Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Identity Management Authenticator (ID-AUTH)

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: 2026.04.09 12:50:34 -04'00' 4/09/2026

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

AN: 03252615342806

U.S. Department of Commerce Privacy Impact Assessment
USPTO Identity Management Authenticator (ID-AUTH)

Unique Project Identifier: EIPL-DS-09-00

Introduction: System Description

Provide a brief description of the information system.

Identity Management Authenticator (ID-AUTH) is an Applications information system consisting of two sub-components.1. Internal Public Key Infrastructure (IPKI) and 2. Machine Identity Management (MIDM). The purpose of the ID-AUTH system is the issuance and management of IPKI digital certificates and management of the cloud-based solution for Public Key Infrastructure (PKI). The Machine Identity Management (MIDM) system (cloud PKI system) consists of system for digital certificates, certification authorities (CAs), Online Certificate Status Protocol (OCSP) and other registration authorities (RAs) that verify and authenticate the validity of each party involved in an electronic transaction through the use of public key cryptography.

Address the following elements:

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

ID-AUTH is a Major Application.

(b) System location

The IPKI production infrastructure is located in the Manassas, VA datacenter.

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

ID-AUTH interconnects with the following systems:

- **Access Accessibility Management Platform (AMP) -** A collection of communication and customer relationship-focused solutions that provides secure and accessible electronic 'front doors' to the USPTO enabling the public and staff to easily connect to Patent and Trademark content & tools, exchange information, and improve customer and employee experiences.

- **Building, Assets & Property Management (BAPM) -** The BAPM Boundary will consist of two (2) P&FM components: Radio Frequency Identification (RFID) is an Enterprise-Level asset tracking solution to reduce the inventory management burden of asset management while increasing asset visibility of critical assets and improved inventory accuracy; Property & Facility Scheduling (PFS) consist of two schedulers, FLU Shot, and RoomRez and are applications used for scheduling appointments around USPTO.

- **OpenWater LI-SaaS -** OpenWater is a general-purpose application and review system. Low impact, non-mission critical information can be collected by OpenWater and centralized for reviewers to provide scores and feedback. USPTO uses OpenWater to collect and review nominations of individuals, teams, and organizations for various award programs. Members of the public submit nominations, to include biographical information and letters of recommendation, and then a committee of judges evaluates and scores the nominations within the system. Nominators and judges have their own unique log-in information to access the system. USPTO staff have administrative access and can change the nomination or judging process as needed.

  USPTO also uses OpenWater to collect and review applications of individuals, teams, and organizations for the Patents and Trademarks for Humanities programs. Members of the public submit an application and then a committee of judges evaluates and scores the nominations within the system. Applicants and judges have their own unique log-in information to access the system. USPTO staff have administrative access and can change the application or judging process as needed.

- **Enterprise Data Services-Databricks (EDS-DBX) -** Databricks provides tools for the Big Data Reservoir (BDR) application to perform data processing and Machine Learning initiatives against datasets to support the agency mission. It performs analysis and studies massive amounts of data.

- **OCCO-Web** - provides the public, internal and key stakeholders with information from USPTO about all aspects of intellectual property. It serves as the main web-based information dissemination channel for the Agency and provides links to public-facing, web-based applications used to conduct the Agency's day-to-day operations at www.uspto.gov. It also includes USPTO's corporate intranet website, PTOWeb serving as the primary internal communication, information dissemination and collaboration system for employees and contractors. Offices within the USPTO are able to utilize the Intranet Website to meet everyday business goals on the ptoweb.uspto.gov web site. Additionally, the Image Gallery provides the ability to catalog, track, and make available accurate set of approved images for use on USPTO web properties. The solution is based

on an Open-source product (Gallery) and is targeted at a limited user group of USPTO internal users.

- **Reference Document Management Services (RDMS) -** The RDMS system is designed to serve as USPTO's enterprise-wide content management solution for reference and guidance documents – a critical tool for patent and trademark examiners and applicants. The current RDMS system state allows intranet web-based access to Manual for Patent Examination Procedures (MPEP) and the Trademark Manual for Examination Procedures, the primary guidance document utilized by Patent and Trademark examiners. RDMS does allow public internet access to applicants who wish to submit patent and trademark applications.

- **AWS Cloud Services (UACS) -** To support the vision to deliver IT Solutions, better, cheaper and faster in an effort to conduct the majority of our business via digital means by 2025 the UACS team is focused on providing a multi-site, scalable, and elastic infrastructure and technology platform to adopt AWS with a cloud-first approach for both new and existing workloads when cost feasible. If done well, it is likely to accelerate the decrease in data center footprint, lower the time to market for new projects and prototypes, and enhance our ability to react to scalability requirements for application hosting and cloud data storage.

