

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



**Privacy Impact Assessment
for the
Enterprise Physical Access Control System**

Reviewed by: Deborah Stephens, 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

TIFFANY DANIEL Digitally signed by TIFFANY DANIEL
Date: 2026.04.15 15:42:12 -04'00'
4/15/2026

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

Date

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

Unique Project Identifier: EBPL-PFM-07-00

Introduction: System Description

Provide a brief description of the information system.

Enterprise Physical Access Control System (EPACS) is a hybrid cloud electronic physical security system that 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 and Regional Offices. The components contained in EPACS include the following:

- CCURE9000
Security management system that provides access control. CCURE9000 automates the retrieval of personal, configuration, hardware and audit data from all facilities within the organization. CCURE9000 is tied into all USPTO badge readers and wired keypads.
- Genetec Security Center
Video management system used to monitor live events as well as record video.
- Briefcam Enterprise Video Analytics
Enables users to accelerate investigations, derive operational intelligence and attain situational awareness.
- Zenitel
Provides intercom capability for improved communications and verbal verification access.

Address the following elements:

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

Major Application

(b) System location

Alexandria, VA

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

EPACS interconnects with the following systems:

Identity Credential Access Management Identity as a Service (ICAM-IdaaS)- is an infrastructure information system that provides authentication and authorization service to secure all USPTO enterprise applications and provides audit ability to user activity. EPACS receives data from USAccess through ICAM-IdaaS.

Network and Security Infrastructure (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 United States Patent and Trademark Office (USPTO).

Enterprise Data Warehouse (EDW)- system is an automated information system (AIS) that provides access to integrated United States Patent and Trademark Office (USPTO) data to support the decision-making activities of managers and analysts in the USPTO's business areas as needed to achieve business goals. It helps USPTO managers and analysts to answer a variety of strategic and tactical business questions using quantitative enterprise business information. Specifically, EDW provides a tool that allows managers and analysts to analyze business processes, resource use and needs, and other facets of the business.

USPTO AWS Cloud Services (UACS)- IT solutions inclusive of public cloud general support systems, scalable multi-site elastic infrastructure.

Identity Management Authenticator (ID-AUTH)- is an end-to-end system tasked with managing the personal identity credentials of United States Patent and Trademark Office (USPTO) employees and contractors. ID-AUTH consists of four sub-components: Card Management System (CMS), Internal Public Key Infrastructure-Smart Card (IPKI), RSA & MIDM. ID-AUTH system supports the personalization and issuance of Smart Card identification credentials under HSPD-12. The HSPD-12 credential (photo ID badge) and the issuance process applies to all USPTO employees and contractors. The ID-AUTH system manages the personal identity credentials (photo ID badge) of all USPTO employees and contractors seeking physical access to USPTO facilities and logical access to USPTO information systems. The ID-AUTH integrates both the physical and logical access controls

Enterprise Software Services (ESS)- An Infrastructure information system and provides a variety of services to support USPTO missions.

Enterprise Windows Servers (EWS)- is an Infrastructure information system, and provides a hosting platform for major applications that support various USPTO missions

SCS-SaaS-Crowdstrike (Crowdstrike)- is a Software as a Service (SaaS) solution, as defined by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145. Crowdstrike enables USPTO to identify unknown malware, detect zero-day threats, identify advanced adversaries, and prevent damage from targeted attacks in real-time.

Security and Compliance Services (SCS)- Provides a centralized command and control console with integrated enterprise log management, security information and event management, network behavior analysis, and reporting through the collection of events, network/application flow data, vulnerability data, and identity information.

Storage Infrastructure Managed Service (SIMS)- Provides access to consolidated, block level data storage and files system storage.

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

EPACS is hybrid a security management system operating on the PTO network, with servers both on-site and in the cloud. It can be accessed from desktops and workstations by authorized security personnel to manage staff access, monitor multiple entry points and oversee video surveillance

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

Authorized users retrieve 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 90 days).

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

The transmission of information is facilitated by an encrypted communication between interconnected systems.

(g) Any information sharing

Information is shared within the bureau

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

35 USC 2, 5 U.S.C. 301, Federal Information Security Management Act (40 U.S.C. §11331), and HSPD-12

- (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.

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): Credential number, Individual Credential issue, and Person identifier (USPTO Unique ID).					

*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. Marital Status	☐
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.

