Template Version Number: 01-2020

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

Privacy Threshold Analysis
for the
Identity Management Authenticator (ID-AUTH)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Identity Management Authenticator (ID-AUTH)

Unique Project Identifier: EIPL-DS-09-00

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 and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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).

Identity Management Authenticator (ID-AUTH) is an end-to-end system tasked with managing the personal identity credentials of USPTO employees and contractors. ID-AUTH will support the personalization and issuance of Smart Card identification credentials under Homeland Security Presidential Directive 12 (HSPD-12). The HSPD-12 credential (photo ID badge) and the issuance process applies to all USPTO employees and contractors. The ID-AUTH system manages the personal identity credentials (photo ID badge) of all USPTO employees and contractors seeking physical access to USPTO facilities and logical access to USPTO information systems. The ID-AUTH integrates both the physical and logical access controls. ID-AUTH consists of the following two (2) sub-systems:

- **Card Management System (CMS)** provides personalization and issuance of the Smart Card identification credentials under Homeland Security Presidential Directive (HSPD - 12).
- **Internal Public Key Infrastructure-Smart Card (IPKI-SC)** provides the management of internal certificates to USPTO

a) Whether it is a general support system, major application, or other type of system
ID-AUTH is a Major Application.

b) System location

ID-AUTH is located at the USPTO Data Center, 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)***

ID-AUTH solution(s) uses the existing USPTO PKI (Entrust) system. It also connects with the existing USPTO Physical Access Control System (PACS) called C-Cure. Workstations to support Enrollment, Production, and Issuance of ID-AUTH credentials are installed in the Security Services Center. ID-AUTH interconnects with the following systems:

- **Enterprise Windows Services (EWS)** is an Infrastructure information system, and provides a hosting platform for major applications that support various USPTO missions.
- **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.
- **Enterprise Desktop Platform (EDP)** is an infrastructure information system which provides a standard enterprise-wide environment that manages desktops and laptops running on the Windows 7 and Windows 10 operating system (OS), providing United States Government Configuration Baseline (USGCB) compliant workstations.
- **Service Oriented Infrastructure System (SOI)** provides the underlying services which provide a mobile, feature-rich, and stable platform upon which USPTO applications can be deployed.
- **Database Services (DBS ORACLE)** provides a Database infrastructure to support the mission of USPTO Database needs. The DBS System is composed of a collection of various versions of Database systems. The subsystems within the DBS System includes: SQL Database Servers (MSSQL); Oracle (Oracle); and MySQL (MySQL).
- **Data Storage Management System (DSMS)** provides the following services or functions in support of the USPTO mission: Secure environment for archival and storage of data and records vital to USPTO's Business Continuity and Disaster Recovery plan. Each of the Automated Information Systems (AISs) comprising Data Storage Management provides a different set of capabilities.
- **Enterprise Software Services (ESS EDS)** provides an architecture capable supporting current software services.
- **Physical Access Control System (PACS)** is an electronic physical security system, and provides the capability to restrict and/or control physical access to USPTO facilities, equipment and resources. This system is used by authorized security personnel to manage and monitor multiple entry points, intrusion detection, and video surveillance at the USPTO Headquarters in Alexandria, Virginia and satellite offices in: San Jose, California; Denver, Colorado; Dallas Texas; and Detroit, Michigan.
- **Security and Compliance Services (SCS)**, formally EMSO, provides enterprise level monitoring to the USPTO.

d) The purpose that the system is designed to serve

The purpose of the ID-AUTH system is the personalization and issuance of the Smart Card identification credentials under HSPD-12.

e) The way the system operates to achieve the purpose

The ID-AUTH system manages the personal identity credentials (photo ID badge) of all USPTO employees and contractors seeking physical access to USPTO facilities and logical access to USPTO information systems. The ID-AUTH integrates both the physical and logical access controls. The USPTO ID-AUTH solution(s) uses the existing USPTO PKI (Entrust) system. It also connects with the existing USPTO Physical Access Control System (PACS) called C-Cure. Workstations to support Enrollment, Production, and Issuance of ID-AUTH credentials are installed in the Security Services Center.

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

ID-AUTH collects, maintains, or disseminates PII/BII for federal employees and contractors. In accordance with HSPD-12 and FIPS 201-1, personal data such as Social Security Numbers (SSNs), fingerprints, personal information, and facial images are collected and stored for issuing Personal Identity Verification (PIV) cards to federal employees and contractors, and for conducting PIV card lifecycle maintenance functions.

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

USPTO employees and contractors who are authorized users have access to information in the system. Authorized users of the system accounts, or roles, with access to ID-AUTH are managed.

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

Only ID-AUTH role holders have access to the application. ID-AUTH role holders must logon to workstation systems prior to authenticating to the ID-AUTH system. ID-AUTH roles are statically defined. Non-privileged access is for the use of all USPTO PIV card holders to only access the self-portal.

i) How information is transmitted to and from the system

Enrollment within Probaris ID is performed using Probaris Enrollment. This is a client module with biometric capture devices and a workflow based client that is integrated with the core Probaris ID servers to provide fast enrollment throughput, flexibility and security. All data is digitally signed and transmitted back to the solution with no privacy data stored locally to meet the stringent privacy guidelines.

ID AUTH system utilizes workstations, identity management software and various peripheral devices to produce the PIV card. USPTO employees and contractors pertinent data is collected, photos are captured, and fingerprints are gathered to provide verification of identity of each applicant. The data along with work detail information are then loaded to the PIV card producing a credentialed Smart Card. The PIV card is printed and issued to the applicant for efficient identification and security control for both physical and logical access to USPTO facilities and assets.

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 (version 01-2015 or 01-2017). *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 (version 01-2019 or later). *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.

ID-AUTH collects, maintains, or disseminates PII/BII for federal employees and contractors. In accordance with HSPD-12 and FIPS 201-2, personal data such as Social Security Numbers (SSNs), fingerprints, personal information, and facial images are collected and stored for issuing PIV cards to federal employees and contractors, and for conducting PIV card lifecycle maintenance functions.

Provide the legal authority which permits the collection of SSNs, including truncated form.
Homeland Security Presidential Directive 12 (HSPD-12).

☐ 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

☒ I certify the criteria implied by one or more of the questions above **apply** to the **Identity Management Authenticator (ID-AUTH)** and as a consequence of this applicability, I will perform and document a PIA for this IT system.

☐ I certify the criteria implied by the questions above **do not apply** to the **Identity Management Authenticator (ID-AUTH)** and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Jimmy Orona, III Office: Software Services Branch 2 (I/SSB2) Phone: (571) 272-0673 Email: Jimmy.Orona@uspto.gov Signature: Users, Orona, Jimmy III Digitally signed by Users, Orona, Jimmy III Date: 2021.12.07 07:34:40 -05'00' 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: DON R Watson Digitally signed by DON R Watson Date: 2021.12.07 17:13:56 -05'00' Date signed: ______________________________
Privacy Act Officer Name: Ezequiel Berdichevsky Office: Office of General Law (G/GLO) Phone: (571) 270-1557 Email: Ezequiel.Berdichevsky@uspto.gov Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2021.12.02 13:45:35 -05'00' 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: 2021.12.09 11:53:05 -05'00' Date signed: ______________________________
Co-Authorizing Official Name: N/A Office: N/A Phone: N/A Email: N/A Signature: ______________________________ Date signed: ______________________________	

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