Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Identity Credential Access Management Identity as a Service (ICAM-IDaaS)

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: 2025.11.25 10:41:33 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Identity Credential Access Management Identity as a Service (ICAM-IDaaS)

Unique Project Identifier: EIPL-DS-03-00

Introduction: System Description

Provide a brief description of the information system.

Identity Credential Access Management Identity as a Service (ICAM-IDaaS) is an infrastructure information system that provides authentication and authorization service to secure all United States Patent and Trademark Office (USPTO) enterprise applications and provides auditability to user activity. The system provides the following services to the enterprise:

- User Provisioning and Life Cycle Management
- User Roles and Entitlement Management
- User Authentication and Authorization to protected resources
- Application Integration/Protection
- National Institute of Standards and Technology (NIST) controls compliance related to Audit and Accountability (AU), Access Control (AC), and Identification and Authentication (IA) security control families

Address the following elements:

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

(b) System location
ICAM-IDaaS is located in Alexandria, Virginia and in the Amazon Web Services (AWS) Federal Risk and Authorization Management (FedRAMP) Cloud.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
Adobe Experience Manager- Managed Services (AEM-MS) - is an enterprise service for signature. The service provides signed receipts to the users for their payment. AEM-MS provides electronic signature services as part of the enterprise services to the consumers of the USPTO systems.

Accessibility Management Platform (AMP) - is used to check for accessibility based on 508 compliance for pdf documents.

Archangel (Archangel) - enables the USPTO to streamline cybersecurity lifecycle; Governance, Risk, and Compliance (GRC) and Continuous Diagnostics and Mitigation (CDM) by eliminating redundancy and automating the process of security accreditation via Continuous Authorization to Operate (cATO). Archangel leverages advance technologies such as Artificial Intelligence (AI), Blockchain and Robotic Process Automation (RPA) to revolutionize security accreditation and risk management. The system automates and streamlines security compliance process by eliminating redundancy, digitalizing workflows, and predicting adherence to security controls. Additionally, it enables continuous monitoring of device logs and proactively identifies vulnerabilities and potential breaches, ensuring robust and adaptive security management for critical systems.

Corporate Administrative Office System (CAOS) - is an application information system. The purpose of the CAOS is to support the Human Resources business functions within the USPTO. The CAOS supports all activities associated with the recruitment and management of USPTO personnel. The CAOS is composed of three (3) Automated Information Systems (AISs) that provide the following capabilities:

- Allows USPTO employees' Time and Attendance information to be entered, verified, electronically certified and collected for transmission to the Department of Agriculture's National Finance Center's (NFC) personnel/payroll system.
- A broad range of data processing and management capabilities including specialized features, capabilities to provide the Office of Security & Safety the ability to track and manage data.
- Enables eligible USPTO employees to manage the information about their primary and secondary telework sites and allows USPTO employee supervisors to review and approve employee telework sites.

Corporate Administrative Office System-Cloud (CAOS-C) – will be hosted in USPTO AWS Cloud Services (UACS) cloud. Enterprise Telework Information System (ETIS) will be the initial application in the boundary. ETIS enables eligible USPTO employees to manage their telework agreements along with the information about their primary and secondary telework sites. USPTO employee supervisors use this to review and approve employee telework sites. Employees enter telework locations and are able to make telework address changes and submit changes to telework programs for approval within the system.

Critical Event Management System (CEM) - is designed to fulfill the USPTO mission of ensuring safety and security during critical emergency events. CEM provides seamless multi-

platform notifications and a unified crisis management platform for coordinated response, ensuring effective command, control, and business resilience during critical events.

Consolidated Financial System (CFS) - is a Master System composed of the following four (3) subsystems: 1) Momentum 2) E-Acquisition (ACQ) and 3) VendorPortal. CFS and its subsystems assist USPTO in executing financial transactions.

Customer Interaction Platform – Salesforce (CIP-SF) - is a cloud-based Software as a Service (SaaS) Customer Relationship Management application that provides functionality focused on events management, event registration, customer service and analytics.

Cloudflare (Cloudflare) - provides protection for USPTO infrastructure by defending against Distributed Denial-of-service (DDoS) attacks, ensuring data integrity through Domain Name System Security Extensions **(**DNSSEC) support using technology as well as providing content filtration and malware defense. DNSSEC is a suite of protocols designed to enhance the security of the Domain Name System (DNS) by enabling the authentication of DNS responses. It uses digital signatures based on public key cryptography to ensure that the data received from a DNS query is authentic and has not
been tampered with.