- **USPTO Subscription Center (USC) -** USPTO Subscription Center is hosted externally on GovDelivery Communication Cloud. The GovDelivery Communications Cloud is a Software as a Service (SaaS) Community Cloud offered by GovDelivery to Federal, State, and Local Government organizations. The Communications Cloud provides these organizations with a number of features to support the efficient communication of timely information to the general public. It provides a comprehensive digital communications management solution tailored to public sector requirements. It is designed to facilitate and increase citizen engagement with public government messaging. It also enables citizens (hereinafter referred to as "End Users") to more effectively communicate with the Government by providing secure case tracking and collaboration mechanisms.

  In addition to facilitating administrators' communication with members of the public, Communications Cloud also provides capabilities that enhance the ability of members of the public to communicate with administrators. The Communications Cloud provides a case management system for tracking issues submitted by members of the public. It also provides secure collaboration portals for the exchange of information on an invite only basis.

- **Adobe Experience Manager-Managed Services (AEM-MS)** - is an enterprise service for signature. The service provides signed receipts to the users for their payment. The system is deployed as a Software as a Service (SaaS) platform with Adobe Corporation managing and maintaining infrastructure and software. AEM-MS is an external system with AEM-MS FedRAMP Package ID F1509037239. USPTO is only responsible for Hardware Security Manager (HSM), which is hosted in the AWS cloud and managed by the USPTO Aws Cloud Services (UACS).

- **CredPriv-ICAM-CredMGMT (CredPriv) -** USPTO uses SailPoint Lifecycle Management (LCM) also known as ICAM-CredMGMT through Continuous Diagnostics and Mitigation (CDM), to manage USPTO privileged users access to devices and users credential workflow. USPTO integrates ICAM-CredMGMT components to incorporate and correlate data into the Master User Record (MUR) for reporting to a centralized SailPoint IIQ at NIST/DOC.

- **USPTO Google Cloud Services (UGCS) -** The UGCS General Support System (GSS) is a standard infrastructure platform used to support the USPTO's Patent Search AI System, USPTOs future AI/ Auto ML systems, and other USPTO Tenants, hosted in the Google Cloud Platform (GCP) us-east4, Northern Virginia, environment. The GCP us-east4 environment is comprised of several sub-components including, Virtual Private Cloud (VPC networks), Cloud Computing (GCP Compute Engine), Identity and Authentication Management (IAM), and resilient cloud storage (GCP Cloud Storage).These services are explained in greater detail below and further in the Google Cloud Platform Services East/West IaaS SSP. UGCS provides administrative efficiency, improves security, and provides better oversight across the Patent Search AI application, which is the only application that resides on the UGCS platform. The system provides a central location for where all USPTO GCP baseline infrastructure services, used in the USPTO's Patent Search AI System, USPTOs future AI/ Auto ML systems, and other USPTO Tenants, can be operated, managed, and monitored. UGCS also provides the ability to improve the facilitation of application development by offloading developers' non-core competencies to the operations and maintenance team supporting UGCS. Essential services such as user account administration, access control, networking infrastructure, logging and the UGCS platform and their support team will address monitoring, standardized server images, and the support of those components.

- **USPTO Microsoft Azure Cloud Services (UMACS) -** The UMACS is a cloud infrastructure platform used to support USPTO Application Information Systems hosted in the Azure East/West environment. The Azure East/West environment is comprised of several sub-components including, Virtual Private Network (vNet) Cloud Computing, Identity and Authentication Management (AAD), and Azure Managed Disks.

UMACS provides administrative efficiency, improves security, and provides better oversight across all applications which reside on the UMACS platform. The system provides a central location for where all USPTO Azure applications can be operated, managed, and monitored. UMACS also provides the ability to improve the facilitation of application development by offloading developers' non-core competencies to the operations and maintenance team supporting UMACS, the Software Services Branch (SSB). Essential services such as user account administration, access control, networking infrastructure, logging and monitoring, standardized server images, and the support of those components will be addressed by the UMACS platform and their support team.

