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

Privacy Impact Assessment
for the
CredPriv ICAM-CredMGMT / ICAM-PrivMGMT (CredPriv)

Reviewed by: Henry J. Holcombe, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO CredPriv ICAM-CredMGMT / ICAM-PrivMGMT (CredPriv)

Unique Project Identifier: PTO-EIPL-DS-05-00

Introduction: System Description

Provide a brief description of the information system.

CredPriv ICAM-CredMGMT / ICAM-PrivMGMT (CredPriv) is a major application system. CredPriv consists of SailPoint Lifecycle Management (LCM) also known as ICAM-CredMGMT and CA Privileged Access Manager (PAM) also known as ICAM-PrivMGMT, both components are part of the Continuous Diagnostics and Mitigation (CDM), is a Department of Homeland Security (DHS) sponsored Federal Government-wide Program used to aggregate user account information from Microsoft Active Directory (AD), RedHat Identity Manager (IDM), Central Enterprise Data Repository (CEDR) (HR database), Learning Center (LC) and Probaris, a (Personal Identity Verification) PIV tracking database, and provides reporting to the Department of Commerce (DOC) and National Institute of Standards and Technology (NIST) through the Master User Record (MUR). The system is also used to manage and control access to USPTO assets such as Windows and Linux systems.

Address the following elements:

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

(b) System location
CredPriv is located at 600 Dulany Street, Alexandria VA 22314.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
In addition to connections with Probaris, LC, IDM, Microsoft Active Directory (AD) and CEDR CredPriv interconnects with the following systems:

Enterprise Unix Services (EUS) is an infrastructure operating system with a sole purpose of providing a UNIX base hosting platform to support other systems at USPTO.

ICAM-IDaaS provides an enterprise authentication and authorization service to all applications/AIS's.

Identity Management Authenticator (ID-AUTH) is an end-to-end system tasked with managing the personal identity credentials of USPTO

Patent Capture and Application Processing System – Capture and Initial Processing (PCAPS IP) is a major application and provides support to the USPTO 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

Commerce Learning Center (CLC) is an enterprise-wide system used to manage professional development, help to plan training, and provide access to online learning.

(d) The way the system operates to achieve the purpose(s) identified in Section 4
CredPriv aggregates user account information from AD, IDM, CEDR, HR, LC, and Probaris to provide reporting to DOC and NIST through the MUR. The system also manages access to USPTO assets, Windows and Linux systems Information flows from the privileged users' account via the AD/IDM onto the Privileged Access Manager (PAM) system, onto the SailPoint system and finally into the DOC/NIST SailPoint dashboard via MUR reporting.

(e) How information in the system is retrieved by the user
CAPAM provides PIV two-factor authentication in order to access any system where admin privilege is required.

(f) How information is transmitted to and from the system
Users access Sailpoint via a web interface and via TLS 1.2 or higher to encrypt the data in transit. Sailpoint ingests a flat file from LC and uses TLS 1.2 or higher to encrypt the data in transit.

(g) Any information sharing
The information within CredPriv is shared via bulk transfer within the bureau and with DOC and NIST.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
The authority is M-19-02, Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements.

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

There is constant communications with the System of Record (SOR), CEDR, and their support team to ensure CredPriv data matches CEDR data (master data). Automated synchronization is in place for both AD and SailPoint which are downstream of the SOR. The accounts management team is constantly verifying AD content and coordinating questions with the CEDR team and the SailPoint team. The accounts management team has access to SailPoint to help them automate account management.

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. Mandatory IT Awareness and role-based training is required for staff who have access to the system and addresses how to handle, retain, and dispose 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):			

☒	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).

CredPriv collects PII about USPTO employees and contractors for administrative purposes and to promote information sharing initiative. CDM is required by DHS to ensure least privilege access is enforced for all USPTO resources. The PII collected such as user name, office location, work email address and office phone are to ensure efficient internal communications and support the ability to apply roles and restrict access to resources.

5.2   Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

In the event of computer failure, insider threats, or attack against the system by adversarial or foreign entities, any PII data stored within CredPriv could be exposed. In an effort to avoid a breach, CredPriv has put certain security controls 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. These audit trails are reviewed by the Information System Security Officer and System Auditor and any suspicious indicators will be immediately investigated and appropriate action taken.

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: • ICAM • ID-AUTH • PCAPS-IP • Commerce Learning Center (CLC) CredPriv has put certain security controls 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. The following are current USPTO policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy (OCIO- POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), USPTO Rules of the Road (OCIO-POL- 36). All offices of 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.
☐	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: Appendix A: Warning Banner
☐	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: Information is required for daily operations and users to not have an opportunity to decline to provide PII.

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: Day-to-day operations and federal mandates require the use of the data and users do not have an opportunity to consent to the particular use.

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: Yes, users have an opportunity to review/update PII pertaining to them. Users review source systems (CEDR/LC/HRconnect/AD) via email or phone request. Users can see their data in the source systems and limited view is available in SailPoint.
☐	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that*

apply.)

☒	All users signed a confidentiality agreement or non-disclosure agreement.
☒	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Audit logs.
☒	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): _____ ☒ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☐	Contracts with customers establish DOC ownership rights over data including PII/BII.
☒	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

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

PII within CREDPRIV is secured using appropriate management, operational, and technical safeguards in accordance with NIST requirements. Such management controls include the Life Cycle 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 CREDPRIV 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. CREDPRIV maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity.

