Version Number: 02-2017

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

Privacy Impact Assessment
for the
Patent Capture and Application Processing System – Examination Support (PCAPS-ES)

Reviewed by: David Chiles, 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: 2018.09.30 19:14:49 -04'00'

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 – Examination Support (PCAPS-ES)

Unique Project Identifier: PTOP-005-00

Introduction: System Description

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

The PCAPS-ES is an Application information system, composed of 19 Components and provides the capabilities and functionality detailed below:

Electronic Business Center Imaging System (EBCIS): The Electronic Business Center Imaging System enables users to store and maintain Customer Number documents or to record numerous other correspondences. The purpose of EBCIS is to develop an automated document management system to provide the capabilities of scanning, indexing, retrieving, and searching for documents. EBCIS is accessible to users via the Patent and Trademark Office (PTO) Intranet. EBCIS does not collect, process or transmit sensitive PII.

Electronic Desktop Application Navigator (eDAN): The eDAN accesses documents from the Patent Application Location and Monitoring System (PALM), the Image File Wrapper (IFW) image repository, the Revenue and Accounting Management (RAM), using Web services, Hyper Text Transmission Protocol (HTTP) requests, and Extensible Markup Language (XML) over HTTP. The eDAN server provides services for other AISs, such as the Order Entry Management System (OEMS) and One Portal Dossier. eDAN does not collect, process or transmit sensitive PII.

File Inspection Utility (FIU): FIU provides some of the Public PAIR functionality plus secure access to pending patent application data. USPTO examiners will be able to access FIU data within the PTONet using USPTO credentials without compromising the confidentiality or security of their applications. FIU does not collect, process or transmit sensitive PII.

Image File Wrapper (IFW): IFW is a document and application management system to support the process of handling Intellectual Property-related documents. IFW interfaces with several USPTO legacy systems. IFW does not collect, process or transmit sensitive PII.

Office Action Correspondence System (OACS): The purpose of OACS is to aid the United States Patent and Trademark Office (USPTO) in creating patent correspondence with the patent applicants. OACS does not collect, process or transmit sensitive PII.

Patent Resource Management System (PRMS): PRMS is integral system to the Commissioner of Patents' forecast of patent production, staff resource planning, pendency and operating costs. The Office of Patent Financial Management builds and stores budget formulations within a central repository and execute the congressionally approved budget as a Decision Support System. PRMS does not collect, process or transmit sensitive PII.

PAIR User Resource Manager (PURM): PURM is a system used to associate customer numbers with their PKI certificates. It provides functionality to search customer association by common name, user id, earliest update date and distinguished name. It also provides retrieving user id, common name, group name, insert and update dates for a given customer number. PURM does not collect, process or transmit sensitive PII.

Patent Application Location Monitoring – Examination and Post-Examination (PALM ExPO): The PALM ExPO subsystem deals with tracking patent application prosecution, publication, the physical location of application, GAU, examiner productivity, patent issuance, quality review, file inventory, and lost file reconstruction. It also supports the production of reports related to examination and publication processes. PALM EXPO interfaces with Revenue Accounting and Management (RAM), Patent Application Security System (PASS), and Image File Wrapper (IFW) in addition to other PALM subsystems. PALM EXPO also provides external services for PASS, IFW, and Electronic Desktop Application Navigator (eDAN) to enable these components to access PALM data. PALM ExPO does not collect, process or transmit sensitive PII.

Patent Application Location Monitoring – Services Gateway (PALM SG): The PALM SG subsystem deals with implementing a robust solution for existing PALM Services based on the USPTO Service Oriented Architecture (SOA) reference architecture and the cots products. It also provides an implementation framework for enterprise components such as logging, security and service versioning for any enterprise wide service implementation. Following are the existing PALM Services which are implemented: Bibliographic Data Services, Utilities Services, Worker Services, Docket Services, PALM Office Action Services. PALM SG does not collect, process or transmit sensitive PII.

