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

Privacy Impact Assessment
for the
Patent Capture and Application Processing System – Initial Processing (PCAPS-IP)

Reviewed by: John B. Owens II, Senior Agency Official for Privacy

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

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

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Patent Capture and Application Processing System – Initial Processing (PCAPS-IP)

Unique Project Identifier: PTOP-006-00

<u>Introduction</u>: System Description

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

The Patent Capture and Application Processing System - Initial Processing (PCAPS-IP) provides multiple applications that allow the submission, categorization, metadata capture, and Patent examiner assignment of Patent applications from internal and external customers of the USPTO. It supports the Patent Business Function of USPTO. The PCAPS-IP is a major Application (MA) that provides the following services or functions in support of USPTO mission:

Application Routing Tool (ART)

ART is an automated patent application processing support system that provides a suggested routing location for new patent applications that have been successfully scanned into the PASS Database. ART uses the Bibliographic Retrieval Service (BRS) Query by Example (QBE) technology to provide a recommended group art unit (GAU) location, class and subclass for routing pending patent applications that have been successfully scanned into the PASS database. For each application, ART searches the text of the background, summary of the invention, and abstract for certain keywords and compares the frequency of those keywords to already published patents. A score is generated, by classification, for how many times the keywords are found within an application that were also found in published patents. The classification with the highest number of hits is used to determine a tentative classification for routing.

ART System Access Groups

Customer Group(s)	User Information	Approximate Number of Users
USPTO SPEs/Routers	USPTO employees	1000-1500
Office of Initial Patent Examination	USPTO employees	1-3
USPTO System Development/Maintenance Managers, Developers	ART Project Team/Contractors	30

Checker

The Checker system provides the United States Patent and Trademark Office (USPTO) with

a state-of-the-art C++/Microsoft Foundation Classes (MFC) based software program that employs a logical and intuitive user interface.
The Checker application enables public users to check sequence listings before submission to the USPTO. The Checker system validates patent applications in compliance with 37 Code of Federal Regulations (CFR) 1.821 – 1.825 for both 'old rules' (October 1990) and 'new rules' (July 1998. The Checker system was designed for use by the general public and is not used internally by the United States Patent and Trademark Office (USPTO). The Checker installer can be downloaded from the public USPTO Web server and installed on personal computers running the Windows operating system. Checker does not facilitate the delivery of sequence listings to the USPTO, and Checker does not connect to USPTO computers in any form. The Checker executable runs locally on the user's computer.

Checker System Access Groups

Customer Group(s)	User Information	Approximate Number of Users
Patent Applicants	Public	Approximately 8,000 applications per year

EAI Hub

The EAI Hub is a scalable, robust, and extensible system that enables the United States Patent and Trademark Office (USPTO) to model and automate business processes at the enterprise level. The EAI Hub supports the USPTO's e-Government strategy and provides a framework for various loosely coupled AISs to share information and services across their heterogeneous environments with minimal or no changes to the existing applications.
The EAI Hub system supports the key functions of asynchronous message routing, data transformation, data types-transformation, message filtering and restructuring to fit the needs of various applications, and data format conversions such as Extensible Markup Language (XML), Portable Document Format (PDF, and Tagged Image File Format (TIFF).

EAI Hub System Access Groups

Customer Group(s)	User Information	Approximate Number of Users
Patent Applicants	No	Unlimited

Electronic Filing System- Web (EFS-Web)

EFS-Web is a Web-Based application that provides a simple, safe and secure method for E-filers to file a patent application and submit documents as Portable Document Format (PDF) or text files to the USPTO over the internet.

EFS-Web System Access Groups

Customer Group(s)	User Information	Approximate Number of Users
Patent applicants	public	11000+
Office of Initial Patent Examination	N/A	30+

Patent Application Services and Security (PASS)

The PASS system provides the capability to use electronic images of patent applications to support USPTO operations. The PASS system was previously identified as Patent Application Capture and Review (PACR). PASS supports two user groups: the Office of Initial Patent Examination (OIPE) and the Licensing and Review (L&R) Group. PASS provided OCR, data extraction and verification, security screening, and application viewing, DTSA CD generation, PGPub, Grant tape publication, and East Data Center (EDC) exports.