- **Private Branch Exchange-Voice over Internet Protocol (PBX-VOIP) -** The PBX-VOIP (Private Branch Exchange-Voice over Internet Protocol) is an infrastructure information system, consisting of the Cisco-VoIP, ECC, OVOC and PTOFAX subsystems that provides the following services in support of analog voice, digital voice, collaborative services and data communications for business units across the entire USPTO:
  - Converged and non-converged analog and digital voice communication services
  - Teleworker collaborative computing environment
  - Customer Contact Center voice and terminal support
  - Administration of MS Teams phones
  - Submission of documents, payments, and provide communication services for external and internal community

- **Trilateral Network (TRINET) -** TRINET is an infrastructure information system, and 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 United States Patent and Trademark Office (USPTO), the European Patent Office (EPO), and the Japanese Patent Office (JPO). The TRINET members consist of the World Intellectual Property Office (WIPO), Korean Intellectual Property Office (KIPO) and the Taiwan Intellectual Property Office (TIPO).

- **DesignVision (DV)** - is a SaaS capability that enables examiners working on patent applications to search images in design databases by using images as a query. DV uses artificial intelligence (AI) technologies. The SaaS vendor is Clarivate and the solution is deployed in Amazon Web Services (AWS) GovCloud (US). DV compares uploaded images, including images from unpublished design applications, with available databases and yields image results based on similarity and sortable by similarity. Available databases include access to design patents, registrations, trademarks, and industrial

designs from global Intellectual Property offices. USPTO employees and USPTO contractors can search, retrieve, and save content provided by the AI-powered image search tool in accordance with USPTO procedures.

- **Patent Exam Center (PEC) -** PEC Allow the USPTO Patent Examiners the ability to search U.S. patent documents in the USPTO databases. The PEC application is deployed in Amazon Web Services (AWS) and operates in an AWS virtual private cloud (VPC). It is a standalone application that interface with other USPTO information systems like PSAI, DAV and OC. The patent text and image data provided to the patent examiners is a replica of examiner search collections used internally in USPTO.

- **Trademark Exam (TM-EXM) -** Trademark Exam (TM-EXM) is a center where trademark attorneys and professional staff have the ability to securely login and complete end-to-end review and processing of trademark applications/registrations. Trademark Exam provides the ability to manage workload, conduct searches of multiple databases, update/change application/registration data, communicate with internal business units and with applicants/registrants, check and update application/registration statuses, and process fees and refunds.

  TM-EXM accomplishes this through the use web application and supporting systems (microservices) in a cloud environment (Amazon Web Services). Backend shared services will provide an API that other USPTO teams will use to retrieve information. Our front-end services will use a web application that trademark attorneys will use to accomplish their mission.

- **Enterprise Desktop Platform (EDP)** is an infrastructure information system which provides a standard enterprise-wide environment that manages desktops and laptops running on the Windows 7 and Windows 10 operating system (OS), providing United States Government Configuration Baseline (USGCB) compliant workstations.

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

- **Data Storage Management System (DSMS)** provides the following services or functions in support of the USPTO mission: Secure environment for archival and storage of data and records vital to USPTO's Business Continuity and Disaster Recovery plan. Each of the Automated Information Systems (AISs) comprising Data Storage Management provides a different set of capabilities.

- **Security and Compliance Services (SCS)**, formally EMSO, provides enterprise level monitoring to the USPTO.

- **Enterprise Software Services (ESS)** provides an architecture capable supporting current software service.

- **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; Dallas Texas; and Detroit, Michigan.

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

ID-AUTH is an Applications information system consisting of two sub-components.1. IPKI and 2. MIDM. The purpose of the ID-AUTH system is the issuance and management of IPKI digital certificates and management of the cloud-based solution for PKI. IPKI also assist with the management for physical access by exchanging information with USPTO Physical Access Control Systems (PACS). The MIDM system (cloud PKI system) consists of a system of digital certificates, CAs, OCSP and other RAs that verify and authenticate the validity of each party involved in an electronic transaction through the use of public key cryptography.

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

Only ID-AUTH privilege users with associated roles have access to the application. ID-AUTH users must logon to workstation systems prior to authenticating to the ID-AUTH system. ID-AUTH users are statically defined.

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

All data is digitally signed and transmitted with no privacy data stored locally to meet the stringent privacy guidelines.

(g) Any information sharing

ID-AUTH integrates with both the physical and logical access control systems to ensure the USPTO facilities and information systems are accessed by authorized personnel. Therefore, PII about employees and contractors will be directly accessible and shared within the bureau. PII about employees and contractors will be shared on a case-by-case basis with other federal agencies and the private sector.

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

Homeland Security Presidential Directive 12 (HSPD-12).

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

ID-AUTH is a Moderate system.

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):					
*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 biometric information that is stored on the USPTO-issued PIV card is controlled and safeguarded by the actual smart card device and the security boundaries that are associated with those tokens. The risk assessments and technical solution provided by these PIV card products has been fully assessed and or tested by NIST and GSA and they have been approved by those agencies as acceptable for federal government use.