Case Management System (CMS) - provides a Cloud based system designed to assist the Office of Civil Rights staff in processing background investigations, employee relations and equal employment cases and requests for reasonable accommodation by collecting and maintaining data.

Collection of Multiple Enterprise Tools (COMET) - is a collection of independent applications that live on the ORACLE's Application Express (APEX) lightweight database.

Design Vision (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 AI technologies. The SaaS vendor is Clarivate and the solution is deployed in AWS GovCloud (US).

Enterprise Contact Center-Cloud (ECC-C) - provides technology that allows the public and USPTO employees the ability to contact USPTO business centers and access interactive and automated information regarding USPTO products, processes, and services.

Enrollment and Discipline Information Technology (EDITS) - is a repository of imaging documents serving the USPTO Office of Enrollment and Discipline (OED) and conforms to USPTO IT infrastructure, platform and application requirements specified by the Chief

Information Officer (CIO). EDITS imaging documents are stored, made searchable and retrievable via the OED Information System (OEDIS).

Enterprise Desktop Platform (EDP) - is an infrastructure information system which provides a standard enterprise-wide environment that manages desktops and laptops running on Windows 10 operating system (OS), providing Defense Information System Agency (DISA) Security Technical Implementation Guides (STIG) compliant workstations.

Enterprise Data Services - Databricks (EDS-DBX) - 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.

E-Discovery Software System Cloud (EDSS-C) - provides for the Collection, Processing, Review, Analysis, and Production phases of the Electronic Discovery Reference Model (EDRM). Attorneys and litigation support personnel employ the tool in a variety of legal matters to help organize, search, and review large volumes of Electronically Stored Information (ESI).

Employee Feedback Survey Tool (EFST) - collects survey responses from email-based surveys, text-based surveys, social emails, phone calls, and web scraping, processes them, and reports individual and aggregated responses that can be used to improve agency employee and customer satisfaction based on feedback.

Enterprise Gateway Services (EGS) - supports application-level infrastructure that provides end-point security and traffic management (load balancing) for all production USPTO applications; Maintains capabilities for Load balancing configurations for external-facing and internal applications is managed by EGS where physical management of the appliances is handled within the Office of the Chief Information Officer (OCIO); Enhance capabilities of application-level infrastructure to provide improved operational response using existing monitoring tools and related appliances.

Enterprise Performance Management System (EPM) - is a central planning and budgeting application supporting various organizations across the USPTO. EPM is replacing some of the technology (Oracle Hyperion Planning and Essbase) in the Enterprise Budget Tool (EBT), which is the on premise equivalent of EPM. The software behind EPM is Oracle EPM Cloud Service to provide automation throughout the USPTO's budgeting lifecycle. The main purpose of EPM is to allow the Office of Planning and Budget (OPB) and business units across the USPTO to project employee compensation and benefits within the current fiscal year as well as the following six fiscal years. End of year projections are calculated for

each organization across the USPTO and can be compared to budgeted amounts to support analysis of results to identify causes for variances. It is also used by OPB and business units to formulation and execute their budgets.

Enterprise Software Services (ESS) - provides the USPTO organization with a collection of programs that utilize common business applications and tools for modeling how the entire organization works. In addition, ESS provides a centralized solution for assisting developers in building applications unique to the organization. The software implemented is intended to solve an enterprise-wide problem, rather than specific departmental issues. Enterprise level software aims to improve the enterprise's productivity and efficiency by providing business logic and support functionality, continuous collaborative and communication tools for organizational personnel to complete their everyday task. ESS includes USPTO's Active Direct in its subsystem Enterprise Directory Services.

Enterprise Virtual Event Services (EVES) - is an application information system that enables business units to share vital knowledge through collaboration capabilities that incorporate data, voice, and video communication technologies. Business units will gain efficiency and effectiveness by communicating and sharing vital business knowledge with internal and external customers.

HireVue Recruitment Assessments and Video Interviewing (HireVue) - provides USPTO with an all in one recruitment and employee hiring platform. The HireVue GovCloud should empower USPTO with a modern candidate interview experience, simplification of the hiring process, and an easy to use graphical interface. HireVue GovCloud provides the capability to host on-demand candidate video interviews, perform side by side assessments of candidates, all coordinated through the HireVue scheduling ability.