PASS System Access Groups

Customer Group(s)	User Information	Approximate Number of Users
Patent applicants	public	11000+
Office of Initial Patent Examination	N/A	100+

PatentIn

PatentIn is a self-contained downloadable application that allows patent applicants to generate nucleic and amino acid sequence listings. PatentIn provides automated validation and error checking mechanisms. This enables users to use a sequence editor to enter or import existing sequences manually, while configuring each sequence according to a specific feature attribute. The application fully complies with World Intellectual Property Organization (WIPO) Standard ST.25 Sequence Listing Requirements. The PatentIn system was designed for use by the general public and is not used internally by the USPTO. PatentIn is downloaded from the public USPTO Web server and installed on personal computers running the MS Windows OS. The user generates output files containing sequence listings that can be submitted with a patent application. PatentIn is a stand-alone application and does not facilitate the delivery of sequence listings to the USPTO. In addition, PatentIn does not connect to USPTO. The PatentIn application runs locally on the user's personal computer.

PatentIn System Access Groups

Customer Group(s)	User Information	Approximate Number of Users
Patent Applicants	Public	Unlimited

Patent Application Location Monitoring Pre-Examination (PALM Pre-Exam)

The PALM Pre-Exam, as identified as PALM Pre-Ex, system supports the prosecution and related administrative functions of a patent application through its life cycle; and also tracks, monitors, and reports on the prosecution status of patent applications. PALM Pre-Exam supports the processing of over 350,000 applications each year. PALM serves the needs of over 5,000 Office of Patents staff, including over 3,700 members of the patent examining corps. The examining corps processes over twelve million transactions per month in addition to Web-based queries and batch processing.

PALM Pre-Exam System Access Groups

Customer Group(s)	User Information	Approximate Number of Users
OIPE	USPTO Employees	150
Patent Examiners	USPTO Employees	100
PGPub Users	USPTO Employees	40
RTIS Contractors	Contractors	50
Pre-Exam Users	USPTO Employees	15

Patent Application Location Monitoring Patent Cooperation Treaty Operations System (PCT Ops)

The PCT Ops also referred as PCT Operations Workflow and Electronic Review System (POWER), system is a USPTO Automated Information System (component) designed to support an automated, workflow-driven, client-server environment that support Patent Cooperation Treaty (PCT) patent application functions. PCT Ops works with an electronic application in an integrated desktop environment. The PCT Ops system minimizes the movement of paper through the United States Receiving Office (RO/US) processing stream and automates the application filing process under Chapter I and Chapter II of the PCT. The PCT Ops system supports the initial receipt of an application or later-submitted papers, review of the application by PCT personnel, generation of outgoing correspondence, and tracking of the application while it is being processed by RO/US. Case files ultimately provide information in an electronic medium that facilitates exchange with PCT Operations' principal internal customer, the USPTO Examining Corps, as well as with the WIO, Trilateral Office partners, and the other international partners of USPTO.

PCT-Ops System Access Groups

Customer Group(s)	**User Information**	**Approximate Number of Users**
Patent Office(PCT Legal, PASS, Supervisors)	USPTO Employees	150
PCTBDE (User directly enters data-authenticated via LDAP	USPTO Employees	20
Administrators	PCT Ops Admin	-

Patent Application Location Monitoring - Reporting System (PRS)
The PRS produces many productivity and statistical reports that are crucial to the Patents Corps business operation. The PRS processes and delivers reports to Patents Corp, supporting various PALM subsystems and business areas, including: PALM-EXPO, Pre-Exam, File Ordering System (FOS), Infrastructure, and PCT Ops. These reports are available via the USPTO Intranet on-line and on-demand to over 5,000 Examiners, Directors, Supervisory Patent Examiners (SPEs), and Clerical staff. The reports are delivered via different means. Static reports are made available electronically on the Web. Dynamic reports are accessible via the USPTO intranet (online) and allow real-time database access for most up-to-date information via the Web; and report distribution via email. PRS provides PALM users (over 7000 examiners, 500 managers, and over 100 other users) with access to PALM data via COTS reporting platform. Most of the reports obtain data from a daily snapshot of the PALM on-line system. The reports can be scheduled to run at a predefined time or display data instantaneously. The scheduled reports are archived. Access to archive and inputs for instantaneous reports are provided via a USPTO Intranet website.

