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

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

Reviewed by: John B. Owens, II, Bureau Chief Privacy Officer

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Catrina D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2016.12.01 15:12:03 -05'00'

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)

Unique Project Identifier: PTOP-003-000

Introduction: **System Description**

Provide a description of the system that addresses the following elements:

(a) a general description of the information in the system

Patent End to End (PE2E) is a Major Application (MA) consisting of next generation 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. PE2E is 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 Federal Information Processing Standard (FIPS) 199 security categorization for PE2E is Moderate. The following AIS' comprise the PE2E master system:

- **PE2E Docket Application Viewer (DAV):** DAV is an AIS that provides a set of useful tools for the Patent examiners to manage and process the patent application in USPTO. The purpose of 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. The users of DAV are USPTO patent examiners and managers. DAV does not interface with any other systems at USPTO for data exchange. A connection to the PALM-INFRA database for data transfer happens occasionally, but the connection is not constant. No SSNs are collected or maintained from PALM-INFRA.

- **Cooperative Patent Classification (CPC)**
  As part of USPTO's PE2E strategic initiative, the CPC establishes the processes and systems to support exchange of data between USPTO and European Patent Office (EPO) for the new CPC System. CPC is an IPC-based bilateral classification system that will be jointly managed and maintained by the EPO and USPTO. The CPC System will have a replicated database for CPC data (Classification Symbols, Class Definitions, Classification Schemes, and Symbol Allocations) residing at USPTO and EPO. The conversion from ECLA to CPC at the EPO will ensure IPC compliance and eliminate the need for the EPO to classify U.S. patent documents. At the USPTO, the conversion will provide an up-to date classification system that is internationally compatible. CPC picks up files that USPTO Reed Technology and Information Services (RTIS) Patent Data Capture (PDCap)/SERCO Patent Processing System (PPS) send (no PII is shared with RTIS and SERCO).

USPTO and EPO Employee Names, Job Titles, and Email Addresses are received from PALM-INFRA. No SSNs are collected or maintained from PALM-INFRA.

- **One Portal Dossier (OPD)**
  OPD provides a new collaborative platform through the implementation of the OPD Specification, an IP5 initiative based on the international agreement between the IP5 Offices (Japan Patent Office [JPO], Korean Intellectual Property Office [KIPO], European Patent Office [EPO], Chinese Patent Office [SIPO], and USPTO), to share patent data search and examination results held by each office for the purpose of facilitating inter-office work sharing.

  OPD provides the following services that will be consumed by the IP5 offices and a Test Harness used for testing all services:

  - OPD DocList Service: providing metadata of the list of available documents associated with a patent application number provided as input.

  - OPD DocContent Service: providing content, in PDF format, of each document of the list provided by DocList service.

  - OPD Citation & Classification Service: all citation and classification information for a given patent application.

  - OPD Web Test Harness: tool for testing EPO Patent Family and DocList/DocContent and citation/classification services offered by all IP5 offices: EPO, JPO, KIPO, SIPO and USPTO.

  This mutual collaboration will promote work-sharing, reducing redundant work among IP5 Office examiners while examining Patent Applications that are members of the same Patent Family. The users of OPD are IP5 and USPTO Examiners/Officers.

- **Patent Global Dossier Public Access Dossier (P-GD-PAD)**
  P-GD-PAD is an application that provides backend services to support modernizing the global patent system and delivering benefits to all stakeholders with secure, one-stop access to related applications across the IP5 offices.

  The objectives of the Public Access to Foreign Application Dossiers project are as follows:
  - Provide a means to process OPD requests from public users sent via the IP5 offices which access USPTO file wrapper content using existing USPTO OPD services.
  - Ensure that the additional demand for US file wrapper content will not degrade the level of performance delivered for patent examiner requested OPD transactions
  - Develop a web base user interface leveraging Public PAIR and OPD services that provides access to dossiers of IP5 patent applications that are in the same family as a US Patent Application.
  - Enhance OPD monitoring and reporting capabilities for system administration and performance management and business manager informational needs.

