Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Identity Management Authenticator (ID-AUTH)

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

Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry
Date: 2023.11.27 16:49:50 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Identity Management Authenticator (ID-AUTH)

Unique Project Identifier: EIPL-DS-09-00

Introduction: System Description

Provide a brief description of the information system.

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 consists of four sub-components: CMS, IPKI, RSA, and MIDM. ID-AUTH system supports the personalization and issuance of Smart Card identification credentials under 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 four sub-components:

- **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.
- **RSA** provides the issuance and management of the RSA Token.
- **MIDM** provides the automated function to manage certificates per application.

Address the following elements:

(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 in Alexandria, VA.

(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 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. No PII.
- **Enterprise Windows Services (EWS)** is an Infrastructure information system, and provides a hosting platform for major applications that support various USPTO missions. No PII.
- **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. Contains PII.
- **Security and Compliance Services (SCS)**, formally EMSO, provides enterprise level monitoring to the USPTO. Contains PII.
- **Enterprise Software Services (ESS EDS)** provides an architecture capable supporting current software service. Contains PII.
- **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. Contains PII.

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

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.

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

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

(f) 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.

(g) Any information sharing

ID-AUTH integrates with both the physical and logical access control systems to ensure the USPTO facilities and information systems are accessed by authorized personnel. Therefore, PII about employees and contractors will be directly accessible and shared within the bureau. PII about employees and contractors will be shared on a case-by-case basis with other federal agencies and the private sector.

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

Homeland Security Presidential Directive 12 (HSPD-12).

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

ID-AUTH 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: ID-AUTH collects, maintains, or disseminates PII/BII for federal employees and contractors. In accordance with HSPD-12 and FIPS 201-3, 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.					

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.

A trusted role holder verifies the information by inspecting the IDs presented by the card applicant. In addition, USPTO implements security and management controls to prevent the inappropriate disclosure of sensitive information. Security controls are employed to ensure information is resistant to tampering, remains confidential as necessary, and is available as intended by the agency and as expected by authorized users. Management controls are utilized to prevent the inappropriate disclosure of sensitive information. In addition, Network and Security Infrastructure System (NSI) provides additional automated transmission and monitoring mechanisms to ensure that PII/BII information is protected and not breached by external entities. Information is collected from the users directly and collected data is used for decision making only.

Any biometric information that is collected from the PIV solution will be immediately and securely stored on Probaris servers (which are located in the USPTO secure data center) once the PIV cards are manufactured and provided to the card applicants. The USPTO PIV system will not store biometric information that pertains to card applicants for any period of time longer than is required to manufacture and maintain the PIV card in order to minimize security exposure that is associated with storing privacy data and the Agency's System of Record. Further, any biometric information that is stored on the PIV card is controlled and safeguarded by the actual smart card device and the security boundaries that are associated with those tokens. The risk assessments and technical solution provided by these PIV card products has been fully assessed and or tested by NIST and GSA and they have been approved by those agencies as acceptable for federal government use.

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): Biometrics may be considered in 2022.			

☐	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).

ID-AUTH 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. To promote administrative matters, during enrollment, two key identity and vetting processes are performed: 1) establishing the applicant's identity, and 2) capturing and validating the applicant's identity data. During this identity proofing process, the applicant is required to appear in person and provide two forms of identification: State or Federal government issued photo ID and one other document from the list of document on Form I-9, OMB No. 1115-0136, and Employment Eligibility Verification. In addition, the photograph and fingerprints of the applicant are captured during enrollment and placed on the credentials for electronic identity validation when the credentials are presented for access to secure areas.

As it relates to intelligence activities, background investigations can include checking the national terrorist watch lists and checks against the Federal Bureau of Investigations (FBI) fingerprint database (AFIS/IAFIS). There are two methods to process the investigations: Automated investigations using the fingerprints and biographic information gathered during enrollment and manual processing using investigations currently on file with the sponsoring organization. The USPTO may decide to use one or both of these methods to issue medium assurance credentials. USPTO collects, secures, and manages the information and lifecycle events to meet secure credentialing requirements. There are five primary lifecycle events: issue, terminate, reissue, suspend, and resume.

