Template Version Number: 01-2020

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

Privacy Impact Assessment
for the
Siemens Physical Access Control System (PACS)

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 Digitally signed by JENNIFER GOODE
Date: 2021.09.09 14:20:16 -04'00' 09/08/2021

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Siemens Physical Access Control System

Unique Project Identifier: PTOC-039-00

<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 Siemens Physical Access Control System (PACS) is an electronic physical security system, and provides the capability to restrict and/or control physical access to USPTO facilities, equipment and resources. This system is used by authorized security personnel to manage and monitor multiple entry points, intrusion detection, and video surveillance at the USPTO Headquarters in Alexandria, Virginia and satellite offices in: San Jose, California; Denver, Colorado; Dallas Texas; and Detroit, Michigan.

The following 4 components comprise PACS:

1. CCURE9000
2. Genetec Security Center
3. Briefcam Enterprise Video Analytics
4. Commend Intercom System

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

(b) System location
The system is located at the Alexandria campus and Dallas, San Jose, Denver and Detroit satellite offices

(c) ***Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)***
PACS is a system on a private security network and connects to the USPTO Network and Security Infrastructure (NSI). PACS receives files from the HSPD-12 Personal Identity Verification System Card Management System (HSPD-12) PIVS/CMS badging system during the PIV badging process but does not have the capability to send any data to the HSPD-12 system. It also forwards non PII badging data regarding employees on a daily basis to a middleware server for eventual use in the Corporate Administrative Office System (CAOS), the Agency's Records Sharing Platform (RSP).

- **Network and Security Infrastructure System (NSI) -** NSI is an infrastructure information system that facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO IT applications.
- **Corporate Administrative Office System (CAOS) -** an Application information system and Records Sharing Platform (RSP) which supports all activities associated with the recruitment and management of USPTO personnel.

- **Personal Identity Verification System/Card Management System (HSPD-12-PIVS/CMS)** provides the personalization and issuance of the smart card identification credentials under HSPD-12 and is used to gather biometrics (fingerprints) and other identity data (name, contact information, birth history and photo of applicant) for the issuance and life cycle management of secure credentials.

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

PACS implements a private, closed network with servers located physically onsite accessed by desktop workstations. Authorized security personnel manage and monitor multiple entry points, intrusion detection, and video surveillance.

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

The user retrieves information by logging into the system and looking up data, having the monitoring portion of the system up and running which provides displays ongoing badging information or by running reports to pull data. Users can also display the video monitoring system or search for specific archived footage based on temporarily saved video monitoring footage (approximately 30-60 days).

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

A one-way connection from HSPD-12 to Siemens PACS is used to transmit data, Siemens PACS transmits data to the RSP system using a one-way connection.

(g) Any information sharing conducted by the system

PACS does not conduct public information sharing and does not share, or provide to any other internal systems.

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

Citation of the legal authority to collect PII and or/BII is United States Code, 2015 Edition Title 5 PART 1 – CHAPTER 3 Sec. 301 – Departmental Regulations (5 U.S.C. 301); Executive Order 9397 Numbering System for Federal Account Relating to Individual Persons (E.O.9397) and Homeland Security Presidential Directive 12 (HSPD-12).

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

PACS is considered a business-essential system with a Federal Information Processing Standard (FIPS) 199 security categorization of Moderate.

<u>Section 1</u>: 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).

☐ 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 01-2017 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:					

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	□		
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	□		
k. 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): Members of the Public					

2.3 Describe how the accuracy of the information in the system is ensured.

From a technical implementation, USPTO implements security and management controls to prevent the inappropriate disclosure of sensitive information. Security controls are employed to ensure information is resistant to tampering, remains confidential as necessary, and is available as intended by the agency and expected by authorized users. Management controls are utilized to prevent the inappropriate disclosure of sensitive information. In addition, the Perimeter Network (NSI) and EMSO provide additional automated transmission and monitoring mechanisms to ensure that PII/BII information is protected and not breached by external entities.

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. 3206-0182 Declaration of Federal Employment 0651-0041 Public Search Facility User ID and Badging
☐	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 PACS is an electronic physical security system, and provides the capability to restrict and/or control physical access to USPTO facilities, equipment and resources. This system is used by authorized security personnel to manage and monitor multiple entry points, intrusion detection, and video surveillance at the USPTO Headquarters in Alexandria, Virginia and satellite offices in: San Jose, California; Denver, Colorado; Dallas Texas; and Detroit, Michigan. The PII that is collected, maintained, or disseminated is used as an identifier. Information collected is from DOC employees, Contractors, Federal Government personnel, and members of the public that enter the USPTO facilities. Place of birth and date of birth are used as personal identifiers or as secondary identification to differentiate among identities. The photograph and name are used as validation for access and badge number.