The users of OPD are USPTO and IP5 Examiners/Officers. P-DG-PAD receives but does not store the PII (Name, Home Address, and Telephone Number) from calling the PALM-INFRA web service.

- **Patents Office Action to XML (P-OA2XML)**
  This project falls under the AIS known as Office Action Correspondence Subsystem (OACS). OACS is a system built on a Microsoft Word platform. Converting existing Office Action data to XML builds upon OACS, allowing patent examiners and applicants the capability to correspond in the next generation system – PE2E. With this project, the MS Word Document versions of completed Office Actions (backfile/continuous data capture (CDC)) that are stored by OACS would be accessed, converted to XML4IP version 2 and uploaded into the content management system for text. The production-ready deliverable is to release migrated XML data into text CMS. USPTO Patent Examiners are the users of P-OA2XML.

- **Patents - Electronic Library for Patents (P-ELP)**
  The CMS Foundation and Migration Project will deploy the next-generation content repository for USPTO's patent application images and patent-related text files and provide a means to store a variety of different forms of content in the future, known as the Electronic Library for Patents (ELP). This system will address the Patent business need to increase document availability, support a nationwide distributed workforce and improve the consistency of performance for content users. The P-ELP system will support the migration of 8% - 10% of the IFW data into the P-ELP. Additionally, the project will support the integration of the Convert Existing Office Action to XML project (OA2XML). The users of P-ELP are the Office of Initial Patent Examination; all Patent Examiners, Supervisory Patent Examiners (SPEs) and Legal Instrument Examiners (LIEs).

  P-ELP is a back end service provider with no user interface; thus no PII is collected.

- **Search For Patents (Search4P)**
  The Search For Patents (Search4P) system is a search tool that reproduces the best aspects of the current patent search tools but presents a modern interface design and will introduce new tools and capabilities. This particular project will further develop the search application already built with the previous projects and will bring it to where it is ready to deploy to a subset of the Examining Corps, but not as a full replacement of the existing search tools. Search4P, formerly known as Exploring Search Technologies (EST) or Patent Application Search and Retrieval (PASR) will replace current search tools, Examiners Automated Search Tool (EAST) and the Web-based Examiners Search Tool (WEST). These systems are over ten years old and are not compatible with the new Patent End to End (PE2E) architecture that is being developed. The new tool provides similar functionality to EAST and WEST, but with a more modern, intuitive user interface and flexible, scalable software architecture. The Search4P search tool developed under the Patent End to End program will provide examiners all the data and functionality required to complete their examining work as well as new search features

that enhance current capabilities. The users of Search4P are the Patent Examiners, DB Admins, and Developers.

Based on the Search4P PTA, signed 7 January 2016, Search4P does not collect, maintain, or disseminate information in identifiable form from or about members of the public or companies or other business entities.

- **Official Correspondence (OC)**
  The OC application provides the document authoring and workflow management components of this PE2E suite of applications. Patent Examiners will use the OC application to create the official correspondence packages consisting of forms and correspondence that go back to the patent applicant. The examiner supervisors will use the OC application to review and approve the official correspondence before it is sent out. The OC application utilizes Microsoft Word 2013 as its base authoring tool and the USPTO Hierarchal Finite State Machine (HFSM) as it base workflow management tool. The OC application will then interface with and leverage numerous other USPTO enterprise systems including Role Based Access Control (RBAC) for user authentication and roles, Central Enterprise Data Repository (CEDR-INFRA) for data storage, PALM-INFRA for application information, DAV, Content Management System (CMS) for document storage, HFSM for workflow management, Examiner Search Technologies (EST), and BRS for examiner support.