The lifecycle associated with secure credentials includes management activities, which are ongoing after a credential has been issued to a cardholder. Credentials can be lost, cardholders may go on extended leave of absences, or cardholders may no longer be affiliated with the sponsoring organization.

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.)

USPTO has identified and evaluated potential threats to PII/BII such as insider threats and adversarial entities which may cause a loss of confidentiality, accessibility, and integrity of information. In the event of computer failure or attack against the system, records of USPTO employees or contractors containing PII could be exposed.

Controls that the bureau/operating unit have put into place to ensure that the information is handled, retained, and disposed appropriately include training, access restriction, password protection, and data retention policies. USPTO has Security Information and Event Management (SIEM) systems that monitor in real-time all the activities and events within the servers storing PII and USPTO C3 personnel review audit logs received on a regular basis and alert the ISSO and/or the appropriate personnel when unusual activity is identified.

The database servers storing the potential PII are segregated in a highly sensitive zone within the USPTO internal network, an additional dedicated network firewall/intrusion prevention system (IPS), and a dedicated network switch through Access control List that limits access restricted to only a few approved and authorized accounts protect the highly sensitive zone.

Stringent physical access controls are in place to restrict access to the datacenter and to the rack with the servers

hosting the database to only a few authorized individuals. The building has security guards and secured doors. All entrances are monitored through electronic surveillance equipment. The hosting facility is supported by 24/7 onsite hosting and network monitoring by trained technical staff. Physical security controls include indoor and outdoor security monitoring and surveillance; badge and picture ID access screening; and pin code access screening. ID-AUTH system utilizes workstations located at Security Service Center (SSC), the identity management software and various peripheral devices for the collection of PII. The USPTO monitors in real-time all activities and events within the servers storing the potential PII data and a subset of USPTO C3 personnel review audit logs received on a regular bases and alert the ISSO and or the appropriate personnel when inappropriate or unusual activity is identified. Access is restricted on a "need to know" basis, and there is utilization of Active Directory security groups to segregate users in accordance with their functions.

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: ID-AUTH interconnects with: • Data Storage Management System (DSMS) • Enterprise Software Services (ESS EDS) • Physical Access Control System (PACS) • Security and Compliance Services (SCS) The database servers storing the potential PII are segregated in a highly sensitive zone within the USPTO internal network, an additional dedicated network firewall/intrusion prevention system (IPS), and a dedicated network switch through Access control List that limits access restricted to only a few approved and authorized accounts protect the highly sensitive zone. Stringent physical access controls are in place to restrict access to the datacenter and to the rack with the servers hosting the database to only a few authorized individuals. The building has security guards and secured doors. All entrances are monitored through electronic surveillance equipment. The hosting facility is supported by 24/7 onsite hosting and network monitoring by trained technical staff. Physical security controls include indoor and outdoor security monitoring and surveillance; badge and picture ID access screening; and pin code access screening. ID-AUTH system utilizes workstations located at Security Service Center (SSC), the identity management software and various peripheral devices for the collection of PII. The USPTO monitors in real-time all activities and events within the servers storing the potential PII data and a subset of USPTO C3 personnel review audit logs received on a regular bases and alert the ISSO and or the appropriate personnel when inappropriate or unusual activity is identified. Access is restricted on a "need to know" basis, and there is utilization of Active Directory security groups to segregate users in accordance with their functions.
☐	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: See Appendix A: Privacy Act Notice.	
☒	Yes, notice is provided by other means.	Specify how: The PIV Card Issuance Privacy Notice is posted in the USPTO Security Services Center where cards will be issued and is also posted on the USPTO Intranet. Additionally, each card applicant is provided a copy of this PIV Card Issuance Privacy Notice at the time of their enrollment. The applicant, at the time of enrollment, is also verbally informed of the purpose of the collected data and has the ability to obtain a privacy notice sheet. They are notified how the collected data will be used to create a PIV card, legal authority for doing so, and other uses of the collected data. In addition, the applicant signature page will identify they have read the privacy implications of the collected personal data, and understand the implications and purpose of the data.
☐	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: Individuals have the opportunity to decline to provide PII when a PIV card is not required for their placement or employment. Information is provided on a voluntary basis.
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Individuals do not have the opportunity to decline to provide PII. Failure to provide the requested information may affect their placement or employment and will affect their ability to obtain a permanent PIV card. If using a PIV credential is a condition of their job, not providing the information will affect their placement or employment prospects.