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.
☒	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).

ID-AUTH manages digital certificates of all USPTO employees and contractors seeking physical access to USPTO facilities and logical access to USPTO information systems. The photograph and fingerprints of the applicant which were captured during enrollment and placed on the credentials for electronic identity validation when the credentials are presented for access to secure areas.

The lifecycle associated with secure credentials includes management activities, which are ongoing after a credential has been issued to a cardholder. Credentials can be lost, cardholders may go on extended leave of absences, or cardholders may no longer be affiliated with the sponsoring organization.

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.)

USPTO has identified and evaluated potential threats to PII/BII such as insider threats and adversarial entities which may cause a loss of confidentiality, accessibility, and integrity of information. In the event of computer failure or attack against the system, records of USPTO employees or contractors containing PII could be exposed.

Controls that the bureau/operating unit have put into place to ensure that the information is handled, retained, and disposed appropriately include training, access restriction, password protection, and data retention policies. USPTO has Security Information and Event Management (SIEM) systems that monitor in real-time all the activities and events within the servers storing PII and USPTO C3 personnel review audit logs received on a regular basis and alert the ISSO and/or the appropriate personnel when unusual activity is identified.

Stringent physical access controls are in place to restrict access to the datacenter and to the rack with the servers hosting the database to only a few authorized individuals. The building has security guards and secured doors. All entrances are monitored through electronic surveillance equipment. The hosting facility is supported by 24/7 onsite hosting and network monitoring by trained technical staff. Physical security controls include indoor and outdoor security monitoring and surveillance; badge and picture ID access screening; and pin code access screening.

USPTO monitors in real-time all activities and events within the servers storing the potential PII data and a subset of USPTO C3 personnel review audit logs received on a regular bases and alert the ISSO and or the appropriate personnel when inappropriate or unusual activity is identified. Access is restricted on a "need to know" basis, and there is utilization of Active Directory security groups to segregate users in accordance with their functions.

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: ID-AUTH interconnects with: • DSMS • AMP • BAPM • OpenWater LI-SaaS • EDS-DBX • OCCO-WEB

	• RDMS • UACS • USC • AEM-MS • CredPriv • UGCS • UMACS • PBX-VOIP • TRINET • DV • PEC • TM-EXM • SCS • ESS • PACS Stringent physical access controls are in place to restrict access to the datacenter and to the rack with the servers hosting the database to only a few authorized individuals. The building has security guards and secured doors. All entrances are monitored through electronic surveillance equipment. The hosting facility is supported by 24/7 onsite hosting and network monitoring by trained technical staff. Physical security controls include indoor and outdoor security monitoring and surveillance; badge and picture ID access screening; and pin code access screening. USPTO monitors in real-time all activities and events within the servers storing the potential PII data and a subset of USPTO C3 personnel review audit logs received on a regular bases and alert the ISSO and or the appropriate personnel when inappropriate or unusual activity is identified. Access is restricted on a "need to know" basis, and there is utilization of Active Directory security groups to segregate users in accordance with their functions.
☐	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: See Appendix A: Privacy Act Notice.	
☐	Yes, notice is provided by other means.	Specify how:
☒	No, notice is not provided.	Specify why not: Due to PIV migrations to USAccess the PIV enrollment was removed from ID-Auth.

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:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Individuals do not have the opportunity to decline to provide PII. Failure to provide the requested information may affect system based digital certificates

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:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: The information requested is required for the purpose of ID-AUTH. Failure to provide the requested information may affect the system ability to obtain digital certificates.

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: Individuals have the opportunity to review/update PII/BII through the electronic web-based portal of the ID-AUTH system, http://ptoweb.uspto.gov/ptointranet/ptosecurity/hspd/hspd_name.htm. See Appendix A
☐	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): 1/16/2026 ☐ 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).*

USPTO uses the following system controls to protect PII/BII on the ID-AUTH system.
Management Controls:

a) The USPTO uses the Life Cycle review process to ensure that management controls are in place for ID-AUTH. 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 perfoming national agency checks on all personnel, including contractor staff.
b) The USPTO uses the Personally Identifiable Data Extracts Policy. This means no extracts of sensitive data may be copied on to portable media without a waiver approved by the DOC CIO.

Operational Controls:

a) Access to all PII/BII data is for users on PTONet who have verified access to ID-AUTH. Additionally, access to PII/BII data is restricted to a small subset of ID-AUTH users.
b) Manual procedures are 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:
    1. 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.
    2. 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.
    3. Obtain management concurrence in the log, if an extract aged over 90 days is still required.

