Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
ID.me (ID.me)

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: 2023.01.09 19:04:37 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO ID.me (ID.me)

Unique Project Identifier: PTOC-00-56-00

Introduction: System Description

Provide a brief description of the information system.

ID.me is a Software-as-a-Service information system, and provides ID verification for MyUSPTO.gov (MyUSPTO) users to prove their legal identity online. Once MyUSPTO receives verified identity information about users they are able to access government services. Currently, ID.me is used by members of the public accessing the Trademark Electronic Application System (TEAS) and Trademark Electronic Application System International (TEASi). USPTO plans to use ID.me throughout the enterprise in the future. However, ID.me will not be used for USPTO employees and government contractors who are already authenticated.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system
ID.Me is a Software-as-a-Service information system.

(b) System location
The system location is in the cloud, it is a Fed RAMP Ready Software as a Service (SaaS) hosted by ID.me. All data and accompanying PII is stored in this cloud.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
ID.me interconnects with MyUSPTO/trademark. MyUSPTO is a single place for users to actively manage their intellectual property portfolio. Users accessing TEAS and TEASi are redirected to MyUSPTO where they are able to track trademark registrations and statuses and access USPTO services in their personalized USPTO gateway.

(d) The way the system operates to achieve the purpose(s) identified in Section 4
As part of the ID verification process, information exchanges between MyUSPTO and the ID.me vendor system through SAML 2.0 once users access TEAS or TEASi. From the TEAS and TEASi systems, the user is directed to the login screen of MyUSPTO where they are able to click the ID proofing button. MyUSPTO then generates SAML with user data such as MyUSPTO ID, role, and name which directs the user browser to ID.me to begin the proofing process. Any information and communication related to proofing will be handled by ID.Me. USPTO is not directly involved in the ID proofing process or any data collection associated with it.

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

Users logging in through TEAS or TEASi will be redirected to MyUSPTO where they will be able to access an ID proofing button. The user will then be redirected over to ID.Me portal where they will provide the necessary identifying details/documents to get proofed. Once they are proofed within ID.Me, users will be sent back to MyUSPTO along with the result of proofing, which is then saved into the user profile record within TEAS or TEASi.

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

USPTO follows strict guidelines regarding handling and transmitting PII/BII. Data transmitted to and from ID.me is protected by secure methodologies, SAML 2.0, and is encrypted at rest and in transit. The data that is transmitted is kept to a minimum, only MyUSPTO ID, roles, and names are encrypted within the body of the SAML message and transported from MyUSPTO to ID.Me.

(g) Any information sharing

ID.Me shares general information such as user ID, first name, middle name, and last name about MyUSPTO trademark registrants on a case-by-case basis with USPTO employees and contractors.

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

35 USC 2 and 35 USC 301, and E.O. 9397

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

ID.Me 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.Me is focused on preventing duplication, impersonation, and deception when verifying identity information. To this end, the collection of SSN is required in order for ID.Me to perform identity proofing in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3. The NIST standards require the identity provider to perform a task known as identity resolution (see NIST800-63A 5.1 https://pages.nist.gov/800-63-3/sp800-63a.html). ID.Me also performs sanctions checks to make sure that an individual is not on a sanctions list where government agencies and other organizations are prohibited from rendering services to the listed individual. Both of these checks currently require SSN as there is no other ubiquitous identifier for Americans that can uniquely identify an individual.					

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): Physical Characteristics					

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): A soft credit inquiry may be conducted.					

2.3 Describe how the accuracy of the information in the system is ensured.

The accuracy of the information in ID.Me is assured through The Federal Risk and Authorization Management Program (FedRAMP), NIST SP 800-63-3 Digital Identity Guidelines, access controls, and system monitoring. FedRAMP is a US government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP requires that ID.Me verify the accuracy, timeliness, and completeness of the data via audit logs and use advanced encryption both during transmission and while stored at rest. In order to meet NIST SP 800-63-3 such as in the case of credit agencies and mobile network operators (MNOs), ID.Me verifies asserted PII against authoritative records. The system only sends asserted PII and receives verification data from source. Access to an individual's PII is controlled through the application. ID.Me 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 such as browsing will be immediately investigated and appropriate action taken.