PRS System Access Groups

Customer Group(s)	**User Information**	**Approximate Number of Users**
Patent Examiners	USPTO Employees	7000
Special Patent Examiners	USPTO Employees	500
Directors and Analysts	USPTO Employees	70-100

Infrastructure Code Table – (ICT)
The ICT system provides the validation of a given geographic region with a specified country, and provides a list of current countries and geographic regions. ICT provides the standard PTO country codes for patent applications. For ICT services, the users are AISs instead of real users. No traditional user interfaces are required in this release.

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

To provide user access to search the USPTO Patent data repositories, which allows Patent Examiners and public users to search and retrieve application data and images and Patent Examiners and applicants to identify individuals and organizations with intellectual property, pre-grant, and published applications.

(c) any information sharing conducted by the system

Data repositories allow information to be shared with internal stakeholders (e.g. patent examiners), and to the public.

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

- USC statutory code 35 U.S.C. Section 122
- The Federal Information Management Security Act of 2002 (FISMA)
- OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, May 2006
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 2006
- U.S. Department of Commerce, IT Privacy Policy
- U.S. Department of Commerce, Electronic Transmission of PII Policy
- U.S. Department of Commerce, Use of Personal E-mail for Official Communication Prohibited, May 28, 2013

(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.)*

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):					

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): Nationality					

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):					

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):			

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).

The PII/BII collected is of the public (U.S. and foreign), Federal employees. Public data is used to file and manage Patent applications. Federal employee data is used for 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: System Name – Organization: EWS – USPTO; DBS – USPTO; EMSO – USPTO; EUS – USPTO; NSI – USPTO; PSS-PS – USPTO; PCAPS-ES – USPTO; RAM – USPTO; RTIS-PDCAP – RTIS; Serco International-PGPCS – Serco; WIPONET – WIPO By restricting access to the system via Active Directory (ESS), EFS-Web' protection of PII data is performed by the implemented AD automated system. Automatic quality control for data checks exist. VPN is used for developer access. There is a network connection to the Internet via the Network Perimeter for EFS-Web users. The EFS-Web services are logically partitioned via a DMZ and an internal USPTO firewall is used as the boundary protection device that secures the communication between Internet users and the EFS-Web. This connection is protected and controlled by the USPTO infrastructure. EFS-Web is a public facing interface that utilizes HTTPS protocol, SSL, and TLS. The web-session is established through PKI X.509 digital certificate authentication. Only authorized users (patent applicants) can access EFS-Web data through the secure web-interface. No sensitive PII information is contained within error messages. For external data transfer to WIPO, PSFTP (SFTP PuTTY) is utilized to transmit data across TriNet. Internally within USPTO, data transmission confidentiality controls are provided by PTOnet. External contractors from RTIS and Serco International-PGPCS connect through Tumbleweed secure data transfer.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

Nested table within the "Yes" cell:

System Name	Organization
EWS	USPTO
DBS	USPTO
EMSO	USPTO
EUS	USPTO
NSI	USPTO
PSS-PS	USPTO
PCAPS-ES	USPTO
RAM	USPTO
RTIS-PDCAP	RTIS
Serco International-PGPCS	Serco
WIPONET	WIPO

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):			

<u>Section 7</u>: 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: By not applying or using the IT system
☐	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.
☐	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: By logging into their patent application and changing the data. The USPTO utilizes HR Connect to provide a means for employees to correct or amend inaccurate PII maintained by the organization.
☐	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): ___3/24/2016_________ ☐ 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.

