Version Number: 09-2017

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 PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.04.10 18:23:44 -04'00'

12/7/2017

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 Federal Information Processing Standard (FIPS) 199 security categorization for PE2E is Moderate.

- **PE2E Docket Application Viewer (DAV)**
  DAV is a web based tool for Patent examiners to examine, track and manage patent cases in their docket and view documents in image and text format. DAV does not collect, process or transmit sensitive PII.

- **Cooperative Patent Classification (CPC)**
  CPC is an International Patent Classification based bilateral classification system is jointly managed and maintained by the European Patent Office (EPO) and USPTO. The EPO's European Classification to CPC conversion 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 a USPTO contractors Reed Technology and Information Services (RTIS) Patent Data Capture (PDCap)/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). CPC does not collect, process or transmit sensitive PII.

- **One Portal Dossier (OPD)**
  OPD is a IP5 collaborative platform 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 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. OPD does not collect, process or transmit sensitive PII.

- **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 IP5 patent examiners/officers. P-GD-PAD receives non-sensitive PII (i.e., name, correspondence address, and telephone number) from CEDR-INFRA (formerly PALM-INFRA). P-GD-PAD does not collect, process or transmit sensitive PII.

- **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. P-OA2XML does not collect, process or transmit sensitive PII.

- **Patents - Electronic Library for Patents (P-ELP)**
  The P-ELP system maintains a content repository for USPTO's patent application images, 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 however; P-ELP does process and store non-sensitive PII (i.e., applicant/examiner name, phone number, correspondence address) that is of a public context. P-ELP does not collect, process or transmit sensitive PII.

- **Search For Patents (Search4P)**
  The Search for Patents (Search4P) system is a patent examiner search tool that replaces legacy (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). Search4P does not collect, process or transmit sensitive PII.

- **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 employee (examiner)/applicant (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. OC does not collect, process or transmit sensitive PII.

- **Patent Center (PC)**
  PC is a web-based patent application and document submission tool to enable external users to file and manage their patent application. Non-registered applicants are encouraged to only provide non-sensitive PII information (i.e. applicant name, email address, function) voluntarily as a necessity to facilitate USPTO/applicant correspondence and customer ID and digital certificate assignment. No other non-sensitive PII is collected or maintained.

- **Central Enterprise Data Repository Infrastructure (CEDR INFRA)**
  CEDR INFRA is transitioning as the replacement of the legacy PALM INFRA as 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), 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 accepts nightly updates via PTOnet of data on USPTO employees from the National Finance Center's (NFC) personnel/payroll system.

- **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. S-DWP does not collect, process or transmit sensitive PII.

- **Patents Automated Pre-Examination Search (P-APES)**
  Patents - Automated Pre-Examination Search (P-APES) provides examiners a fully automatic prior art searching solution that uses document content from existing unexamined patent applications as search query inputs and provides relevant search results against the corpus of US Patents and Pre-Grant Publications. P-APES does not collect, process or transmit sensitive PII.

(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 information from USPTO authorized contractor facilities RTIS PDCAP and SERCO PPS to support the USPTO patent application process (no PII is shared with RTIS and SERCO). OPD and CPC systems enable patent data search and ensures 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.

(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): CEDR has been included as a new AIS that collects and stores USPTO employees (federal) SSN, date of birth, and place of birth data.					

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: The SSN are cross-referenced to USPTO HR assigned employee ID. Federal employee SSN are 7-digits and contractors are the last two digits of the SSN. Federal employee SSN 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. The assigned Employee ID is utilized across USPTO as a unique reference to identify examiner actions, back office actions, etc.					
*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: National Finance Center has not provided any further guidance for SSN substitutions.					
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): Non-sensitive PII (correspondence information) is collected to facilitate processing and/or patent application examination submissions and issuance of U.S. patent to the inventor (patent applicant). Sensitive PII is maintained for USPTO HR and National Finance Center employee data synchronization.			

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 enable USPTO patent business mission and supports HR administrative functions. PE2E processes applications for the issuance and granting of U.S. patents. To support this public mission, federal employees and public (U.S. and foreign) non-sensitive PII is collected to facilitate public communications. 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. Although

limited in scope; PE2E supports HR administrative function by securely collecting/storing USPTO employee sensitive-PII. The sensitive-PII is necessary to uniquely identify employees for National Finance Center (NFC) and USPTO HR pay synchronization purposes only. Payroll data is not collected/stored within the PE2E system boundary. Also all employee sensitive-PII (SSN) are paired with an employee ID; this employee ID is used for internal use only.

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 (to be replaced by CEDR-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 sensitive-PII is shared with either system. • IP5

	o For external data transfer to IP5, data is transmitted across USPTO's Trilateral Network (TriNet) which is a Point-to-Point dedicated Virtual Private Network (VPN). No sensitive-PII is shared.
☐	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): 12/04/2017 ☐ 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. All sensitive-PII at-rest and in-transit are protected in accordance with NIST recommended encryption.

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 • Attendance, Leave, and Payroll Records of Employees and Certain Other Persons—COMMERCE/DEPT-1
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	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 (CEDR INFRA) 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 correspondence. The sensitive PII data maintained by CEDR

		INFRA is restricted for USPTO HR and the National Finance Center payroll administration only.
☐	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 accessed within USPTO on-campus systems. Sensitive PII (SSN) are located on USPTO on-campus systems.
☐	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.