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: Henry J. Holcombe, Bureau Chief Privacy Officer

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

Jennifer Goode
_____   05/13/2021
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-006-00

<u>**Introduction:**</u> **System Description**

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

The PCAPS-ES system purpose is to process, transmit and store data and images to support the data-capture and conversion requirements of the USPTO to support the USPTO patent application process.

(a) Whether it is a general support system, major application, or other type of system
Major application

(b) System location
600 Dulany Street, Alexandria, VA 22314

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

- **EWS (Enterprise Windows Services)**: EWS is an Infrastructure information system that provides a hosting platform for major applications supporting various USPTO missions.
- **EUS (Enterprise UNIX Services)**: The EUS System consists of assorted UNIX operating system (OS) variants each comprised of many utilities, along with the master control program, the kernel.
- **NSI (Network and Security Infrastructure System)**: The NSI is an Infrastructure information system, which provides an aggregate of subsystems that facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO IT applications.
- **PSS-PS (Patent Search System – Primary Search and Retrieval)**: PSS-PS is a Master system portfolio consisting of multiple Automated Information Systems (AIS). PSS-PS supports legal determination of prior art for patent applications, including text and image search of repositories of US application and grant publications, foreign application and grant publications, various concordances, and non-patent literature. It represents the databases that contain the images and text data for US Patent Grants, Published applications, and unpublished applications.
- **PCAPS-IP (Patent Capture and Application Processing System – Initial Processing)**: The PCAPS-IP is an Application Information System that provides support to the USPTO for the purposes of capturing patent applications and related metadata in electronic form;

processing applications electronically; reporting patent application processing and prosecution status; and retrieving and displaying patent applications. PCAPS-IP is comprised of multiple Automated Information Systems (components) that perform specific functions, including submissions, categorization, metadata capture, and patent examiner assignment of patent applications.

- **RAM (Revenue Accounting and Management System)**: RAM is a Master System that collects fees for all USPTO goods and services related to intellectual property. While the Fee Processing Next Generation (FPNG) system provides secure web applications from which internet customers can pay these fees, FPNG forwards those payments to RAM to be processed and recorded. Fees submitted to the USPTO by mail are processed through the RAM Desktop application by designated USPTO staff. Collected payment information is shared with the U.S. Treasury's Pay.gov system for credit card and ACH verification and processing.
- **EDP (Enterprise Desktop Platform)**: The EDP is an infrastructure information system that provides a standard enterprise-wide environment that manages desktops and laptops running on the Windows operating system (OS), providing United States Government Configuration Baseline (USGCB) compliant workstations.
- **SOI (Service Oriented Infrastructure)**: SOI provides a feature-rich and stable platform upon which USPTO applications are deployed.
- **ESS (Enterprise Software System)**: ESS supports services such as Enterprise Directory Services, Role-Based Access Control System, Email as a Service, PTO Exchange Services, Symantec Endpoint Protection, Enterprise SharePoint Services, etc.
- **EMSO (Enterprise Monitoring and Security Operations)**: EMSO provides Security Incident and Event Management, Enterprise Forensic, Enterprise Management System, Security and Defense, Enterprise Scanner, Enterprise Cybersecurity Monitoring Operations, Performance Monitoring Tools, Dynamic Operational Support Plan, and Situational Awareness and Incident Response. EMSO does not collect, maintain, and disseminate PII/BII.
- **DBS (Database Services)**: DBS is an Infrastructure information system, which provides a Database Infrastructure to support mission of USPTO database needs.
- **TRINET (Trilateral Network)**: TRINET is an Infrastructure information system, which provides secure network connectivity for electronic exchange and dissemination of sensitive patent data between authenticated endpoints at the Trilateral Offices and TRINET members. The Trilateral Offices consist of the USPTO, the European Patent Office (EPO), and the Japanese Patent Office (JPO). The TRINET members consist of the World Intellectual Property Office (WIPO), the Canadian Intellectual Property Office (CIPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO) and the Intellectual Property Office of Australia (IPAU).
- **IPLMSS (Intellectual Property Leadership Management Support System)**: The IPLMSS is an Application information system, which provides Adjudicated Case Tracking System, Electronic Freedom of Information Act System, Electronic System for Trademark Trials and Appeals, FOIA Electronic Management System, General Counsel Case Tracking System, General Counsel Library System, Office of Enrollment and Discipline Item Bank, Office of Enrollment and Discipline Information System,

Trademark Trial and Appeal Board, Trademark Trial and Appeal Board Information System, E-Discovery Software Suite, & NOSPS.