Fee-Processing Next Generation (FPNG) - is the fee management and revenue collection system at USPTO.

General Counsel Case Tracking System (GCCTS-C) - The Solicitor's Office requires a legal practice management system that performs case docketing, document management, document full text search, ticklers, calendar scheduling, and contact management. These functions are largely met with the COTS web application Legal Files.

Government Retirement and Benefits (GRB) - is a web application that allows Federal Employees or Federal Benefits Specialists to access various retirement and benefits functions and information from a web browser. The main functions of the system

are retirement and benefits administration as well as employee self-service. The GRB Platform provides benefits specialist tools to prepare service histories, create retirement estimate reports, as well various other related estimate reports.

Integrated Automations - Platform (IA) - provides the necessary infrastructure to support Robotic Process Automation in development, test, and production environments. The IA software tools currently used include: UiPath Studio; UiPath Robot; and UiPath Orchestrator.

International Data Exchange - Moderate (IDE-M) - is a system developed by the USPTO that help exchange published and unpublished application data with international stakeholders, including foreign intellectual property offices (IPOs) and the World Intellectual Property Organization (WIPO).

Information Delivery Product (IDP) - is a Master System composed of three subsystems: Enterprise Data Warehouse, Electronic Library for Financial Management Services, and Financial Enterprise Data Management Tools.

Intellectual Property Assignment Systems (IPAS) - is the overall product and systems comprised of all IPAS subsystems which allows Patent and Trademark customers to request for the re-assignment of patents or trademarks via a website. Users are able to create a re-assignment request using a Trademark or Patent template, with dynamic business logic, so that all key data elements are identified and populated, attach required supporting legal documents, and make payments as necessary.

Intellectual Property Leadership Management Support System (IPLMSS) - is an Application Information System that provides capabilities and functionality for patent examiners to perform their roles.

Integrated Workplace Management System (IWMS) - manages all aspects of USPTO facilities—from space and lease management to capital improvement tracking to ensuring timely maintenance.

Legal Document Management System - Cloud (LDMS-C) - is a Microsoft Azure multi-government-only community SaaS solution using NetDocuments software.

Microsoft 365 (M365) - is a product family of productivity software, collaboration and cloud-based services owned by Microsoft.

Master Data Management (MDM) - is a foundational tool of the agency's enterprise data management practices consisting of a FedRAMP moderate authorized SaaS solution known as the Collibra Data Intelligence Cloud (CDIC).

MyUSPTO-C - is the webpage where external and internal users can create a uspto.gov account and start customizing a homepage specific for their profile. The new uspto.gov accounts are designed for individuals, not groups or organizations. Future updates will add the ability for organizations to share information between colleagues.

OpenWater Awards Management Software (OCCO-WEB) - is an external system that USPTO uses to collect and review nominations of individuals, teams, and organizations for the National Medal of Technology and Innovation. 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. The judges are comprised of public experts appointed by the Secretary of Commerce. 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.

Open Data/Big Data Master System (OD/BD MS) - consists of subsystems which support the Big Data Portfolio. OD/BD resides on the USPTO AWS Cloud Services (UACS) platform, which employs IaaS and PaaS services from AWS. The current subsystems under this master system consists of Big Data Reservoir (BDR)/Data Modeling Tool (DMT), Developer Hub (DH)/Open Data Portal (ODP), Collection of Economic Analysis Tools (COEAT) and Bulk Data Storage System (BDSS)

Office of Enrollment and Discipline Item Bank – Cloud (OEDIB-C) - is a FedRAMP Authorized SaaS product implemented with Questionmark OnDemand for Government. OEDIB-C is used by the Office of Enrollment and Discipline (OED) staff to develop and maintain exam content for the Attorney and Agent Registration Exams.

OpenWater LI-SaaS (Open Water LI-SaaS) - 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.

Patent Administrative Center (PAC) - provides central tracking and recording of patent application status and bibliographic data; and its components will directly support the administration of the application processing lifecycle by facilitating the scanning of application documents, initialization of new patent applications, review of security,

formality, document & fee requirements; automated routing of applications; generation, review and mailing of official correspondence to applicants; tracking examiner productivity; and the publication and issuing of patents.

Patent Capture and Application Processing System - Initial Processing (PACPS-IP) - is an Application Information System that provides support for the purposes of capturing patent applications and related metadata in electronic form, processing applications electronically, reporting patent application processing and prosecution status, and retrieving and displaying patent applications. PCAPS-IP is comprised of multiple Automated Information Systems (components) that perform specific functions, including submissions, categorization, metadata capture, and patent examiner assignment of patent applications.

