Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
USPTO Microsoft Azure Cloud Services (UMACS)

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

NICHOLAS CORMIER Digitally signed by NICHOLAS CORMIER
Date: 2026.08.07 11:09:26 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Microsoft Azure Cloud Services (UMACS)

Unique Project Identifier: EIPL-IHSC-03-00

Introduction: System Description

Provide a brief description of the information system.

The United States Patent and Trademark (USPTO) Microsoft Azure Cloud Services (UMACS) is a cloud infrastructure platform used to support USPTO Application Information Systems hosted in the Azure East/West environment. 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 Cloud Services Branch 2 (CSB2). As part of the UMACS Services for Platform as a Service (PaaS) and Software as a Service (SaaS), it provides following services to its consumers: Sentinel, Microsoft Defender, Azure Virtual Desktop, Azure Microsoft Entra ID, formerly known as Microsoft Active Directory, Azure Advanced Threat Protection, Azure Information Protection, Flow, Intune, Microsoft Cloud App Security, Microsoft Graph, Microsoft Power Apps, Microsoft Stream, Multi-Factor Authentication, Power BI, Power Platform Admin Center, and can offer other USPTO approved Azure services as needed.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system
UMACS provides an Infrastructure as a Service (IaaS), PaaS, and SaaS for its consumers

(b) System location
North Central US, Central US, and East US 2

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

UMACS hosts PaaS Tenants and maintains direct network connection and inheritance relationships with the following USPTO systems:

- **Microsoft Azure Cloud Services (Azure):** 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 (IAM), and Azure Managed Disks. These services are explained in greater detail below and further in the Azure East/West IaaS System Security Privacy Plan (SSPP).

- **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 SSPP.

- **UACS-USPTO AWS Cloud Services (UACS):** UACS General Support System (GSS) is an infrastructure platform, infrastructure as a service, used to support USPTO Product Team Components, hosted in the AWS East/West environment. The AWS East/West environment is comprised of several sub-components including, Virtual Private Cloud (VPC), Elastic Cloud Computing (EC2), Identity and Authentication Management (IAM), Simple Storage Service and other Fed Ramp approved services These services are explained in greater detail below and further in the UACS System Description, UACS SSPP, and/or the AWS East/West IaaS SSPP.

- **DS-ACS-Admin Credential System:** The mission of the DS-ACS is to provide an enterprise Admin Credential System services to all applications for Approved Information Systems (AIS's). As part of the enterprise services, it will also provide compliance for some of the National Institute of Science and Technology (NIST) 800-53 controls

- **ICAM Identity as a Service (ICAM-IDaaS):** The mission of the ICAM-IDaaS is to provide an enterprise authentication and authorization service to all applications/AIS's. As part of the enterprise services, it will also provide compliance for some of the NIST 800-53 controls (e.g. Access Control (AC), Audit and Accountability (AU)). The system provides following services to the enterprise: User Provisioning and Life Cycle Management, User Roles and Entitlement Management, User Authentication & Authorization to protected resources, application Integration/Protection, NIST controls compliance related to AU, AC, and Identification and Authentication (IA) family

- **Identity Management Authenticator (ID-AUTH):** Provides for Personal Identity Verification (PIV) Card users network authentication. All USPTO users must use PIV card and/or equivalent multi-factor authentication. Privileged users access the USPTO network through authentication to the USPTO domain with the use of PIV Card + PIN, and the permissions to the application are role based and granted to the certificate on the user's PIV card. Authentication is performed using the PIV card. PIV Card and PIN are used for authentication to privilege accounts. These information systems inherit

identification and authentication system remote access controls from Microsoft Entra ID accounts supplied by ESS. In order to gain access to privileged accounts, the administrator must have an AD username and an active Okta Verify token. This provides multi-factor authentication for the system.

- **Enterprise Software Services (ESS):** ESS system provides an architecture capable of supporting current software services as well as providing the necessary architecture to support growth. ESS - EDS to serve the USPTO enterprise with use of System Center Configuration Manager (SCCM) drive accounts management issues with the Service Desk/Accounts Management team. The Accounts Management team reviews the report and creates ITSM tickets to manage accounts and equipment.