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 information requested is required for the purpose of ID-AUTH. Failure to provide the requested information may affect their placement or employment and will affect their ability to obtain a permanent PIV card. If using a PIV credential is a condition of their job, not providing the information will affect their placement or employment prospects.

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	Specify how: Individuals have the opportunity to review/update PII/BII through the electronic web-based portal of the ID-AUTH

	PII/BII pertaining to them.	system, http://ptoweb.uspto.gov/ptointranet/ptosecurity/hspd/hspd_name.htm. See Appendix B
☐	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): 1/11/2023 ☐ 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).*

USPTO uses the following system controls to protect PII/BII on the ID-AUTH system.
Management Controls:

a) The USPTO uses the Life Cycle review process to ensure that management controls are in place for ID-AUTH. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the Security Plan. The Security Plans specifically address 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.

b) The USPTO uses the Personally Identifiable Data Extracts Policy. This means no extracts of sensitive data may be copied on to portable media without a waiver approved by the DOC CIO.

Operational Controls:

a) Access to all PII/BII data is for users on PTONet who have verified access to ID-AUTH. Additionally, access to PII/BII data is restricted to a small subset of ID-AUTH users.

b) Manual procedures are followed for handling extracted data containing sensitive PII which is physically transported outside of the USPTO premises. In order to remove data extracts containing sensitive PII from USPTO premises, users must:

1. Maintain a centralized office log for extracted datasets that contain sensitive PII. This log must include the date the data was extracted and removed from the facilities, a description of the data extracted, the purpose of the extract, the expected date of disposal or return, and the actual date of return or deletion.
2. Ensure that any extract which is no longer needed is returned to USPTO premises or securely erased and that this activity is recorded on the log.
3. Obtain management concurrence in the log, if an extract aged over 90 days is still required.
4. Store all PII data extracts maintained on a USPTO laptop in the encrypted My Documents directory. This includes any sensitive PII data extracts downloaded via the USPTO Virtual Private network (VPN).
5. Encrypt and password-protect all sensitive PII data extracts maintained on a portable storage device (such as CD, memory key, flash drive, etc.). Exceptions due to technical limitations must have the approval of the Office Director and alternative protective measures must be in place prior to removal from USPTO premises.

USPTO is using the following compensating controls to protect PII data:

a) No extracts of sensitive data may be copied on to portable media without a waiver approved by the DOC CIO. The request for a waiver must include specifics as to how the data and device are protected, how long the data will be maintained, and how the data on the device will be deleted when no longer required.

b) All laptop computers allowed to store sensitive data must have full disk encryption.

