Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
MyUSPTO Cloud (MyUSPTO-C)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO MyUSPTO Cloud (MyUSPTO-C)

Unique Project Identifier: PTOC-054-00

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).

MyUSPTO Cloud (MyUSPTO-C) is a web site for USPTO employees, contractors, and members of the public to track patent applications and grants, check trademark registrations and statuses, and to actively manage their intellectual property portfolio within a personalized gateway.

Address the following elements:

a) Whether it is a general support system, major application, or other type of system

MyUSPTO-C is a minor application.

b) System location

MyUSPTO-C is located within a cloud-based platform hosted by AWS East Primary location: 7 Walnut Grove Drive, Horsham, Pennsylvania.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

MyUSPTO-C interconnects with the following systems:

- **Network and Security Infrastructure System (NSI)** is an infrastructure information system, and provides an aggregate of subsystems that facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO information technology (IT) applications.
- **Service Oriented Infrastructure (SOI)** is a general support system, and provides a feature-rich and stable platform upon which USPTO applications can be deployed.

- **Enterprise Software Services (ESS)** is comprised of multiple on premise and in-the-cloud software services, which support the USPTO in carrying out its daily tasks. Within this system, the services are broken up into several subsystems. These subsystems are Enterprise Active Directory Services (EDS), MyUSPTO, Role Based Access Control (RBAC), Email as a Service (EaaS), Enterprise SharePoint Services (ESPS), Symantec Endpoint Protection, and PTOFAX.
- **Enterprise UNIX Services (EUS)** is an infrastructure operating system, and provides a UNIX-based hosting platform to support other systems at USPTO.
- **Security and Compliance Services (SCS)** is a general support system comprised of subsystems, and provides enterprise-level monitoring to the USPTO.
- **Fee Processing Next Generation (FPNG)** is a major application, and provides fee-processing solutions within USPTO. FPNG replaced the Revenue Accounting and Management (RAM) system, which served as a subsidiary to the core financial system, Momentum.
- **TPS-ES Trademark Processing System (External) (TPS-ES)** is a major application, and supports USPTO staff and public users through the trademark application process.
- **Patent End to End (PE2E)** is a major application, and provides examination tools used for the examination, issuance, and granting of patents.
- **Patent Capture and Application Processing System - Capture and Initial Processing (PCAPS-IP)** is a major application, and supports initial patent application process with data capture, application processing, and reporting.
- **Patent Capture and Application Processing System - Examination Support (PCAPS-ES)** is a major application, and supports the patent application process with data capture and conversion support.

d) The purpose that the system is designed to serve

MyUSPTO-C is a web site for USPTO employees, contractors, and members of the public to actively manage their intellectual property portfolio. For example, users may track patent applications and grants, check trademark registrations and statuses, and actively manage their intellectual property portfolio within a personalized gateway. The site is also used for purposes of disaster recovery if in the event the local system, which is located on USPTO premises, fails.

e) The way the system operates to achieve the purpose

Users access MyUSPTO-C via the Uniform Resource Locator (URL) www.myuspto.gov. At the home page of MyUSPTO.gov, users can create a new account with information such as an email address, first name, last name, and phone number or log into an existing account, with an email address and password. Once logged into the site, users manage their intellectual property portfolio within a personalized gateway.

MyUSPTO-C is the AWS environment for disaster recovery in the event that the MyUSPTO servers in both the blue and green environments become unavailable.

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

MyUSPTO-C collects, maintains, uses, or disseminates information to members of the public about USPTO services. Members of the public provide general information such as name, phone number, email address, and password to create an account and access the system. Data related to system monitoring and auditing may also be captured.

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

Individuals who have access to the system include USPTO employees, contractors, and members of the public.

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

Users enter their username and password to gain access to their personalized USPTO Business Gateway. The personalized gateway is composed of widgets. Widgets consist of links to various USPTO backend services. Patent and Trademark docket widgets allow users to create collections containing applications, registered trademarks, and patents that they can track, share, and monitor. Notifications on docket widgets provide status updates and recent status changes. For example, within the Trademark Form Finder widget, users click on the File application link. The link will open to the Trademark Electronic Application System (TEAS) to complete and file an application.

*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 MyUSPTO-C is protected by secure methodologies such as Hypertext Transfer Protocol Secure (HTTPS), used for secure communication over a computer network and Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security 1.2 (TLS 1.2). Security Assertion Markup Language 2.0 (SAML 2.0) is used for exchanging authentication and authorization identities between security domains. All data stored at rest is also encrypted.

Questionnaire:

1. Status of the Information System

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

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

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

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

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

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

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

☒ Yes. This is a new information system.

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

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

☐ No. This is not a new information system.

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

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

☐ Yes. *(Check all that apply.)*

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

☒ No.

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

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

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

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?
As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

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

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

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

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

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

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

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

Provide the legal authority which permits the collection of SSNs, including truncated form.

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

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

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

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

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?
Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

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

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

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

CERTIFICATION

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

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

System Owner Name: Jimmy Orona, III Office: Enterprise Software Services Division Phone: (571) 272-0673 Email: Jimmy.Orona@uspto.gov Signature: Users, Orona, Jimmy III Digitally signed by Users, Orona, Jimmy III Date: 2022.01.27 08:59:51 -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: 2022.01.31 11:14:44 -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: 2022.01.26 13:49:56 -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: 2022.01.31 12:55:31 -05'00' Date signed: ________________________________
Co-Authorizing Official Name: N/A Office: N/A Phone: N/A Email: N/A Signature: ________________________________ Date signed: ________________________________	

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