5.2 Describe any potential threats to privacy 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.)

Inadvertent private information exposure is a risk and USPTO has policies, procedures and training to ensure that employees are aware of their responsibility of protecting sensitive information and the negative impact on the agency if there is a loss, misuse, or unauthorized access to or modification of sensitive private information. These are the controls in place to address potential threats and insider threats: USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees. The following are USPTO current policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy - (OCIO- POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), USPTO Rules of the Road (OCIO-POL- 36). All offices of USPTO adhere to USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

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: HSPD-12 PIV system. The PACS system receives information from HSPD-12 but does not have the ability to transmit information back to HSPD-12 PIV system. There is a 'one way' sharing from the HSPD-12 PIV system to the PACS system with appropriate firewalls and security controls in place.
□	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: Banner warning – See Appendix A	
☐	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: Information is provided on a voluntary basis. If personnel do not provide the requested information in whole or in part, USPTO will not be able to give immediate access or entry to facilities. The person in question will have to go through a longer process before they will be given entry or access. Failure to provide the requested information may affect their placement or employment, and will affect their ability to obtain permanent access to the facility.
☐	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: All information requested is provided on a voluntary basis for purposes of employment and is obtained during the onboarding process for employees and contractors. Members of the public provide consent while providing PII for purposes of obtaining access to USPTO facilities.
☐	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:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: The PACS system does not utilize an external interface but relies on information retrieved from the HSPD-12 PIV system. USPTO's employees have the opportunity to review and update their personal information online through their Employee Personal Page or the Department of Treasury's HR Connect system. Employees may also visit the USPTO's Office of Human Resources (OHR) department for additional assistance. Public visitors can access logs of their information through a FOIA request.

<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. Suspicious system log behavior and log failures are reported to the appropriate personnel to troubleshoot and remediate the issue
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 5/13/2021 ☐ 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 supporting 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 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).*

The information is protected in accordance with the NIST 800-53, Revision 4 control set.
Security Assessment and Authorization activities are routinely conducted for PACS. Secured technical architecture is incorporated into the system to prevent any unauthorized access. Data is maintained in areas accessible only to authorized personnel who are required to use two-factor authentication.

Management Controls:

a. The USPTO uses the Life Cycle review process to ensure that management controls are in place for PACS. 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 checks on all personnel, including contractor staff.
b. The USPTO Personally Identifiable Data Extracts Policy

Operational Controls:

1. Automated operational controls include securing all hardware associated with PACS 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 a 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.

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 is in place.

Encrypt and password-protect prior to transmission any sensitive PII data extracts that are sent to an external e-mail address via the Internet. The password key should be forwarded to the recipient in a separate e-mail from the attached file.

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 and number *(list all that apply)*: COMMERCE/PAT-TM-17 USPTO Security Access Control and Certificate Systems COMMERCE/ PAT-TM-18 USPTO Personal Identification Verification (PIV) and Security Access Control Systems COMMERCE/DEPT-25 Access Control and Identity Management System
☐	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: • GRS 5.6, items 090, 110, 111, 120, and 130 • Transmittal 31 Schedules ONLY (no crosswalks or FAQs) (archives.gov)
☐	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. *(The PII Confidentiality Impact Level is not 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 levels. *(Check all that apply.)*

☒	Identifiability	Provide explanation: Name, Birth date, Birth Place, Photograph are all personal identifiers that can help identify a particular individual.
☒	Quantity of PII	Provide explanation: Collectively, the number of records collected generate an enormous amount of PII and a breach in such large numbers of individual PII must be considered in the determination of the impact level.
☒	Data Field Sensitivity	Provide explanation: a combination of name, birth date, and birth place can make the data more sensitive.
☒	Context of Use	Provide explanation: Information is for identifying individuals to provide physical access to USPTO assets.
☒	Obligation to Protect Confidentiality	Provide explanation: Based on the data collected USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974.
☒	Access to and Location of PII	Provide explanation: Necessary measures must be taken to ensure the confidentiality of information during processing, storing and transmission of the data. Access controls are used to ensure only authorized personnel have access to the sites including satellite sites where the system is located.
☐	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.)

Insider threats and foreign entities are the potential threats to the data in the system. USPTO has several controls in place to address these threats: USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees. The following are USPTO current policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy - (OCIO- POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), USPTO Rules of the Road (OCIO-POL- 36). All offices of USPTO adhere to USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

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.

Appendix A – Banner Warning

**************WARNING***WARNING***WARNING************

This is United States Patent and Trademark Office (USPTO) computer system, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access, use, modification, or disclosure of the data contained herein or in transit to/from this system constitutes a violation of the Computer Fraud and Abuse Act, Pub. L. No. 99-474, codified at 18 U.S.C. 1030, state criminal and civil law and may subject violators to criminal, civil and/or administrative action and penalties. Regardless of geographic location, authorized use of this system must comply with USPTO policy, as documented in the USPTO AAO 202-737 (Limited Personal Use of Government Equipment), AAO 212-4 (Information Technology Security Policy) and the USPTO Rules of the Road. Unauthorized use or actions exceed authorized use of USPTO systems will be investigated, and, when appropriate, official sanctions will be imposed. All data contained on USPTO computer systems is owned by the USPTO may be monitored, intercepted, recorded, read, copied, or captured in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may give to law enforcement officials, for investigation and prosecution, any potential evidence of crime found on USPTO computer systems. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, OR CAPTURING and DISCLOSURE. Suspected access, violations or policy infractions should be reported to the USPTO Service Desk, (571) 272-9000.