Template Version Number: 01-2020

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

## Privacy Threshold Analysis
## for the
## OKTA Identity as a Service (IdaaS)

# U.S. Department of Commerce Privacy Threshold Analysis

# USPTO OKTA IDaaS

**Unique Project Identifier: PTOC-043-00**

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

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

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

USPTO is leveraging OKTA IDaaS hosted within FedRAMP Certified Cloud to provide the enterprise services for the Identity and Access Management (IAM). The supporting components for the USPTO IAM services are located at the United States Patent and Trademark Office (USPTO), 600 Dulany St, Alexandria. The system provides Identity Management (including user provisioning for the public), Authentication and coarse grained Authorization to the USPTO systems. This allows the USPTO user community, systems, and its employees to access the resources provided by the organization while protecting those services from unauthorized access and/or individuals and systems. OKTA IDaaS FedRAMP'd system has placed security controls in place or planned, as derived from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4. The supporting components that are part of the OKTA IDaaS Identity Management System that is deployed within the USPTO on-prem data center also has placed security controls as derived from the NIST SP 800-53 Revision 4. The system is designed and configured to protect all communications between systems within USPTO and all transactions from USPTO to OKTA IDaaS.

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

This system is a major application.

***b) System location***

System will be deployed in a hybrid deployment architecture where the core components of the systems will be deployed and supported by the SaaS vendor (OKTA) and the supporting

components will be deployed in the USPTO datacenter located in USPTO facilities at, 600 Dulany St, Alexandria, VA.

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

The system will be leveraged by other USPTO applications. The system is currently integrated with over 50 applications and the goal of the organization is to integrate all the applications that are deployed within the USPTO Network.

***d) The purpose that the system is designed to serve***

The system is designed to provide enterprise authentication/authorization services to the integrated applications/systems. The application will integrate with the OKTA IDaaS services to protect and leverage the services to meet NIST controls compliance for Access Control (AC), Auditing (AU), and Identification and Authentication (IA).

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

The purpose of the system is to protect USPTO services by authenticating and authorizing users and systems. The system disambiguates the user and provides the integrated partner/system with user's identity and ability to make fine grained authorization decision.

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

The system collects user attributes (name, telephone number, email address) for USPTO employees, members of the public, and contractors working on behalf of USPTO.

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

- System administrators have system management and configuration access
- System analysts have system access

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

Administrators retrieve the information in the system for the purpose of making profile specific changes and for supporting users and/or the system during troubleshooting. All information in the system is encrypted in transit and at rest and access is restricted using user specific role policies. The information can be accessed by logging into the administrator consoles via a web browser and/or through a user interface.

***i) How information is transmitted to and from the system***

There is not information sharing between systems. The internal USPTO users are accessed via active directory agents and there is a one way synchronization between Active Directory (AD) and OKTA IDaaS identity store.

**Questionnaire:**

1. Status of the Information System

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

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

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

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

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

☐ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017). *Continue to answer questions and complete certification.*

☐ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later). *Skip questions and complete certification.*

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

☒ Yes. This is a new information system.

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

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

☐ No. This is not a new information system.

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

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

☐ Yes. *(Check all that apply.)*

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

☒ No.

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

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

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

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

4. Personally Identifiable Information (PII)

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

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

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

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

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

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

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

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

| Provide an explanation for the business need requiring the collection of SSNs, including truncated form. |
|---|
| 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 OKTA IDaaS 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 OKTA IDaaS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

| | |
|---|---|
| **System Owner**<br>Name: Jimmy Orona III<br>Office: I/ESSD – Software Services Branch 2<br>Phone: (571) 272-0673<br>Email: Jimmy.Orona@uspto.gov<br><br>Signature: Users, Orona, Jimmy III Digitally signed by Users, Orona, Jimmy III Date: 2021.07.13 09:38:01 -04'00'<br><br>Date signed: _____ | **Chief Information Security Officer**<br>Name: Don Watson<br>Office: Office of the Chief Information Officer (OCIO)<br>Phone: (571) 272-8130<br>Email: Don.Watson@uspto.gov<br><br>Signature: DON R Watson Digitally signed by DON R Watson Date: 2021.07.14 13:54:47 -04'00'<br><br>Date signed: _____ |
| **Privacy Act Officer**<br>Name: John Heaton<br>Office: Office of General Law (O/GL)<br>Phone: (571) 270-7420<br>Email: Ricou.Heaton@upsto.gov<br><br>Signature: Users, Heaton, John (Ricou) Digitally signed by Users, Heaton, John (Ricou) Date: 2021.07.08 15:53:47 -04'00'<br><br>Date signed: _____ | **Bureau Chief Privacy Officer and Authorizing Official**<br>Name: Henry J. Holcombe<br>Office: Office of the Chief Information Officer (OCIO)<br>Phone: (571) 272-9400<br>Email: Jamie.Holcombe@uspto.gov<br><br>Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2021.07.16 09:32:22 -04'00'<br><br>Date signed: _____ |
| **Co-Authorizing Official**<br>Name: N/A<br>Office: N/A<br>Phone: N/A<br>Email: N/A<br><br>Signature: _____<br><br>Date signed: _____ | |