BII Not Previously Deployed (TUCPNPD)			
Smart Cards	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other(specify):			

<input checked="" type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
-------------------------------------	--

## **Section 3: System Supported Activities**

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

Activities			
Audio recordings	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other(specify): <a href="#">Click or tap here to enter text.</a>			

<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	For administering human resources programs	<input checked="" type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input checked="" type="checkbox"/>
For litigation	<input checked="" type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>
For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input checked="" type="checkbox"/>	For employee or customer satisfaction	<input type="checkbox"/>
For web measurement and customization technologies (single-session)	<input type="checkbox"/>	For web measurement and customization technologies (multi-session)	<input type="checkbox"/>
Other(specify):  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-POL-36). 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.

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 adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.

## **Section 6: Information Sharing and Access**

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

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Private sector	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

<input type="checkbox"/>	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?

<input type="checkbox"/>	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input checked="" type="checkbox"/>	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	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.

<input checked="" type="checkbox"/>	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:</p> <p>DSMS SCS SIMS TRINET PCAPS-ES PCAPS-IP PSS-SS SERCO-PPS PSS-PS ESS</p> <p>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 adhere to the USPTO Records</p>
-------------------------------------	--

	Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.
<input type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 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	<input checked="" type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
Other (specify):			

## **Section 7: Notice and Consent**

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

<input checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input checked="" type="checkbox"/>	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: <a href="https://www.uspto.gov/privacy-policy">https://www.uspto.gov/privacy-policy</a>	
<input type="checkbox"/>	Yes, notice is provided by other means.	Specify how:
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

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

<input type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
--------------------------	---	--------------

<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Individuals do not have the opportunity to decline to provide PII/BII. The PII/BII is required to process an application. By declining to provide PII/BII the individual would not be able to submit an application for processing. The individuals 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.
-------------------------------------	---	---

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

<input type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: The PII/BII requested is required for the processing of an application. When an individual submits information, it constitutes their 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.

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

<input type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Individuals can not update their information directly in PE2E after submission however, Individuals can work with USPTO to update their records if contact information changes.

## **Section 8: Administrative and Technological Controls**

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

<input checked="" type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: By reviewing Audit Logs
<input checked="" type="checkbox"/>	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): 2/24/2023 <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input checked="" type="checkbox"/>	Contracts with customers establish DOC ownership rights over data including PII/BII.
<input checked="" type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input checked="" type="checkbox"/>	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).

<p>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 an 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.</p> <p>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.</p> <p>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.</p>
---

## **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."

<input checked="" type="checkbox"/>	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i>  Patent Application Files- <a href="#">COMMERCE/PAT-TM-7</a> Patent Assignment Records- <a href="#">COMMERCE/PAT-TM-9</a> Petitioners for License to File for Foreign Patents- <a href="#">COMMERCE/PAT-TM-13</a> USPTO PKI Registration and Maintenance System- <a href="#">COMMERCE/PAT-TM-16</a> Employee Personnel Files Not Covered by Notices of Other Agencies- <a href="#">COMMERCE/DEPT-18</a> Attendance, Leave, and Payroll Records of Employees and Certain Other Persons— <a href="#">COMMERCE/DEPT-1</a> Access Control and Identity Management System- <a href="#">COMMERCE/DEPT 25</a>
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on (date).
<input type="checkbox"/>	No, this system is not a system of records and a SORN is not applicable.

## **Section 10: Retention of Information**

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

<input checked="" type="checkbox"/>	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
<input type="checkbox"/>	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:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

<b>Disposal</b>			
Shredding	<input checked="" type="checkbox"/>	Overwriting	<input checked="" type="checkbox"/>
Degaussing	<input checked="" type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
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.)*

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

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

<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	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".
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	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).
<input checked="" type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation: USPTO examiners are obligated to protect applicant's identity and application while the application is undergoing patent prosecution.
<input checked="" type="checkbox"/>	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.

<input type="checkbox"/>	Other:	Provide explanation:
--------------------------	--------	----------------------

**Section 12: Analysis**

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

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.

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

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

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