Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
ID.me (ID.me)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO ID.me (ID.me)

Unique Project Identifier: PTOC-00-56-00

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

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

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

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 purpose that the system is designed to serve

The ID.Me is a Software-as-a-Service information system, and provides ID verification for MyUSPTO users. USPTO is the consumer of ID.Me ID verification services.

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

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.

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

ID.me will collect user data such as MyUSPTO ID, Roles, and Names. This information is currently stored as part of the user record. 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.

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

USPTO employees, contractors, and ID.me team have access to information on the system.

h) 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.

i) 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.

Questionnaire:

1. Status of the Information System

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

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

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

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	☐	d. Significant Merging	☐	g. New Interagency Uses	☐
b. Anonymous to Non-Anonymous	☐	e. New Public Access	☐	h. Internal Flow or Collection	☐
c. Significant System Management Changes	☐	f. Commercial Sources	☐	i. Alteration in Character of Data	☐
j. Other changes that create new privacy risks (specify):					

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

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

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

☐ Yes. This is a new information system.

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

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

☒ No. This is not a new information system.

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

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

☐ Yes. *(Check all that apply.)*

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

☒ No.

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

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

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

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

4. Personally Identifiable Information (PII)

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

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

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

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

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

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

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

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

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

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 NIST 800-63A 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.
Provide the legal authority which permits the collection of SSNs, including truncated form. 35 U.S.C. 2

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

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

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

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

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

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

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

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

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

CERTIFICATION

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

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

System Owner Name: Matthew Duckett Office: Corporate Systems Division (I/AEDCSD) Phone: (571) 272-5468 Email: Matthew.Duckett@uspto.gov Signature: Users, Duckett, Matthew Digitally signed by Users, Duckett, Matthew Date: 2022.11.25 16:37:57 -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: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2023.01.01 12:42:05 -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 Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2022.12.20 09:50:21 -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: 2023.01.09 19:02:35 -05'00' Date signed: _____
Co-Authorizing Official Name: N/A Office: N/A Phone: N/A Email: N/A Signature: _____ Date signed: _____	