  OC receives PII pertaining to Employees (Name, ID, Email Address, Telephone Number, Fax Number, Location, Worker Type Code, and Job Class Code) from PALM-INFRA; however, only Employee IDs are stored within the OC database. No SSNs are collected or maintained from PALM-INFRA.

- **Patent Center**
  The Modernize Patent eCommerce (eMod) Phase 1 is first of several phases to modernize the eCommerce business area. Currently the eCommerce business area consists of electronic acquisition of patent applications, applicant information retrieval and public search of published patents. The new AIS developed under eMod project is Patent Center which will ultimately replace EFS-Web, Private PAIR and Public PAIR to service as AIS to perform eCommerce business. For the first phase, Patent Center (Release 1.0) will be deployed as the primary processing engine for new text (.DOCX) intake, display and download capability. The user interfaces will continue to be legacy systems EFS-Web and Private PAIR. Patent Center host a set of services to convert, save and handle text (.DOCX) documents that are consumed by the legacy systems.

- **Global Patent Search Network (GPSN)**
  As a result of cooperative effort between the USPTO and State Intellectual Property Office (SIPO) of the People's Republic of China, GPSN provides public access to Chinese patent documentation for search and retrieval via the cloud. This tool will enable the user to search Chinese patent documents in the English or Chinese language. The data available include full-text Chinese patents and machine translations. Also available are full document images of Chinese patents which are considered the

authoritative Chinese patent document. Users can search documents including published applications, granted patents and utility models, all which contain non-PII public Chinese information.

(b) a description of a typical transaction conducted on the system

PE2E collects and maintains information from patent applicants (inventors) or their legal representative as well as Federal employees as part of the patent application submission and examination process. Information from the applicant must be submitted on the patent application form either electronically or in paper copy. PE2E contains information provided as part of the patent application, which includes; full name, address, phone number, email address, and citizenship status of patent applicant (inventor). Additional information is collected for each additional inventory, company, Legal Representative under 35 U.S.C. 117, or Party of Interest under the authority of 35 U.S.C. 118.

Information is collected to examine and issue a U.S. patent to the inventor (patent applicant) as well as uniquely identify the applicant. "This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14."

(c) any information sharing conducted by the system

PE2E receives patent applicant information from PALM-INFRA. Additionally, PE2E receives information from RTIS PDCAP and SERCO PPS to support the USPTO patent application process (no PII is shared with RTIS and SERCO). Via the OPD and CPC systems, patent data search and examination results are available to be shared between the International Intellectual Property (IP) Offices under an international agreement and applicable legal authorities to promote work-sharing and reduction of redundant work.

(d) a citation of the legal authority to collect PII and/or BII

- 5 U.S.C. 301, Departmental Regulations
- 35 U.S.C. 1, Establishment
- 35 U.S.C. 6, Patent Trial and Appeal Board
- 35 U.S.C. 115, Inventor's Oath or Declaration
- 35 U.S.C. 184, Filing of application in foreign country
- 35 U.S.C. 261, Ownership; Assignment
- 35 U.S.C. 371, National Stage: Commencement

(e) the Federal Information Processing Standard (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.)

☒   This is an existing information system in which changes do not create new privacy
         risks. *Continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	☐	d. Significant Merging	☐	g. New Interagency Uses	☐
b. Anonymous to Non-Anonymous	☐	e. New Public Access	☐	h. Internal Flow or Collection	☐
c. Significant System Management Changes	☐	f. Commercial Sources	☐	i. Alteration in Character of Data	☐
j. Other changes that create new privacy risks (specify): There are no new Privacy Risks. This is an annual update to address new Privacy Impact Analysis template requirements.					