Patent Application Location Monitoring – File Ordering System (PALM FOS): The File Ordering System (FOS) tracks the physical location and status of issued or abandoned patents, as well as registered or abandoned Trademark files. As a PALM FOS interface, Warehouse File Tracking System (WFTS) is a tracking program used by the USPTO to track the location of each patent and trademark file as it is transported and reviewed by Patent or Trademark Examiners. PALM FOS does not collect, process or transmit sensitive PII.

Patent Application Location Monitoring - Infrastructure (PALM INFRA): The Patent Application and Location Monitoring Infrastructure (PALM) subsystem supports the management of basic information and contact details about the USPTO (its organizational structure, workers, and physical locations – including special purpose locations such as search rooms and how they interact with each other).

PALM INFRA's functionalities are currently being ***subsumed*** within the next-generation replacement, CEDR-INFRA. However; CEDR INFRA's data (including PII) is still synced to

PALM INFRA as the original source. CEDR INFRA accepts nightly updates via PTOnet of data on USPTO employees from the National Finance Center's (NFC) personnel/payroll system.

PALM INFRA stores 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. SSNs (full 9-digits for government and last 2 digits for contractors) are captured for assigning a unique employee ID number. The employee ID number is subsequently used to help identify PTO employees within USPTO. Federal employee SSNs are only acceptable for verifying government pay with the NFC.

Patent Application Information Retrieval - Private (Private PAIR): Private PAIR allows restricted Internet access to patent application status to patent applicants and/or their designated legal representative(s) without compromising the confidentiality or security of applicants' data. PRIVATE PAIR requires all users to be registered and to be issued an x.509 digital certificate by USPTO. Private PAIR does not collect, process or transmit sensitive PII.

Patent Enterprise Access Integration Public Patent Application Information Retrieval - Public (Public PAIR): Public PAIR allows public access to published patent applications and additional information regarding published patents. PUBLIC PAIR provides a web based interface for the public at large to access published patent applicants. This data has been publicly released and is accessible to everyone in read-only format. Public PAIR does not collect, process or transmit sensitive PII.

Trilateral Document Access (TDA): The TDA application allows the United States Patent and Trademark Office (USPTO) to access the European Patent Office (EPO), Korean Patent Office (KIPO), Japanese Patent Office (JPO,) and World Intellectual Property (WIPO) document content information about patents via TriNet. TDA provides access to published documents through the File Wrapper Access (FWA) service and unpublished documents through the Document Exchange (PDX) service that are available at the participating foreign offices. TDA does not collect, process or transmit sensitive PII.

Patent File Wrapper (PFW): PFW provides patent prosecution services or functions in support of the USPTO mission. PFW streamlines the patent application examination process by consolidating the text provided through electronic filing and Early Data Capture (EDC) of patent applications into a centralized data repository where the information can be leveraged to implement and automated content management, workflow, and patent application management rule engine. PFW does not collect, process or transmit sensitive PII.

Quality Review System (QRS): QRS provides a web-based interface to the reviewers to view the patent applications in order to review, evaluate and create reports for the examiners work. QRS (formerly called as Patent Quality Review System (PQRS)) provides interfaces for the Technology Centers (TCs) and Office of Patent Quality Assurance (OPQA) personnel to enter data on Allowed Reviews, In Process Reviews (IPRs), New Application Reviews, Amendment Reviews, and New Examiner Reviews. QRS provides the following functionality to authorized users. QRS does not collect, process or transmit sensitive PII.

Supplemental Complex Repository for Examiners (SCORE): The SCORE component is a non-image repository as defined in the FY04 Patent Automation Program Charter. SCORE is a component that provides the Patent examiners with access to unpublished mega content associated with a patent application. SCORE does not collect, process or transmit sensitive PII.

Technology Assessment and Forecast (TAF): TAF is a database that supports the USPTO's need for many of the general annual patent statistics reports required to meet agency/office obligations. Reports such as: the Commissioner's Annual Report, the Annual submission of patent statistics to the World Intellectual Property Organization, the Annual patent statistics submission to Statistical Abstracts, the Census Bureau's annual government statistics fact book, and specialized patent statistics reports prepared for the National Science Foundation. Selected bibliographic data pertaining to patents and pre-grant patent publications are loaded weekly; other data are loaded on a monthly, bi-monthly, or annual basis. Data verification and correction are performed on selected data elements. Statistical reporting is performed by means of standardized reporting programs and by custom data extraction and aggregation efforts. Support is also provided for optical disc products produced by Office of Electronic Information Products (OEIP). TAF does not collect, process or transmit sensitive PII.