- **National Oceanic and Atmospheric Administration (NOAA):** The NOAA network backbone provides an architecture capable of physical lines to support connection to external network and WAN infrastructure from boundaries internal to USPTO including NSI and SASE.

- **Network and Security Infrastructure System (NSI):** The NSI system provides an architecture capable of supporting network and security infrastructure and services to USPTO systems, including routing, firewalls, and participation in the USPTO Security Monitoring stack with Security and Compliance Services (SCS).

- **Secure Access Service Edge (SASE):** The USPTO users of Netskope use their PIV credentials to authenticate to the web administration console interface through strict enforcement of Multi Factor Authentication (MFA) on the system. The SASE system utilizes Security Assertion Markup Language (SAML) to prove SSO/PIV card authentication is enforced.

- **CrowdStrike (SCS-SaaS):** CrowdStrike provides Host Based Intrusion Detection and Anti-Malware Services to the USPTO Agency. Allowing inheritance for these services.

- **Security and Compliance Services (SCS):** SCS provides Security Incident and Event Management, Enterprise Forensic, Enterprise Management System, Security & Defense, Enterprise Scanner, Enterprise Cybersecurity Monitoring Operations, Performance Monitoring Tools, Dynamic Operational Support Plan, & Situational Awareness and Incident Response.

- **Cyber Infrastructure and Security Agency (CISA's Talon):** Nicknamed Cloud Log Aggregation Warehouse (CLAW)**,** Talon provides across agency centralized logging and Security Incident and Event Management, Enterprise Forensic, Enterprise Management System, Security & Defense, Enterprise Scanner, Enterprise Cybersecurity Monitoring Operations, Performance Monitoring Tools, Dynamic Operational Support Plan, & Situational Awareness and Incident Response, from a cross-government perspective.

UMACS also indirectly connects with some external systems, via agency connections through USPTO NSI and/or USPTO SASE. USPTO NSI and/or SASE systems connect to

external systems such as National Oceanic and Atmospheric Administration (NOAA N-Wave), Microsoft Azure, a Cloud Services Provider (CSP), Amazon Web Services (CSP), and Cyber Infrastructure and Security Agency's Talon (also referred to as CISA Talon). These external connections are documented and described in the associated interagency agreements.

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

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 UMACS platform, Services, and their support team will address essential services such as user and account administration, access control, networking infrastructure, logging monitoring, security monitoring and alerts, standardized server images, and the support of those components.

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

Azure Microsoft Entra ID, formerly known as Azure Microsoft Entra ID, grants access to the UMACS platform. UMACS is also integrated with ICAM-IDaaS for portal and web application access.

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

USPTO accesses information in UMACS via secure web and network protocols (Hypertext Transfer Protocol Secure (HTTPS), Transport Layer security (TLS) 1.2+).

(g) Any information sharing
UMACS offloads/forwards native security agent data, and associated logs, to USPTO Security and Compliance Services Security Information and Event Management (SIEM), and in FY23 began forwarding security event logs, which includes Microsoft Entra ID sign-in logs, to Cybersecurity and Infrastructure Security Agency (CISA) as part of Trusted Internet Connections (TIC) 3.0 (TALON).

Logs are sent from USPTO SIEM to CISA Cloud Log Aggregation Warehouse (CLAW)/Talon. The logs sent from USPTO SIEM are buffered in an Azure Event Hub hosted by USPTO. The Event Hub is considered part of the CLAW/Talon system. USPTO owns and controls the Event Hub, CISA owns and controls elements after messages leave the Event Hub.

Logs are pulled from the Event Hub by CISA on a schedule controlled by CISA. Logs are buffered for 7 days prior to automatic deletion from the Event Hub. Logs are transmitted over

Hypertext Transfer Protocol Secure (HTTPS) (443) for data security. The Event hub is monitored for inbound and outbound data flow. Only logs destined for CISA are sent the Event Hub for ingestion by CISA.

(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; the Electronic Signatures in Global and National Commerce Act, Pub. L. 106-229; Federal Information Security Management Act (Pub. L. 107-296, Sec. 3544); E-Government Act (Pub. L. 107-347, Sec. 203); Homeland Security Presidential Directive 12 (HSPD-12) "Policy for a Common Identification Standard for Federal Employees and Contractors" (August 27, 2004).