Patent Business Content Management Services (PBCMS) - provides enterprise service pattern that can be leveraged by USPTO systems for processing documents conversion.

Planning and Budgeting Products (PBP) - is a Master System composed of the following three subsystems: 1) Activity Based Information system (ABIS), 2) Enterprise Budgeting Tool (EBT) 3) Patent Resource Management System (PRMS).

VOIP-Private Branch Exchange-Voice over Internet Protocol (PBX-VOIP) - is an infrastructure information system that provides the following services in support of analog voice, digital voice, collaborative services and data communications for business units across the entire USPTO.

Patent Center (PC) - is a unified interface that allows applicants to file, review, and manage patent applications

Patent Capture and Application Processing System - Examination Support (PCAPS-ES) - is an Application Information System (AIS) composed of 19 components to provide patent capture and application processing capabilities and functionality.

Patent End to End (PE2E) - provides a search tool that Patent Examiners use to conduct prior art search.

Patent Exam Center (PEC) - allows the USPTO Patent Examiners the ability to search U.S. patent documents in the USPTO databases. The PEC application is deployed in AWS and operates in an AWS virtual private cloud (VPC).

PEWLAN2-Public & Enterprise Wireless Local Area Network 2 (PEWLAN2) - is a productivity enhancer for the mobile staff, guests, and contractors. A smoothly implemented

wireless LAN facilitates secure wifi network connectivity from anywhere within the organizations spaces. It also provides simple flexibility for cube-sharing, hoteling, and other situations where staff move around and the number of network connections varies over time. Staff with wireless connectivity may not need or even want docking stations, reducing cost and equipment clutter. The USPTO enterprise system is designed to provide not only secure access to PTONet, but to provide guest access outside of the secure boundary using the same infrastructure.

Patent Public Search (PPUBS) - allows public users to search for patent information used during examination to make patentability determinations

Patent Search System - Specialized Search and Retrieval (PSS-SS) - is a General Support System that provides access to specialized data that may include annual submissions of nucleic and amino acid sequence or prior-art searching of polynucleotide and polypeptide sequences, and other types of information that may be more scientific or the technology-based, Patent Linguistic Utility Service (a query by example search system), Chemical Drawing ability, and Foreign Patent Data.

Patent Trial and Appeal Case Tracking System (P-TACTS) - is an application information system and provides supporting USPTO's administrative law body Patent Trial and Appeal Board for electronically filing documents in connection with the proceedings established under the Leahy-Smith America Invents Act (AIA).

Reference Document Management Services (RDMS) - facilitates the revision, publication, and presentation of reference documents used by USPTO employees and the public. A principal benefit of the RDMS is that it replaces disparate revision and publication processes (each having multiple interfaces) into a centralized enterprise-wide content creation and publishing platform; built using a commercial off the shelf (COTS) for content management and XML delivery. Reference documents in RDMS include the Manual of Patent Examination Procedures (MPEP), Trademark Manual of Examination Procedures (TMEP), Trademark Federal Statutes and Rules (TFSR) and Trademark Trial and Appeal Board Manual of Procedure (TBMP).

Rally Development System (RDS) - serves as USPTO Agile Platform and development tool for USPTO employees and projects. Rally allows USPTO developers to continuously track and prioritize work, reallocate development resources, collaborate between teams, and align strategy and development with the USPTO System Development Lifecycle (SDLC) and strategic roadmap. The RDS is externally hosted and is available to USPTO users via a web interface.

Secure Access Service Edge (SASE) - data / voice equip; transport methods to connect systems and people; core connectivity within data centers; connectivity to and within office building & remote locations.

Security and Compliance Services (SCS) - is used to provide enterprise-wide security capabilities.

Service Management Platform (SMP) - leverages established policies and structured processes, performed by the USPTO to plan, deliver, operate, and control the information technology (IT) services offered to customers.

Trademark Exam (TMEXM) - provides systems for internal users, such as examining attorneys, paralegals, and professional staff, to conduct all activities necessary for trademark examination and maintenance including the ability to review application and registration documents, search the Trademark register, draft and issue notices and Office actions, and modify application and registration data.

Trademark Next Generation (TMNG) - is an application information system that provides support for the automated processing of trademark applications for the USPTO.