2.4 Is the information covered by the Paperwork Reduction Act?

☐	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
☒	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	☐	Biometrics	☐
Caller-ID	☐	Personal Identity Verification (PIV) Cards	☐
Other (specify):			

☒	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	☐	Building entry readers	☐

Video surveillance	☐	Electronic purchase transactions	☐
Other (specify): Click or tap here to enter text.			

☒	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program	☐	For administering human resources programs	☐
For administrative matters	☒	To promote information sharing initiatives	☐
For litigation	☐	For criminal law enforcement activities	☐
For civil enforcement activities	☐	For intelligence activities	☐
To improve Federal services online	☒	For employee or customer satisfaction	☐
For web measurement and customization technologies (single-session)	☐	For web measurement and customization technologies (multi-session)	☐
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

ID.Me collects, maintains, and or stores PII/BII about members of the public who opt to use the service via MyUSPTO when submitting information for trademarks using the TEAS and TEASi systems. ID.me platform is used to assist with verifying applicants and for administrative matters. It is also used to improve federal services online by allowing users who access TEAS or TEASi via MyUSPTO and ID.Me to conduct official Trademark business online. Once a user's identity is verified with ID.Me, they will be able to conveniently access the TEAS or TEASi system to fill out online USPTO forms, submit forms directly to the USPTO over the Internet, and pay by credit cards, electronic funds transfer, or through an existing USPTO deposit account.

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 potential PII data from MyUSPTO users stored within the system could be exposed. In an effort to avoid a breach, ID.Me 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 an individual's PII is controlled through the application and all personnel who access to 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 such as browsing will be immediately investigated and appropriate action taken. NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.

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.Me connects with the following systems authorized to process PII/BII: • MyUSPTO • TEAS NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.
☐	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: ID.Me Privacy Bill of Rights https://www.id.me/privacy
☐	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: ID.me is not mandatory for individuals who want to use the TEAS or TEASi system. Individuals who do not want to verify their identity online and through ID.Me can instead submit their identity verification information in paper form directly to USPTO.
☐	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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: No, individuals do not have an opportunity to consent to particular uses of their PII/BII. However, when users create an ID.Me account and use the ID.Me service, they opt in by providing the information they want to use to verify their identity. Users consent by choosing which information to provide but they can not consent to particular uses of their PII/BII.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

☒	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Users may change any of their PII/BII by logging into their ID.Me account or contacting ID.Me directly at help@ID.Me.
☐	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): 10/26/2022 ☐ 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): DOC only owns the data passed back, consisting of user ID, first name, middle name, and last name.

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 ID.Me is secured using appropriate management, operational, and technical safeguards in accordance with FedRAMP requirements. Such management controls include the Life Cycle review process to ensure that management controls are in place and documented in the System Security Plan (SSP). The SSP 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 ID.Me 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. ID.Me 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-26/USPTO-26- Trademark Application and Registration Records COMMERCE/PAT-TM-23- User Access for Web Portals and Information Requests COMMERCE/PAT-TM-16- USPTO PKI Registration and Maintenance System COMMERCE/PAT-TM-17- USPTO Security Access Control and Certificate 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, item 031, System Access Records
☐	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 could be large and would depend on the number of MyUSPTO users requiring ID verification services through TEAS.
☒	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: ID.ME is used to verity applicants via MyUSPTO that want to support applications to the TEAS and TEASi systems.
☒	Obligation to Protect Confidentiality	Provide explanation: FedRAMP and NIST SP 800-63-3 provide the guidance to protect confidentiality. FedRAMP is a US government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
☒	Access to and Location of PII	Provide explanation: General data such as user ID, first name, middle name, and last name about TEAS and TEASi applicants will be located on computers within USPTO. Any information and communication related to identity proofing such as SSN will be handled by ID.Me.
☐	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.)

Foreign and adversarial entities, insider threats, and computer failure are activities which may raise privacy concerns related to the collection, maintenance, and dissemination of PII. ID.Me mitigates such threats through minimizing the collection of PII and by securing the system with appropriate management, operational, and technical safeguards in accordance with FedRAMP requirements, including system Life Cycle review, restricting access to PII/BII data to a small subset of ID.Me users, screening users for suitability, maintaining data in areas accessible only to authorize personnel, and continuously monitoring the system for inappropriate activity.