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)*: **COMMERCE/PAT-TM-17**: USPTO Security Access Control and Certificate Systems **COMMERCE/DEPT-25**: Access Control and Identity Management System **COMMERCE/PAT-TM-18**: USPTO Personal Identification Verification (PIV) and Security Access Control 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: GRS 3.2, items 030, 031, 060, 061, 062 GRS 5.1 item 020 GRS 5.2 item 020
☐	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: General data fields such as user ID, first name, middle name, and last name alone or in combination could uniquely identify an individual.
☒	Quantity of PII	Provide explanation: Quantity of PII is minimal and pertains to 15,000 accounts and 17,000 records in total.
☒	Data Field Sensitivity	Provide explanation: General data fields such as user ID, first name, middle name, and last name have little relevance outside the context of use.
☒	Context of Use	Provide explanation: CREDPRIV allows DOC to have centralized user records to ensure uniqueness and lack of duplication. CDM is required by DHS to ensure least privilege access is enforced for all USPTO resources. The PII collected such as user name, office location, and office phone are to ensure efficient internal communications and support the ability to apply roles and restrict access to resources
☒	Obligation to Protect Confidentiality	Provide explanation: 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) and the Privacy Act of 1974.
☒	Access to and Location of PII	Provide explanation: CREDPRIV is an on-premise system, mostly receiving information from other on-premise (Alexandria, VA) systems. The PII captured, stored, and, transmitted by the CredPriv system is accessible by internal USPTO employees and contractors and DOC with access permissions.
☐	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.)

System users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers are restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zone within the USPTO internal network and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved an authorized account. 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.

Appendix A: Warning Banner

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

You have accessed a United States Government computer system. Unauthorized access or actions exceeding authorized access is a violation of Public Law 99-474; 18 U.S.C. 1030 and may result in criminal, civil or administrative penalties. Authorized use of this system is limited to work needed to perform official US Patent and Trademark Office (USPTO) business. While using this system, users must comply with USPTO policy as documented in the USPTO AAO 212-4, Information Technology Security. Unauthorized use, or modification or disclosure of the data contained herein or in transit to/from this system constitutes a violation of Public Law 99-474; 18 U.S.C. 1030 and state criminal and civil laws. Users of this system may be monitored in order to ensure its continued operational effectiveness and integrity. Users of this system are reminded that such monitoring does occur and that use of this system constitutes consent to such monitoring. Unauthorized use or actions exceeding authorized use of USPTO systems will be investigated and, when appropriate, official sanctions will be imposed. If criminal activity is discovered, systems information will be provided to the appropriate law enforcement officials for investigation and prosecution. Report access violations or policy infractions to the Service Desk at (571) 272-9000.

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

Please Login

Username [   ] Password [   ]

[Log in]

⚠ WARNING: After successful login and your work is complete, be sure to use the 'LOGOUT' button (upper right) before closing the browser.
If you repeatedly close your browser without logging out, you will eventually exceed your max number of sessions and will be blocked from logging in.

USPTO Points of Contact and Signatures

<table>
<tr>
<td>

System Owner
Name: Jimmy Orona, III
Office: Enterprise Software Services Division
Phone: (571) 272-0673
Email: Jimmy.Orona@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: Users, Orona, Jimmy III
Digitally signed by Users, Orona, Jimmy III
Date: 2022.01.26 09:37:57 -05'00'

Date signed: _____

</td>
<td>

Chief Information Security Officer
Name: Don Watson
Office: Office of the Chief Information Officer (OCIO)
Phone: (571) 272-8130
Email: Don.Watson@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: Users, Watson, Don
Digitally signed by Users, Watson, Don
Date: 2022.01.26 14:23:47 -05'00'

Date signed: _____

</td>
</tr>
<tr>
<td>

Privacy Act Officer
Name: Ezequiel Berdichevsky
Office: Office of General Law (O/GL)
Phone: (571) 270-1557
Email: Ezequiel.Berdichevsky@uspto.gov

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

Signature: Users, Berdichevsky, Ezequiel
Digitally signed by Users, Berdichevsky, Ezequiel
Date: 2022.01.26 09:01:44 -05'00'

Date signed: _____

</td>
<td>

Bureau Chief Privacy Officer and Authorizing Official

Name: Henry J. Holcombe
Office: Office of the Chief Information Officer (OCIO)
Phone: (571) 272-9400
Email: Jamie.Holcombe@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: Users, Holcombe, Henry
Digitally signed by Users, Holcombe, Henry
Date: 2022.01.26 14:38:11 -05'00'

Date signed: _____

</td>
</tr>
<tr>
<td>

Co-Authorizing Official
Name: N/A
Office: N/A
Phone: N/A
Email: N/A

I certify that this PIA accurately reflects the representations made to me herein by the System Owner, the Chief Information Security Officer, and the Chief Privacy Officer regarding security controls in place to protect PII/BII in this PIA.

Signature: _____

Date signed: _____

</td>
<td>
</td>
</tr>
</table>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page <u>must</u> be removed prior to publication of the PIA.