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*	☐	e. File/Case ID	☒	i. Credit Card	☐
b. Taxpayer ID	☐	f. Driver's License	☐	j. Financial Account	☐
c. Employer ID	☒	g. Passport	☐	k. Financial Transaction	☐
d. Employee ID	☒	h. Alien Registration	☒	l. Vehicle Identifier	☐
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					
*If SSNs are collected, stored, or processed by the system, please explain if there is a way to avoid such collection in the future and how this could be accomplished:					

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

Work-Related Data (WRD)						
a. Occupation	☒	d. Telephone Number	☒	g. Salary	☐	
b. Job Title	☒	e. Email Address	☒	h. Work History	☐	
c. Work Address	☒	f. Business Associates	☐			
i. Other work-related data (specify): Fax Number, Organization Name, Job Class Code, Supervisor Indicator, Worker Type Code						

Distinguishing Features/Biometrics (DFB)						
a. Fingerprints	☐	d. Photographs	☐	g. DNA Profiles	☐	
b. Palm Prints	☐	e. Scars, Marks, Tattoos	☐	h. Retina/Iris Scans	☐	
c. Voice Recording/Signatures	☐	f. Vascular Scan	☐	i. Dental Profile	☐	
j. 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	☐	d. 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   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			
To determine eligibility	☒	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): PII is collected to process and/or examine patent application submissions and issue a U.S. patent to the inventor (patent applicant).			

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).

PE2E systems process applications for the issuance and granting of U.S. patents. PII data is collected in support of this mission is of the public (U.S. and foreign) and Federal employees. Public data is used to process and/or examine Patent applications and to uniquely identify the Patent applicant. Mailing and email addresses are used for correspondence concerning the application. Federal employee data is used for identification of patent examiners, patent examiner work, management of Federal employees, and the management of the IT systems that support the USPTO.

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   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: • USPTO's PALM-INFRA systems under the Patent Capture and Application Processing System – Examination Support (PCAPS-ES) Master System

☐	- o Information is protected through a layered security approach which incorporates the use of secure authentication, access control, mandatory configuration settings, firewalls, Virtual Private Network (VPN), and encryption, where required. Internally within USPTO, data transmission confidentiality controls are provided by PTOnet. • Reed Technology and Information Services (RTIS) Patent Data Capture (PDCap)/SERCO Patent Processing System (PPS) - o External contractors from RTIS and SERCO connect through secure data transfer. No PII is shared with either system. • World Intellectual Property Organization (WIPO) / Foreign Patent Offices - o For external data transfer to WIPO, data is transmitted across USPTO's Trilateral Network (TriNet) which is a Point-to-Point dedicated Virtual Private Network (VPN)
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3   Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	☒	Government Employees	☒
Contractors	☒		
Other (specify): The general public does not have direct access to the PE2E system, only the public-facing components, through which they will have access to the publically releasable PII stored by the system.			

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 the information that they submit 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: Audit logs
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 12/5/2015 ☐ 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 (POAM).

☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish ownership rights over data including PII/BII.
☒	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

8.2   Provide a general description of the technologies used to protect PII/BII on the IT system.

Personally identifiable information in PE2E is secured using appropriate administrative, physical, and technical safeguards in accordance with the applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

All access has role based restrictions, and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to 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.

Section 9: Privacy Act

9.1   Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C.
        § 552a. *(A new system of records notice (SORN) is required if the system is not covered
        by an existing SORN).*
        As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which
        information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned
        to the individual."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(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 • Employee Personnel Files Not Covered by Notices of Other Agencies-COMMERCE/DEPT-18
☐	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u>.
☐	No, a SORN is not being created.

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 Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

☐	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 levels. *(Check all that apply.)*

☒	Identifiability	Provide explanation: The information captured by the PE2E system could identify an individual.
☐	Quantity of PII	Provide explanation:
☐	Data Field Sensitivity	Provide explanation:
☒	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.
☐	Obligation to Protect Confidentiality	Provide explanation:
☒	Access to and Location of PII	Provide explanation: The information captured, stored, and transmitted by the PE2E system is maintained within USPTO systems. No PII is shared with external contractors.
☐	Other:	Provide explanation:

Section 12: Analysis

12.1 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.

12.2 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.