Trademark Processing System - External (TPS-ES) - is Major Application information system, and provides customer support for processing Trademark applications for USPTO.

Trademark Trial and Appeal Board Center (TTABC) - provides intake and exam centers for Administrative Judges, Interlocutory Attorneys, and Professional Staff. The functionality/workflow will ensure all adversary proceedings brought before the Board are reviewed, processed and routed accordingly to affected Trademark business units or the public, and ensuring all necessary filing fees are of record.

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

USPTO AINS eCase SaaS System (UAECSS) - is a commercial SaaS implemented with AINS eCase /FOIAXpress. This SaaS provides for end-to-end processing of FOIA and Privacy Act requests and appeals. The system electronically stores, retrieves, and redacts documents for delivery to requesters.

USPTO CoSo Cloud Adobe Connect Solution (UCCACS) - instance of CoSo Cloud Adobe Connect solution, is a web communication solution that enables USPTO to provide

online computer-based training to internal audiences. The purpose of this system is to enable USPTO business units to share vital knowledge with USPTO staff.

USPTO Cisco Webex for Government (UCWG) - purpose is to allow internal and external customers to send messages, conduct video communications, share files, join meetings, and hold white-boarding sessions in real time.

USPTO Google Cloud Services (UGCS) - is a General Support System (GSS) that is hosted in the GCP Infrastructure as a Service (IaaS) US-Regions in order to meet high-availability requirements in addition to providing rapid elasticity and easy provisioning of computing resources to meet the demands of end-user consumption.

USPTO Microsoft Azure Cloud Services (UMACS) – is an Infrastructure as a Service (IaaS) will provide a standardized, stable, and security compliant platform for which USPTO systems, project can build upon and be able to inherit core functionality, and security controls implementations.

VBrick Rev Cloud (VRC) - enables large organizations to securely and efficiently deliver high quality live and on-demand video to thousands of viewers using the corporate wide area network and Internet. It provides centralized management over video ingest and storage, user access and permissions, video capture and delivery devices, and video publishing and distribution.

Zoom For Government (ZFG) - is a COTS software hosted on the Cloud; it is used as a USPTO enterprise level videoconferencing tool, primarily used by Global International Intellectual Property (GIPA) staff. Zoom is not a USPTO production-managed software. It is authorized for use with USPTO IT asset.

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

The purpose of the system is to protect USPTO services by authenticating and authorizing users and systems. The system disambiguates the user and provides the integrated partner/system with user's identity and ability to make fine grained authorization decision.

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

Administrators retrieve the information in the system to make profile-specific changes and to support users and/or the system during troubleshooting. All information in the system is encrypted in transit and at rest and access is restricted using user specific role policies. The information can be accessed by logging into the administrator consoles via a web browser

and/or through a user interface. End users may only retrieve their own information once they are authenticated.

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

The internal USPTO users are accessed via Active Directory agents which is part of ESS. There is a one-way synchronization between USPTO Active Directory (AD) and ICAM-IDaaS identity store. All information is encrypted during transmission.

(g) Any information sharing

The system does not share PII with any other systems, USPTO employees and contractors have their information retrieved from AD through a one-way synchronization between AD and ICAM-IDaaS identity store.

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

5 U.S.C. 301; 35 U.S.C. 2; Public Law 106-229; Homeland Security Presidential Directive 12 and, 15 U.S.C. 1051 et seq.

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

The system is categorized as FIPS 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):					
*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.

Internal users are updated via USPTO AD records and external users are verified through their email address. All communications are conducted over secure communications. Access management follows least access privilege policies. User accounts are governed by Access Control, Audit and Accountability, and Assessment, authorization and monitoring policies. The access to user profiles and information is via well-controlled interfaces and process flows. The non-sensitive Personally Identifiable Information is secured using appropriate administrative, physical, and technical safeguards. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access and changes as part of verifying the integrity of data.

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).

PII/BII Information is capture to authenticate user and make/access (authorization) decisions.

For USPTO employees and contractors, who are the internal users, PII/BII is collected via Active Directory synchronization of required traits. Data that is collected from Active Directory are listed below. IP and data/time of access is collected during the login process.
Name
Work Address
Work Email Address
User ID
IP Address
Date/Time of Access

For external users, who are the members of the public, PII/BII is collected via web forms that are populated when the user requests access to USPTO services. Data that is collected via web forms are listed below.
Name
Email address,
IP and date/time of access

Data from the public (1) is used to authenticate and authorize system access, (2) is used at various service desks to assist users, (3) is shared with the Electronic Data Warehouse to assess and report for financial purposes, and (4) is used to assess system performance.