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)*: PAT/TM-8 Patent Application Secrecy Order Files GSA/GOV-7: HSPD–12 US Access COMMERCE/PAT-TM-18, USPTO Personal Identification Verification (PIV) and Security Access Control Systems. PAT/TM-17 USPTO Security Access Control and Certificate Systems COMMERCE/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 5.6, items 120 and 121, Personal Identification Credentials and Cards GRS 3.2, items 060 and 06, PKI Administrative Record
☐	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: ID-AUTH collects, maintains, or disseminates PII about USPTO employees and contractors. The types of information collected, maintained, used or disseminated by the system includes, for example, SSN, name, and fingerprint. When combined or alone, this data set uniquely and directly identifies individuals. If the PII were inappropriately accessed, used, or disclosed, potential harm could result to the subject individuals and or the organization.
☒	Quantity of PII	Provide explanation: PII/BII is collected for all USPTO employees and contractors who have logical and physical access to USPTO assets. Collectively, the number of records collected generate an enormous amount of PII and a breach would result serious collective harm to a substantial number of individuals and harm to the organization's reputation.
☒	Data Field Sensitivity	Provide explanation: SSN, or a combination of name, fingerprint, and birth history, make the data field more sensitive. For example, individuals and organizations will be vulnerable to harms such as identity theft, embarrassment, or loss of trust.
☒	Context of Use	Provide explanation: Information is for identifying individuals to provide logical and physical access to USPTO assets.
☒	Obligation to Protect Confidentiality	Provide explanation: USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974 and USPTO Privacy Policy requires the PII information collected within the system to be protected in accordance with NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information.
☒	Access to and Location of PII	Provide explanation: 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 accounts. Authorized privileged users access the applications for administrative functions only, and authorized non-privileged users access some applications as required for their roles within their group.

☐	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 has identified and evaluated potential threats to PII/BII such as insider threats and adversarial entities which may cause a loss of confidentiality, accessibility, and integrity of information. In the event of computer failure or attack against the system, records of USPTO employees or contractors containing PII could be exposed.

Controls that the bureau/operating unit have put into place to ensure that the information is handled, retained, and disposed appropriately include training, access restriction, password protection, and data retention policies. USPTO has SIEM systems that monitor in real-time all the activities and events within the servers storing PII and USPTO C3 personnel review audit logs received on a regular basis and alert the ISSO and/or the appropriate personnel when unusual activity is identified.

In addition, database servers storing PII are segregated in a highly sensitive zone within the USPTO internal network, and an additional dedicated network firewall/intrusion prevention system (IPS) and a dedicated network switch through Access Control list that limits access restricted to only a few approved and authorized accounts protect the highly sensitive zone. Stringent physical access controls are in place to restrict access to the datacenter and to the rack with the servers hosting the database to only a few authorized individuals. The building has security guards and secured doors. All entrances are monitored through electronic surveillance equipment. The hosting facility is supported by 24/7 onsite hosting and network monitoring by trained technical staff. Physical security controls include indoor and outdoor security monitoring and surveillance; badge and picture ID access screening; and pin code access screening. ID-AUTH system utilizes workstations located at SSC, the identity management software and various peripheral devices for the collection of PII.

In addition, the biographic and biometric information will be used to conduct a criminal history records via fingerprints. The fingerprints will be used to verify identity of the holder of the credential and the photograph will be collected so that it can be printed on the PIV card as a means to identify the cardholder. Biometric minutiae data will be deposited onto secure containers within the PIV cards in accordance with the requirements from FIPS 201-3 and NIST SP 800-76. Any biometric information that is collected from the PIV solution will be immediately and securely stored on Probaris servers (which are located in the USPTO secure data center) once the PIV cards are manufactured and provided to the card applicants. The USPTO PIV system will not store biometric information that pertains to card applicants for any period of time longer than is required to manufacture and maintain the PIV card in order to minimize security exposure that is associated with storing privacy data and the Agency's System of Record. Further, any biometric information that is stored on the PIV card is controlled and safeguarded by the actual smart card device and the security boundaries that are associated with those tokens. The risk assessments and technical solution provided by these PIV card products has been fully assessed and or tested by National Institute of Standards and Technology (NIST) and General Services Administration (GSA) and they have been approved by those agencies as acceptable for federal government use.