4. 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).
5. 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.

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.

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)*: PAT/TM-8 Patent Application Secrecy Order Files GSA/GOV-7: HSPD–12 US Access PAT/TM-17 USPTO Security Access Control and Certificate 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 120 and 121, Personal Identification Credentials and Cards GRS 3.2, items 060 and 06, PKI Administrative Record
☐	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: ID-AUTH collects, maintains, or disseminates PII about USPTO employees and contractors. The types of information collected, maintained, used or disseminated by the system includes, for example, name, and fingerprint. When combined or alone, this data set uniquely and directly identifies individuals. If the PII

		were inappropriately accessed, used, or disclosed, potential harm could result to the subject individuals and or the organization.
☒	Quantity of PII	Provide explanation: PII/BII is collected for all USPTO employees and contractors who have logical and physical access to USPTO assets. Collectively, the number of records collected generate an enormous amount of PII and a breach would result serious collective harm to a substantial number of individuals and harm to the organization's reputation.
☒	Data Field Sensitivity	Provide explanation: A combination of name and fingerprint makes the data field more sensitive. For example, individuals and organizations will be vulnerable to harms such as identity theft, embarrassment, or loss of trust.
☒	Context of Use	Provide explanation: Information is for identifying individuals to provide logical and physical access to USPTO assets.
☒	Obligation to Protect Confidentiality	Provide explanation: USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974 and USPTO Privacy Policy requires the PII information collected within the system to be protected in accordance with NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information.
☐	Access to and Location of PII	Provide explanation:
☐	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.)

USPTO has identified and evaluated potential threats to PII/BII such as insider threats and adversarial entities which may cause a loss of confidentiality, accessibility, and integrity of information. In the event of computer failure or attack against the system, records of USPTO employees or contractors containing PII could be exposed. Controls that the bureau/operating unit have put into place to ensure that the information is handled, retained, and disposed appropriately include training, access restriction, password protection, and data retention policies.

USPTO has SIEM systems that monitor in real-time all the activities and events within the servers storing PII and USPTO C3 personnel review audit logs received on a regular basis and alert the ISSO and/or the appropriate personnel when unusual activity is identified. In addition, database servers storing PII are segregated in a highly sensitive zone within the USPTO internal network, and an additional dedicated network firewall/intrusion prevention system (IPS) and a dedicated network switch through Access Control list that limits access restricted to only a few approved and authorized accounts protect the highly sensitive zone. Stringent physical access controls are in place to restrict access to the datacenter and to the rack with the servers hosting the database to only a few authorized individuals. The building has security guards and secured doors. All entrances are monitored through electronic surveillance equipment. The hosting facility is supported by 24/7 onsite hosting and network monitoring by trained technical staff. Physical security controls include indoor and outdoor security monitoring and surveillance; badge and picture ID access screening; and pin code access screening. The biometric information that is stored on the PIV card is controlled and safeguarded by the actual smart card device and the security boundaries that are associated with those tokens. The risk assessments and technical solution provided by these PIV card products has been fully assessed and or tested by National Institute of Standards and Technology (NIST) and GSA and they have been approved by those agencies as acceptable for federal government use.

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: Privacy Act Statement

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Points of Contact and Signatures

Approval Number: 03252615342806

System Owner Name: Bar Bill Office: Integration Services Branch 2 (I/ISB2) Phone: (571) 272-8678 Email: Bar.Bill@uspto.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Barr, Bill approved on 2026-03-29T12:23:45.0196246 Date signed: 3/29/2026 12:23:00 PM	**Chief Information Security Officer** Name: Timothy S. Goodwin Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-0653 Email: Timothy.Goodwin@uspto.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Goodwin, Timothy approved on 2026-03-30T13:33:44.5502144 Date signed: 3/30/2026 1:33:00 PM
Privacy Act Officer Name: Ricou Heaton Office: Office of General Law (O/GL) Phone: (703) 756-1240 Email: Ricou.Heaton@uspto.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: Heaton, John (Ricou) approved on 2026-03-26T07:11:54.7205355 Date signed: 3/26/2026 7:11:00 AM	**Bureau Chief Privacy Officer and Authorizing Official** Name: Deborah Stephens Office: Office of the Deputy Chief Information Officer (I/DCIO) Phone: (571) 272-9410 Email: Deborah.Stephens@uspto.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: Stephens, Deborah approved on 2026-04-06T13:01:12.3945546 Date signed: 4/6/2026 1:01:00 PM