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.)

Insider threats and foreign governments are the potential threats to the system. USPTO has employed several controls to mitigate these threats.
Account activity monitoring:
• Access to privileged operations/resources
• Inactivity is monitored, e.g., accounts not accessed in last 90 days are flagged for deactivation
• Least access policies are in place
• Auditing is in place for non-repudiation
• Auditing logs are reviewed based on policies

All Internal users are required to take privacy and security awareness training.

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: All systems listed in introduction section c (interconnections) send information to ICAM-IDaaS in order for ICAM-IDaaS to ensure the users identity. USPTO Active Directory for internal users (USPTO Government Full Time Equivalent (GFTE) and Contractors) is connected to the Information Technology (IT) system. Technical controls are in place to address security concerns. Least privilege access policies and controls are in place. All information is encrypted during transmission and at rest, users and administrator are required to take security awareness training. Audit records are captured and periodically reviewed. Identity governance system is in place to

	manage and enforce security controls related to Access Control (AC), Audit and Accountability (AU), and Identification and Authentication (IA).
☐	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 privacy policy. The Privacy Act statement and privacy policy can be found at: https://www.uspto.gov/privacy-policy and on login screen https://auth.uspto.gov/app/UserHome	
☒	Yes, notice is provided by other means.	Specify how: This PIA serves as a 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: For members of the public, the service is voluntary, but it can only be provided if they are registered.
☒	No, individuals do not have an opportunity to decline to provide	Specify why not: USPTO employees and contractors do not have the ability to consent to particular uses of their PII. They

	PII/BII.	consent to providing their name (which is then used for the email address) and phone number as part of accepting employment at USPTO.

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: For members of the public, the service is voluntary, but it can only be provided if they are registered.
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: The information is not shared/used for any other purposes other than identification and authentication. USPTO employees and contractors do not have the ability to consent to particular uses of their PII. They consent to providing their name (which is then used for the email address) and phone number as part of accepting employment at USPTO. That information is then used for the primary purpose of acquiring access to applications and the network during onboarding.

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: External users have an opportunity update their profile through MyUSPTO but their information cannot be updated by ICAM-IDaaS. USPTO employees and contractors can update their profiles through Human Resources and active directory administrators

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): 2/3/2025 ☐ 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 5 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 the 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 authorize 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.

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)*: DEPT-25, Access Control and Identity Management System GSA/GOV-7: HSPD-12 USAccess PAT-TM-17, USPTO Security Access Control and Certificate Systems
☐	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: **General Technology Management Records - Information technology operations and maintenance records – GRS 3.1:020 -** Including System logs – **Temporary:** Destroy 3 years after (See GRS for cutoff instructions). **3.2: Information Systems Security Records** 030-031 - System Access Records **Systems not requiring special accountability for access.** These are user identification records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users. **Temporary**. Destroy when business use ceases. **Systems requiring special accountability for access.** These are user identification records associated with systems which are highly sensitive and potentially vulnerable. **Temporary.** Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.
☐	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: User name, phone number, email address, and User ID information could be used to identify a user.
☒	Quantity of PII	Provide explanation: The quantity of PII in the system is large since it will be used for every USPTO employee and some members of the public.
☒	Data Field Sensitivity	Provide explanation: The combination of the different types of PII collected from Active Directory can cause the data to become more sensitive.
☒	Context of Use	Provide explanation: The information is used to authenticate users for access to USPTO resources.
☒	Obligation to Protect Confidentiality	Provide explanation: In accordance with NIST 800-53 Rev. 5, USC implements both AR-2 (Privacy Impact and Risk Assessment) and AR-7 (Privacy-Enhanced System Design and Development) security controls to ensure the confidentiality of all users is protected. Based on the data fields and in accordance with the Privacy Act of 1974, PII must be protected due to requirements.

☒	Access to and Location of PII	Provide explanation: The PII in ICAM-IDaaS is secured using appropriate administrative, physical and technical safeguards. Authorized USPTO staff and contractors have access to the data stored in ICAM-IDaaS. ICAM-IDaaS does not disseminate PII information to any other systems.
☐	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.)

PII in this system pose 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 highly sensitive zones 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.

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.