Patents Telework Enterprise System (PTES): The Patent Telework Enterprise System (PTES) is an online application for applying to the various telework programs in Patents. Telework at the USPTO supports mission achievement and goal fulfillment via a distributed workforce. Employees in Patents use PTES to apply for telework programs. Management uses PTES to manage telework, review and approve telework eligibility, and provide telework data for annual reports.

PTES is for internal use only and is not available outside of the USPTO firewall. The application process requires an employee to submit their Alternate Work Site (AWS), telephone number, and an Internet Service Provider (ISP) statement as proof that they meet the USPTO VPN connection requirements. The AWS is defined as the employee's home address and a location in the employee's home designated by the employee as the location that the employee will use to perform their official USPTO duties.

PTES collects the following PII data – employee's home address, phone number, and ISP statement. PTES has a role-based access control, and an employee can only view/update their own records. Managers and designated managers that are assigned the duties of telework coordinators can view the information submitted by employees as part of the telework application review and approval process. PTES does collect sensitive PII for example home address, phone number, and ISP statement.

Integrated Quality System (IQS): The Integrated Quality System (IQS) is designed for use by the Office of Patent Quality Assurance and the Patents Technology Centers to conduct quality reviews of patent examiners' office actions. Personalized dockets allow users to monitor work pending and work completed. Reviews are conducted using the Master Review Form developed by Patents in response to an Inspector General mandate. Depending on the business unit conducting the review and the result of the review, reviews may be routed for supervisory approval and/or sent to the examining organization for rebuttal and appeal. All results are stored in a single database, allowing an OPQA statistician to find quality trends. IQS does not collect, process or transmit sensitive PII.

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

Providing user access to search the USPTO Patent data repositories, which allows Patent Examiners and public users to search and retrieve application data and images, Patents 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

35 U.S.C. 1 and 115; 5 U.S.C. 301.

(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.

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: The SSN are cross-referenced to USPTO HR assigned employee ID. Federal employee SSN are 9-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. These fields are restricted only a select admin group. The assigned Employee ID is utilized within USPTO as a unique reference to identify USPTO employees, examiner actions, back office actions, etc. Sensitive PII is obfuscated (masked) when viewed directly by unauthorized viewers, such as administrators.					
*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 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 Patent Search System Primary Search (PSS-PS); Patent Capture and Application Processing System – Initial Processing (PCAPS-IP); and Revenue and Account Management (RAM), Information Dissemination Support System (IDSS), Intellectual Property Leadership Management Support System (IPLMSS), Patent End to End (PE2E): 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) o External contractors from RTIS 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 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):			

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: 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.
☐	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

<u>Section 8</u>: 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): ___7/25/2017___ ☐ 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.

PCAPS-ES collects voluntary applicant(s) correspondence information to facilitate direct communications between the applicant(s) and the Office. PCAPS-ES applications are managed and secured by the USPTO's Active Directory (AD) and Unix Enterprise infrastructure and other OCIO established technical controls, which include password authentication at the server and database levels. HTTPS is used for all data transmissions to and from the Internet, USPTO DMZ, and PTOnet. A dedicated socket is used to perform encryption and decryption.

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 Employees Personnel Files Not Covered By Notices of Other Agencies--Commerce/Dept-18 USPTO PKI Registration and Maintenance System--Commerce/PAT–TM–16
☐	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: Whether the data given could identify an individual. Name, mailing address, phone number, email address
☐	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: The data captured, stored, or transmitted by the PCAPS-ES 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 PCAPS-ES system is maintained within USPTO systems. The sensitive data are the employee and contractor SSNs that are stored in PALM INFRA. Sensitive PII is obfuscated (masked) when viewed directly by unauthorized viewers, such as administrators. 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.