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: Privacy Act Statement

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Appendix B

Office of Administrative Services (/oas/) Security Division (/ptointranet/ptosecurity/)
HSPD-12 (/ptointranet/ptosecurity/hspd_more.htm) Name Change Information

Name Change Information

Names often change due to marriage, divorce, or other legal actions. When you have completed your legal name change, your Personal Identify Verification (PIV) badge must be reissued/reprinted with your new name.

PIV Badges are reissued the business day after OCIO has created your new email name and, if requested, Log-On ID, and OCIO has posted the changes to the Patent Application Locating and Monitoring system (PALM)/Employee Locater. **Log-On ID are not routinely changed.** When a Log-On ID change is requested, they are generally only done on Thursdays to allow many systems not under OCIO control to update.

The name and account change process is slightly different for civil servant and contract employees, however in general all employees will need to present a legal "bridging or linking" document showing both names and a minimum of one additional legal document and/or ID in your new name.

- Obtain government issued IDs in your new name. The minimum documents are:
  The original or a certified copy of the legal "bridging or linking" document changing your name that shows your old and new name. This may be a court decree changing your name, a marriage or a divorce document.

  A government issued document or identification document (ID), i.e. a new original Social Security Card, in your new name.

  A government issued ID with a picture. This document can be in your new or old name, but **cannot** be your current USPTO ID.

- A complete list of allowable forms of identification are listed **here (http://ptoweb.uspto.gov/ptointranet/ptosecurity/hspd/hspd_fips_id.htm)**.

Civil Servants

- OCIO requires notification from the Office of Human Resources (OHR) of your name change.
- Make changes to Human Resource records through HR Connect (Instructions are on the Human Resources Finance Frequently Asked Questions (/ptointranet/ohr/faqs/faqs_payroll.htm#address) page).
- The Office of Human Resources will require you to present a Social Security card in your new name

- ***Updating OHR records is done in conjunction with the National Finance Center. The entire OHR process may take several weeks from when you submit your documents, the record is sent to and returns from the National Finance Center, and OCIO is informed your record change is complete.***
- After you receive notification of the changes to your Human Resources records, use this link (mailto:Servicedesk@uspto.gov;OSOS_Windows@uspto.gov; PIVBadging@USPTO.gov &subject=Email and HSPD-12/PIV Badge Name Change&body= I've completed a legal name change and am requesting the changes below to my email address and ID Badge record..%0D %0D I understand OCIO may not be able to use the exact name I'm requesting.%0D ----------%0D %0D FROM: %0D %0D Email address: %0D %0D Log On ID: %0D %0D Last Name: %0D %0D First Name: %0D %0D Middle Initial: (or ﷿None﷿): %0D %0D Suffix (or ﷿None﷿): %0D %0D ----------%0D TO%0D ----------%0D %0D New: %0D %0D Email address: %0D %0D Log On ID (I've read and understand the guidance on log-on ID changes and understand there may be a 24 - 48 hr. synchronization lag): %0D %0D Last Name: %0D %0D First Name: %0D %0D Middle Initial: (or ﷿None﷿): %0D %0D Suffix (or ﷿None﷿): %0D) to generate a request to OCIO for a new email address, and to Security for a new badge.

Contract Employees

Use this link (mailto: &subject=Email and HSPD-12/PIV Badge Name Change&body= COTAR, please forward this request to these addresses:%0D Servicedesk@uspto.gov;OSOS_Windows@uspto.gov; PIVBadging@USPTO.gov %0D %0D The employee listed below has completed a legal name change and I am requesting the changes below to their email address, PALM record, and ID Badge record.%0D They understand OCIO may not be able to use the exact email address requested.%0D ----------%0D %0D FROM: %0D %0D Email address: %0D %0D Log On ID: %0D %0D Last Name: %0D %0D First Name: %0D %0D Middle Initial: (or ﷿None﷿): %0D %0D Suffix (or ﷿None﷿): %0D %0D ----------%0D TO%0D ----------%0D %0D New: %0D %0D Email address: %0D %0D Log On ID (I've read and understand the guidance on log-on ID changes and understand there may be a 24 - 48 hr. synchronization lag): %0D %0D Last Name: %0D %0D First Name: %0D %0D Middle Initial: (or ﷿None﷿): %0D %0D Suffix (or ﷿None﷿): %0D %0D) to generate a request to send to your Contracting Officer's Representative (COR). They will forward it to the OCIO and Security addresses provided.