Management Controls:
1. The USPTO uses the Life Cycle review process to ensure that management controls are in place for the PCAPS-IP. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the Security Plan. The Security Plans specifically address the management, operational and technical controls that are in place, and planned, during the operation of the enhanced system. Additional management controls include performing national agency check on all personnel, including contractor staff.

2. The USPTO Personally Identifiable Data Extracts Policy

Operational Controls:
1. Automated operational controls include securing all hardware associated with the PCAPS-IP in the USPTO Data Center. The Data Center is controlled by access card entry, and is manned by a uniformed guard service to restrict access to the servers, their Operating Systems and databases. Contingency planning has been prepared for the data. Backups are performed on the processing databases. Backups are stored on tape and are secured off-site. Additional operation controls include: (1) Logical edit checks to ensure proper sequence of actions; (2) Physical terminal identification; (3) Database User ID; (4) Restricted data display, as required; and (5) Restricted access.
2. Manual procedures shall be followed for handling extracted data containing sensitive PII which is physically transported outside of the USPTO premises. In order to remove data extracts containing sensitive PII from USPTO premises, users must:
a. Maintain a centralized office log for extracted datasets that contain sensitive PII. This log must include the date the data was extracted and removed from the facilities, a description of the data extracted, the purpose of the extract, the expected date of disposal or return, and the actual date of return or deletion.
b. Ensure that any extract which is no longer needed is returned to USPTO premises or securely erased, and that this activity is recorded on the log.
c. Obtain management concurrence in the log, if an extract aged over 90 days is still required.
d. Store all PII data extracts maintained on an USPTO laptop in the encrypted My Documents directory. This includes any sensitive PII data extracts downloaded via the USPTO Virtual Private network (VPN).
e. Encrypt and password-protect all sensitive PII data extracts maintained on a portable storage device (such as CD, memory key, flash drive, etc.). Exceptions due to technical limitations must have the approval of the Office Director and alternative protective measures must be in place prior to removal from USPTO premises.

Encrypt and password-protect prior to transmission any sensitive PII data extracts that are sent to an external e-mail address via the Internet.

7. How will the data extract log and verify requirement be met?
USPTO has not developed a centralized logging system for PII data extracts. Such a system would track the following categories of information:

a. Who performed the extract,
b. When extract was done,
c. What was the extract,
d. Where was the extract taken from,
e. Has the extract been deleted and,
f. If not deleted after 90 days, to monitor that it is still needed in 90 day intervals.

Until a system is implemented, USPTO is using the following compensating controls to protect PII data:
a. No extracts of sensitive data may be copied on to portable media without a waiver approved by the DOC CIO. The request for a waiver must include specifics as to how the data and device are protected, how long the data will be maintained, and how the data on the device will be deleted when no longer required.
b. All laptop computers allowed to store sensitive data must have full disk encryption.
c. All remote access to public USPTO systems containing sensitive data must be encrypted. All remote access to internal USPTO systems containing sensitive data must fully comply with DoC Remote Access Policy requirements.
d. All flexi place/telework agreements for working off site require that adequate data protection be in place.

<u>Section 9</u>: 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)*: The USPTO Publishes their SORNS in the Federal Register and can be accessed in the following location: http://www.uspto.gov/uspto-systems-records-notices. These SORNs are subject to required oversight processes for systems containing PII. The USPTO SORNs are kept current (updated at least annually) and contains statements from the Privacy Act of 1974.
☐	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:
☐	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: Whether the data given could identify an individual.
☒	Quantity of PII	Provide explanation: Whether the data given is enough to identify an individual.
☐	Data Field Sensitivity	Provide explanation:
☒	Context of Use	Provide explanation: Why the data is being used, stored, and transmitted.
☐	Obligation to Protect Confidentiality	Provide explanation:
☒	Access to and Location of PII	Provide explanation: How the data is being used, stored, and transmitted.
☐	Other:	Provide explanation:

<u>Section 12</u>: 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.