Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
CredPriv ICAM-CredMGMT / ICAM-PrivMGMT (CredPriv)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO CredPriv ICAM-CredMGMT / ICAM-PrivMGMT (CredPriv)

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

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system: *Provide a brief description of the information system.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

CredPriv ICAM-CredMGMT / ICAM-PrivMGMT (CredPriv) is a major application system. CredPriv consists of SailPoint Lifecycle Management (LCM) also known as ICAMCredMGMT and CA Privileged Access Manager (PAM) also known as ICAM-PrivMGMT, both components are part of the Continuous Diagnostics and Mitigation (CDM) program which 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 in Virginia, USA.

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.

PE2E's subsystem Central Enterprise Data Repository (CEDR-INFRA) - 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.

ESS's subsystem Enterprise Directory Services (EDS) - provides the USPTO organization with a collection of programs that utilize common business applications and tools for modeling how the entire organization works.

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 purpose that the system is designed to serve

USPTO uses ICAM-CredMGMT and ICAM-PrivMGMT, both components of CDM, to manage USPTO user privileged access to devices and credential workflow. USPTO also uses ICAMPrivMGMT and ICAM-CredMGMT components to incorporate and correlate unprivileged and privileged user account data into the MUR for reporting to a centralized SailPoint IIQ at NIST and DOC.

e) *The way the system operates to achieve the purpose*

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.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

CredPriv holds user account information related to USPTO employees and contractors including user ID, office, and telephone information. It includes a simple annotation stating whether they are privileged users or regular users based on information transmitted via

Active Directory or RedHat Identity Manager. It also retrieves information on the completion of the user's annual security training and if the individual has passed a background investigation for the PIV card allocation.

g) Identify individuals who have access to information on the system

Access to CredPriv is limited to USPTO employees and contractors.

h) How information in the system is retrieved by the user

Computer Associates Privileged Access Manager (CAPAM) provides PIV two-factor authentication to access any system where admin privilege is required.

i) How information is transmitted to and from the system

Users access Sailpoint via a web interface 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.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

☐ This is a new information system. *Continue to answer questions and complete certification.*

☐ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*

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

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

☐ Yes. This is a new information system.

☐ Yes. This is an existing information system for which an amended contract is needed.

☐ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

☒ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

☐ Yes. *(Check all that apply.)*

Activities			
Audio recordings	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify):			

☒ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☐ Yes, the IT system collects, maintains, or disseminates BII.

☒ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when

combined with other information that is linked or linkable to a specific individual."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- ☒ DOC employees
- ☒ Contractors working on behalf of DOC
- ☐ Other Federal Government personnel
- ☐ Members of the public

☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

☐ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

☒ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

☐ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☒ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ The criteria implied by one or more of the questions above **apply** to the CredPriv ICAM-CredMGMT / ICAM-PrivMGMT (CredPriv) and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

☐ The criteria implied by the questions above **do not apply** to the CredPriv ICAM-CredMGMT / ICAM-PrivMGMT (CredPriv) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Jimmy Orona, III Office: Enterprise Software Services Division Phone: (571) 272-0673 Email: Jimmy.Orona@uspto.gov Signature: Users, Orona, Jimmy III Digitally signed by Users, Orona, Jimmy III Date: 2023.03.14 08:13:08 -04'00' Date signed: _____	**Chief Information Security Officer** Name: Don Watson Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-8130 Email: Don.Watson@uspto.gov Signature: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2023.03.15 20:06:16 -04'00' Date signed: _____
Privacy Act Officer Name: Ezequiel Berdichevsky Office: Office of General Law (O/GL) Phone: (571) 270-1557 Email: Ezequiel.Berdichevsky@uspto.gov Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2023.03.14 09:17:00 -04'00' Date signed: _____	**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 Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2023.03.16 16:11:18 -04'00' Date signed: _____
Co-Authorizing Official Name: N/A Office: N/A Phone: N/A Email: N/A Signature: _____ Date signed: _____	