- **IDSS (Information Dissemination Support System)**: The IDSS system supports the Trademark and Electronic Government Business Division, the Corporate Systems Division (CSD), the Patent Search System Division, the Office of Electronic Information Products, and the Office of Public Information Services. It provides automated support for the timely search and retrieval of electronic text and images concerning patent applications and patents by USPTO internal and external users.
- **PE2E (Patent End to End)**: Patents End-to-End (PE2E) is a Master system portfolio consisting of next generation Patents Automated Information Systems (AIS). PE2E makes the interaction of USPTO's users as simple and efficient as possible in order to accomplish user goals. PE2E is a single web-based examination tool providing users with a unified and robust set of tools..
- **RTIS-PDCAP**: RTIS is an off-campus contractor system that captures critical fields from applicant's applications, which are pre-loaded into an index file to reduce examiners and public search times.
- **National Finance Center (NFC):** NFC is a U.S. Department of Agriculture (USDA) personnel and payroll system.

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

PCAPS-ES uses twenty applications to 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.

(e) How information in the system is retrieved by the user

Public internet websites, Internal web applications on PTONet.

(f) How information is transmitted to and from the system

For internal USPTO communication, transmission integrity is provided by internal access controls, firewalls, and VPN. Device management connections are protected by Secure Shell (SSH) based encrypted connections. PCAPS-ES data transmission is protected by the PTONet infrastructure.

For external connections to the DMZ, Contractor Access Zone (CAZ), and/or external networks, device management connections use SSH, PKI, and Secure ID VPN-based connections. User data connections use PKI and Secure ID VPN and SSL/TLS. Additional session-level communication protection mechanisms are not utilized within PCAPS-ES. Limited session confidentiality is provided by the PTONet Local Area Network (LAN). Only authorized USPTO systems may access the internal PTONet.

Public users transmit information to and from Public PAIR and Private PAIR via HTTPS.

(g) Any information sharing conducted by the system

Data repositories allow information to be shared with internal stakeholders and external stakeholders (e.g. patent examiners, state agencies and foreign governments etc.) and to the public.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

Executive Order 9397, 35 U.S.C. 1 and 115; 5 U.S.C. 301.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system.

Moderate

Section 1: Status of the Information System

1.1   Indicate whether the information system is a new or existing system.

☐   This is a new information system.

☐   This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

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):					

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

☒   This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017).

☐   This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later).

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*	☒	f. Driver's License	☐	j. Financial Account	☐
b. Taxpayer ID	☐	g. Passport	☐	k. Financial Transaction	☐
c. Employer ID	☒	h. Alien Registration	☒	l. Vehicle Identifier	☐
d. Employee ID	☒	i. Credit Card	☐	m. Medical Record	☐

e. File/Case ID	☒				
n. Other identifying numbers (specify):					

*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: PCAPS-ES uses SSNs, which are cross-referenced to USPTO HR assigned employee ID. Federal employee SSNs 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 to select admin groups. 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.

General Personal Data (GPD)

a. Name	☒	h. Date of Birth	☒	o. Financial Information	☐
b. Maiden Name	☐	i. Place of Birth	☒	p. Medical Information	☐
c. Alias	☐	j. Home Address	☒	q. Military Service	☐
d. Gender	☐	k. Telephone Number	☒	r. Criminal Record	☐
e. Age	☐	l. Email Address	☒	s. Physical Characteristics	☐
f. Race/Ethnicity	☐	m. Education	☐	t. Mother's Maiden Name	☐
g. Citizenship	☐	n. Religion	☐		
u. Other general personal data (specify):					

Work-Related Data (WRD)

a. Occupation	☒	e. Work Email Address	☒	i. Business Associates	☐
b. Job Title	☒	f. Salary	☐	j. Proprietary or Business Information	☐
c. Work Address	☒	g. Work History	☐	k. Procurement/contracting records	☐
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	☐		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)

a. Fingerprints	☐	f. Scars, Marks, Tattoos	☐	k. Signatures	☐
b. Palm Prints	☐	g. Hair Color	☐	l. Vascular Scans	☐
c. Voice/Audio Recording	☐	h. Eye Color	☐	m. DNA Sample or Profile	☐
d. Video Recording	☐	i. Height	☐	n. Retina/Iris Scans	☐
e. Photographs	☐	j. Weight	☐	o. Dental Profile	☐
p. 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	☒	f. 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   Describe how the accuracy of the information in the system is ensured.