Facts to be aware of

- Email addresses **must** be changed prior to issuing your replacement badge.
- When OCIO changes your email address or log-on ID, your badge will **no longer work** to "Badge-On" to the PTONET. You will need to obtain your replacement badge to "Badge-On."
- Due to a lag between updating first the Patent Application Locating and Monitoring (PALM) employee locater and then the PTONet log-on and email systems, Security will not be able to issue a new ID until the business day after OCIO has notified you the changes have been made.
- Delete any WebEx meetings. You **will not** be able to access them after your email address change, nor can OCIO access them.

Log On IDs are Not Routinely Changed Along with Email Addresses

- You must make a specific request to change your log-on ID. To allow sufficient time for system synchronization, log-on IDs are processed on Thursdays making Friday the day your new badge can be issued.
- While your Universal Laptop (UL) or Universal Desktop (UD) login should work on the business day following a change to your log-on ID, some of your applications, network drive access, and Telework FOB may **not** work until your login ID is updated in systems not under the control of Accounts Management. This synchronization may take up to 24 ﷿ 48 business hours (or more if any complications arise).

You will be contacted by Accounts Management to coordinate the changes.

Scheduling Your Badge Replacement

- Ensure you have the necessary documents:
  The original or a certified copy of the legal "bridging or linking" document changing your name that shows your old and new name. This may be a court decree changing your name, a marriage or a divorce document.

A government issued document or identification document (ID), i.e. a new original Social Security Card, in your new name.

A government issued ID with a picture. This document can be in your new or old name, but **cannot** be your current USPTO ID.

- A complete list of allowable forms of identification are listed **here. (http://ptoweb.uspto.gov/ptointranet/ptosecurity/hspd/hspd_fips_id.htm)** A new photograph will be taken.
- Due to server lag across systems, there will a **one business day delay** following OCIO's notification that your email name and/or log on ID change is posted and when Security can issue your replacement badge. You should receive an email from Security informing you that your ID Card record has been updated and to schedule an appointment.
- To obtain your new badge at the Alexandria Campus, appointments are strongly encouraged. However if one isn't available to meet your schedule, the Security Services Center will ensure you are issued your card as a walk-in. You only need to make a single **Issuance appointment** (http://w-pattr-102:8040/eventregistration.aspx?task=issue).
- Appointments at Regional Offices must be coordinated with the specific Regional Office (/ptointranet/ptosecurity/hspd/hspd_region_poc.htm) security representatives.

For Additional Questions Contact

- The USPTO HSPD-12/PIV Badging specialists (mailto:PIVBadging@USPTO.gov?subject=HSPD-12/PIV Badge Replacement Question)
- Regional Office (/ptointranet/ptosecurity/hspd/hspd_region_poc.htm) security representatives.
- The Alexandria campus Security Services Center Security Services Center (mailto:SecurityPTO@uspto.gov?subject=HSPD-12/PIV Badge Replacement Question) at 2-8000
- Regional Office (/ptointranet/ptosecurity/hspd/hspd_region_poc.htm) security representatives.
- The Chief Information Officer (OCIO) Service Desk. (mailto:Servicedesk@USPTO.GOV;OSOS_Windows@uspto.gov?subject=Log On ID and Name Change Request Question)

Request Contractor PIV Badge (/ptointranet/ptosecurity/hspd/hspd_contractor.htm)

Active Shooter Information (/ptointranet/ptosecurity/active_shooter.htm)