The system is secured using appropriate administrative physical and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, and auditing). Mandatory IT awareness and role-based training is required for staff who have access to the system and address how to handle, retain, and dispose of data. All access has role-based restrictions and individuals with privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random, periodic reviews (quarterly) to identify unauthorized access and changes as part of verifying the integrity of administrative account holder data and roles. Inactive accounts will be deactivated and roles will be deleted from the application.

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 Security and Compliance Services (SCS) provide additional automated transmission and monitoring mechanisms to ensure that PII/BII information is protected and not breached by external entities. 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 Privacy Act request. They can also amend incorrect information through filing a Privacy Act amendment request.

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 for 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): Click or tap here to enter text.			

☐	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).

Access to EPACS is restricted to authorized Federal employees, contractors, and system administrators, who authenticate via government issued laptops using Okta – Single Sign On. The system collects and processes information such as employee ID, user ID, name, work email, and telephone number to support security and system access.

For individuals entering the facility including employees, contractors, and members of the public, additional information may be collected, but not all is stored including date of birth, place of birth, driver's license, badge data, date/time of access, vehicle identifiers, credential number, individual credential issue, and person identifier. All information is used solely to ensure secure access, monitor facility entry, and maintain overall security.

- 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.)

In the event of computer failure, insider threats, or attack against the system by adversarial or foreign entities, any potential PII data stored within the system could be exposed. To avoid a breach, the system has certain security controls in place to ensure the information is handled, retained, and disposed of appropriately. Access to individual's PII is controlled through the application, and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. These audit trails are based on application server out-of-the-box logging reports reviewed by the Information System Security Officer (ISSO) and System Auditor and any suspicious indicators such as browsing will be immediately investigated and appropriate action taken. Also, system users undergo annual mandatory training regarding appropriate handling of information.

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 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 or the General 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 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: EDW ICAM-IDaaS ID AUTH ESS UACS EWS NSI CrowdStrike SCS SIMS USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation. Encryption and access controls are used to prevent PII/BII leakage
☐	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: https://www.uspto.gov/privacy-policy	
☒	Yes, notice is provided by other means.	Specify how: Notice is provided when entering USPTO that the facilities are being monitored. This PIA serves as notice.
☐	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: Visitor information is provided on a voluntary basis. If visitors 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 ability to obtain temporary access to the facility.
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Employees are required to provide information. Failure to provide the requested information may affect their placement or employment, and will affect their ability to obtain permanent access to the facility.

- 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	Specify how: All information requested is provided on a voluntary basis for purposes of employment and is obtained
-------------------------------------	---	--

	PII/BII.	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: Individuals do not have the opportunity to consent to particular uses of their PII/BII as it is necessary to gain access of the facility and monitor the security of the USPTO.

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: USPTO's employees have the opportunity to review and update their personal information online through their Employee Personal Page and/or HR Connect
☐	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): ☒ 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).

PII within the system is secured using appropriate management, operational, and technical safeguards in accordance with NIST requirements. Such management controls include a review process to ensure that management controls are in place and documented in the System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII/BII data to a small subset of users. All access has role-based restrictions and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The system maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity. Data is encrypted in transit and at rest.

The information is protected in accordance with the NIST 800-53, Revision 4 control set. Security Assessment and Authorization activities are routinely conducted for EPACS. 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 EPACS. 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 EPACS 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.

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. <i>(list all that apply):</i> COMMERCE/PAT-TM-18 USPTO Personal Identification Verification (PIV) and Security Access Control Systems COMMERCE/DEPT-25 Access Control and Identity Management System GSA/GOV-7 HSPD-12 USAccess
☐	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
☐	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: GENERAL RECORDS SCHEDULE 5.6: Security Management Records 110 - Visitor processing records. 111 - All other facility security areas. 120 - Personal identification credentials and cards. 130 - Temporary and local facility identification and card access records. 090- Facility security management operations records GRS 3.1: General Technology Management Records Item - 020 Information technology operations and maintenance records. Which include access and audit logs. GRS 3.2. Information Systems Security Records , Item 010, 020, 040, 050 Which include system security logs.
☐	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: Name, Birth date, 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. There over 10,000 employees within USPTO.
☒	Data Field Sensitivity	Provide explanation: A combination of name and birth date 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.)

The PII in this system poses a risk if exposed. System users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zone within the cloud and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized accounts. USPTO monitors, in real-time, all activities and events within the servers storing the potential PII data and personnel review audit logs received on a regular bases and alert the appropriate personnel when inappropriate or unusual activity is identified.

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 or the General 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.