PCAPS-ES employs system checks to ensure accuracy, completeness, validity, and authenticity. Each PCAPS-ES component has established specific rules or conditions for checking the syntax of information input to the system such as numbers or text; numerical ranges and acceptable values are utilized to verify that inputs match specified definitions for format and content. PCAPS-ES components have rules in place to validate the content of input information based on field requirements (i.e., date fields are validated for date format and legitimacy). Some PCAPS-ES applications have rules in place to validate the content of input information based on field requirements (i.e., date fields are validated for date format and legitimacy).

2.4   Is the information covered by the Paperwork Reduction Act?

☒	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. The data processed by this system is collected under the following OMB control numbers: 0651-0031 Patent Processing 0651-0032 Initial Patent Processing 0651-0033 Post Allowance and Refilling 0651-0035 Representative and Address Provisions 0651-0071 Matters Related to First Inventor to File
☐	No, the information is not covered by the Paperwork Reduction Act.

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

Technologies Used Containing PII/BII Not Previously Deployed (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			
For a Computer Matching Program	☐	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, and DOC contractors. Public data is used to file and manage Patent applications. Federal employee data is used for Patent examiner work, management of Federal employees and contractors, and the management of the IT systems that support the USPTO.

5.2   Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

> Nation states (foreign governments) and insider threats are the predominant threat to the system's privacy and data leakage. USPTO has implemented NIST security controls (encryption, access control, auditing) and selected a FedRAMP authorized cloud provider to reduce the risk. Mandatory IT Awareness and role-based training are required for staff who have access to the system and address how to handle, retain, and dispose of data. Contract terms between the cloud provider and USPTO provide guidance on how data should be handled, retained, and disposed.

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   Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

☐	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☒	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☐	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3   Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

☒	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): • 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): • External contractors from RTIS connect through secure data transfer. No PII is shared with either system. World Intellectual Property Organization (WIPO) / Foreign Patent Offices: • 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.

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

Class of Users			
General Public	☒	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 for a patent 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 parent application and changing the data.
☐	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 the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): _____6/26/2020_____ ☐ 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 (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish DOC 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. *(Include data encryption in transit and/or at rest, if applicable).*

> 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 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   Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

☒   Yes, the PII/BII is searchable by a personal identifier.

☐   No, the PII/BII is not searchable by a personal identifier.

9.2   Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*:
	
	   • Employee Production Records- Commerce/PAT-TM-3
	   • Patent Application Files-- COMMERCE/PAT-TM-7
	   • USPTO PKI Registration and Maintenance System-- Commerce/PAT–TM–16
	   • USPTO Security Access and Control and Certificate Systems – Commerce/ PAT-TM-17
	   • USPTO Personal Identification Verification (PIV) and Security Access Control Systems – Commerce/PAT-TM -18
	   • Employees Personnel Files Not Covered By Notices of Other Agencies-- Commerce/Dept-18
	   • Access Control and Identity Management System-- Commerce/DEPT-25

☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

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

☒	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 Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

☐	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 level. *(Check all that apply.)*

☒	Identifiability	Provide explanation: The combination of Social Security, Employer ID, Alien Registration, File Case ID, Name, Date of Birth, Place of Birth, Home address, Email address, Occupation, Job Title, Work address, Work email, Work phone number, User ID, IP Address can be easily used to identify an individual.
☒	Quantity of PII	Provide explanation: The number of data items collected for Employees: SSN, Alien Registration, Name, Date of Birth, Place of Birth, Home Address, Telephone Number and Email Address is large enough to be concerned if disclosed.
☒	Data Field Sensitivity	Provide explanation: The data includes personal and work related elements that include identifying numbers. PII stored in the system is data collected from USTPO HR in which the information is confidential and unique to those individuals. Any unauthorized access, modification, and/or disclosure of sensitive data would have a High impact on the organization and its operations
☒	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: USPTO employees including Contractors undergo annual cyber security awareness training related to handling of PII/BII within USPTO and are obligated by the organizational rules related to handling of PII/BII. In accordance with NIST 800-53 Rev. 4, PCAPS-ES implements both AR-2 (Privacy Impact and Risk Assessment) and AR-7 (Privacy-Enhanced System Design and Development) security controls to ensure all stakeholder's confidentiality is protected. This system is governed by The Privacy Act of 1974, which prohibits the disclosure of information from a system of records absent of the written consent of the subject individual.

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

Nation states (foreign government), insider threats and adversarial entities are the predominant threats to the information collected and its privacy. Security controls following FedRAMP and NIST guidance were implemented to deter and prevent threats to privacy.

12.2   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.

12.3   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.