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

Moderate

Section 1: Status of the Information System

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

☐ This is a new information system.

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

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	☐	d. Significant Merging	☐	g. New Interagency Uses	☐
b. Anonymous to Non-Anonymous	☐	e. New Public Access	☐	h. Internal Flow or Collection	☐
c. Significant System Management Changes	☐	f. Commercial Sources	☐	i. Alteration in Character of Data	☐
j. Other changes that create new privacy risks (specify):					

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

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

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	☐	f. Driver's License	☐	j. Financial Account	☐
b. Taxpayer ID	☐	g. Passport	☐	k. Financial Transaction	☐
c. Employer ID	☐	h. Alien Registration	☐	l. Vehicle Identifier	☐
d. Employee ID	☒	i. Credit Card	☐	m. Medical Record	☐
e. File/Case ID	☐				
n. Other identifying numbers (specify):					
*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): Company affiliation					

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					
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.

Personally Identifiable Information (PII)in UMACS (Azure Microsoft Entra ID, formerly known as Azure Microsoft Entra ID. Microsoft Entra ID is secured using appropriate administrative, physical and technical safeguards in accordance with the applicable federal Executive Orders, directives, policies, and standards. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The USPTO/UMACS maintains an audit trail and performs random periodic reviews to identify unauthorized access and changes as part of verifying the integrity of data. The information in Microsoft Entra ID is a copy of information from on-prem AD. If the user uses the web version of a Microsoft product, they would be able to view their PII. They can create a service ticket to fix any inaccurate information identified.

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).

The PII is collected primarily on-premise Microsoft Entra ID for use within the Enterprise Directory Services (EDS) system to identify the users and partners when authenticating through the USPTO network. Microsoft Entra ID is synchronized with UMACS Microsoft Entra ID. User credentials are managed through Microsoft Entra ID which is a part of EDS and will integrate with ICAM-IDaaS. This will allow users to access USPTO's network and various systems through Single Sign-On within the UMACS Platform.

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.)

UMACS implements security and management controls to prevent the inappropriate disclosure of sensitive information. Automated mechanisms are in place to ensure the security of all data collected. Security controls are employed to ensure information is resistant to tampering (Physical and Access Controls), the confidentiality of data in transit (Encryption), and that data is available for authorized users only (Access Control). Management controls are utilized to prevent the inappropriate disclosure of sensitive information. In addition, the Perimeter Network (NSI) and SASE provide additional automated transmission and monitoring mechanisms to ensure that PII is protected and not breached by any outside entities. In the event of disposal, USPTO uses degaussing to permanently remove data according to government mandate and security policy. Other systems may connect with the Microsoft Entra ID to authenticate user and access user traits as part of the access decisions making and/or processing application workflow. Information is protected through a layered security approach which incorporates the use of secure authentication, access control, mandatory configuration settings, firewalls, Virtual Private Network (VPN), and encryption, where required. Internally within USPTO, data transmission confidentiality controls are provided by PTOnet.

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: • Microsoft Azure Cloud Services • USPTO AWS Cloud Services (UACS) • USPTO Google Cloud Services (UGCS) • DS-ACS-Admin Credential System • ICAM Identity as a Service (ICAM-IDaaS) • Identity Management Authenticator (ID-AUTH) • Enterprise Software Services (ESS) • Network and Security Infrastructure System (NSI) • Secure Access Service Edge (SASE) • CrowdStrike (SCS-SaaS) • Security and Compliance Services (SCS) • Cyber Infrastructure and Security Agency (CISA's Talon) UMACS Product Team does have visibility into sensitive BII/PII in other FISMAs. This above is simply a list of UMACS interconnections. NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation. Other systems may connect with the Microsoft Entra ID to authenticate user and access user traits as part of the access decisions making and/or processing application workflow. Information is protected through a layered security approach which incorporates the use of secure authentication, access control, mandatory configuration settings, firewalls, Virtual Private Network (VPN), and encryption, where required. Internally within USPTO, data transmission confidentiality controls are provided by PTOnet.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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

Class of Users			
General Public	☐	Government Employees	☒
Contractors	☒		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

☒	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
☒	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.uspto.gov/privacy-policy	
☒	Yes, notice is provided by other means.	Specify how: this PIA serves as notice
☐	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

☐	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: PII collection is part of the registration process, account creation and tracking internal user's work location. The information is synchronized with EDS system via automated process.