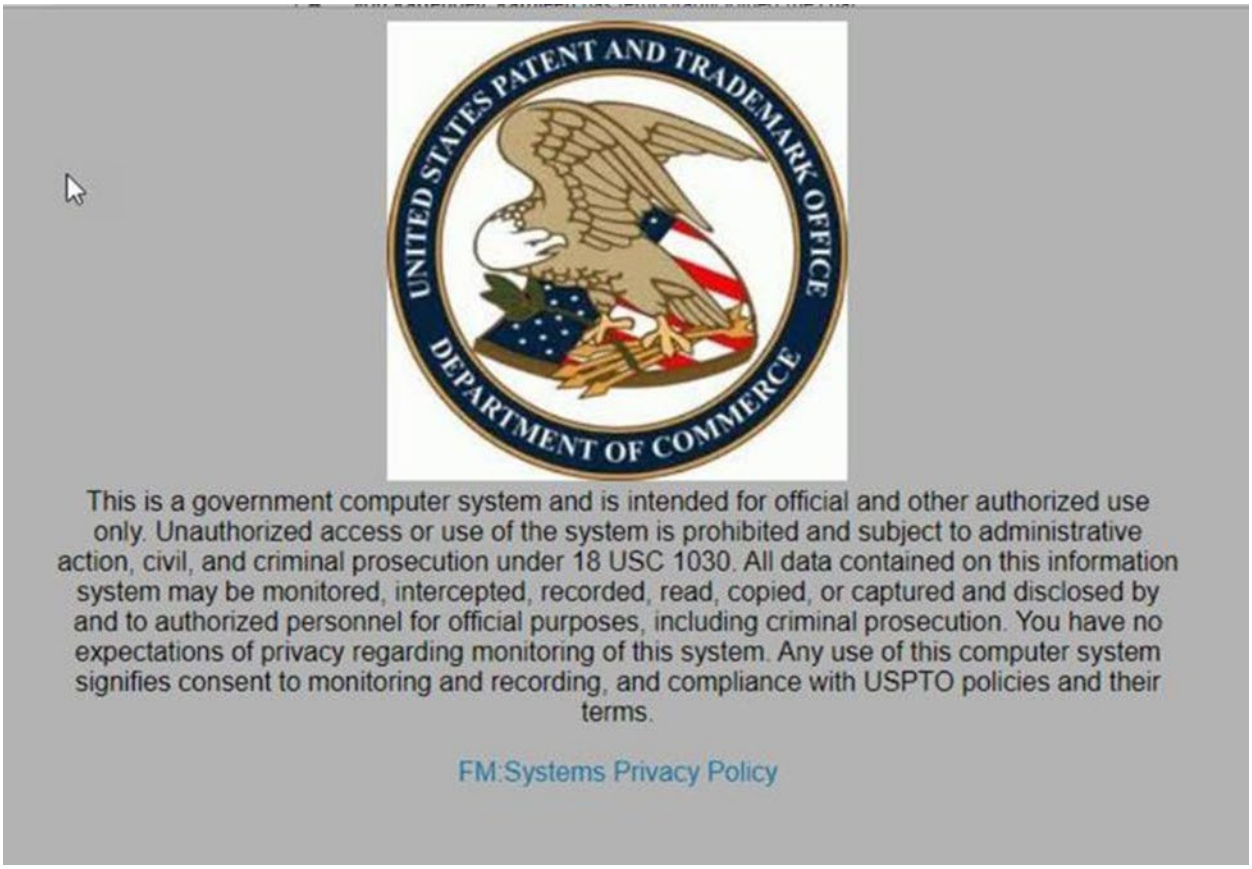
12.2 Indicate whether the conduct of this PIA results in any required business process changes.

☐	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



Points of Contact and Signatures

System Owner
Name: Matthew Duckett
Office: Corporate Systems Division (I/AEDCSD)
Phone: (571) 272-5468
Email: Matthew.Duckett@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, Duckett, Matthew — Digitally signed by Users, Duckett, Matthew Date: 2022.11.25 16:33:37 -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

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: 2023.01.01 12:40:59 -05'00'

Date signed: _____

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

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: 2022.12.20 09:53:51 -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

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: 2023.01.09 19:05:22 -05'00'

Date signed: _____

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: _____

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