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 PII within the system is necessary for the authentication of individuals. Individuals do not have the opportunity to consent to particular uses of their PII/BII.

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: Individuals are not able to update their information on UMACS directly. For an individual to update their information the individual can submit a request via USPTO ticketing system (ServiceNow).

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: Access to PII is restricted to internal personnel only. Azure AD has monitoring and auditing enabled with various native Microsoft tools (Data Loss Prevention (DLP), Information Protection Labels, Defender, Purview, and Sentinel).
☒	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): 12/8/2025 ☐ 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): FIPS 140-2 encryption is applied

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The information system provides protection of resources in accordance with NIST 800-18 Rev. 1 and NIST 800-53 Rev. 5; the UMACS System Security Plan (SSP) addresses the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment. The SSP is reviewed on an annual basis. In addition, annual assessments and Continuous Monitoring reviews are conducted on the UMACS services and data. The USPTO Cybersecurity Division (CD) conducts these assessments and reviews based on NIST SP 800-53 Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations and NIST SP 800-53 Revision 5 Assessing Security and Privacy Controls in Federal Information. Systems and Organizations. The results of these assessments and reviews are documented in the UMACS Security Assessment Package as part of the system's Security Authorization process.

Management Controls
1. USPTO uses the Life Cycle review process to ensure that management controls are in place for UMACS. During the enhancement of any component, the security controls are reviewed, reevaluated, and updated in the System Security Plan. The System Security Plan specifically addresses the management, operational, and technical controls that are in place, and planned, during the operation of the enhanced system. Additional management controls include performing national agency checks on all personnel, including contractor staff. Additionally, USPTO develops privacy and PII-related policies and procedures to ensure safe handling, storing, and processing of sensitive data.

Operational Controls
1. Automated operational controls include securing all resources associated with the UMACS in the operational boundary. The UMACS tenant access is controls through Multifactor Authentication (MFA). All access and management are audited by the system.

Technical Controls
1. UMACS is secured by various USPTO infrastructure components, including the Network and Security Infrastructure (NSI) system and other OCIO established technical controls to include password authentication at the server and database levels. Web communications leverages modern encryption technology such as TLS 1.2 over HTTPS or HTTP Strict Transport Security (HSTS). Dedicated interconnections offer protection through Internet Protocol Security (IPSec) VPN tunnels.

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
☐	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 3.1: General Technology Management Records** Item - 020 Information technology operations and maintenance records. Which include access and audit logs. **GRS 3.2. Information Systems Security Records** Item 010, 020, 030, 031, 040 Which include system security logs.
☐	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
☒	Yes, retention is monitored for compliance to the schedule.
☐	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	☐	Overwriting	☒
Degaussing	☒	Deleting	☒
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

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

☒	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
☐	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☐	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

☒	Identifiability	Provide explanation: Name, mailing address, phone number, and email address collected.
☒	Quantity of PII	Provide explanation: The PII quantity per user would be approximately 6 PII data Points and there are approximately 17k users.
☒	Data Field Sensitivity	Provide explanation: The PII sensitivity is low as most of the PII points are publicly available PII.
☒	Context of Use	Provide explanation: Information is for identifying, authenticating and tracking of users. Internal authorized user credentials are managed through the EDS system. Also, the collected information is intended to be used by the USPTO Service Desk for verifying the identity of customers interacting with the system.
☒	Obligation to Protect Confidentiality	Provide explanation: USPTO Privacy Policy requires the PII information collected within the system to be protected in accordance to NIST SP 800- 122, Guide to Protecting the Confidentiality of PII.
☒	Access to and Location of PII	Provide explanation: Access is limited only to the identified and authenticated users and partners. The information collected will not be shared with any other agency. This information is to be used only by the USPTO for the purpose of identity proofing and verification.
☐	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 have identified and evaluated potential threats to PII such as loss of confidentiality and integrity of information. Based upon USPTO's threat assessment the Agency have implemented baseline of security controls to mitigate these risks to sensitive information to an acceptable level.

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.