Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
KUDO Platform (UKP)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO KUDO Platform (UKP)

Unique Project Identifier: EIPL-EUS-07-00

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).

USPTO Kudo Platform (UKP) enables business units to share vital knowledge through collaboration capabilities that incorporate data, multilingual voice, and video communication technologies. The UKP is a FedRAMP ready cloud-based solution for over-the-web meetings and video conferencing in multiple languages. Attendees can participate in webinars, web meetings and training sessions, share content and collaborate globally. KUDO streams real-time language interpretation to participants' smartphones and computers, so everyone can join in their own language from anywhere. Attendees are able to cast votes and voice their ideas while the meeting unfolds.

The purpose of this system is to enable USPTO business units to collaborate with external customers who speak a language other than English through hosting online meetings on a secure cloud-based video conferencing platform with real-time multilingual interpretation. USPTO business units gain efficiency and effectiveness by communicating and sharing vital business knowledge with internal customers. The UKP system users are comprised of employees and contractors, including system administrators and regular users that access the system internally through PTO Net and external customers who access the system over the Internet. Users include USPTO Office of Policy and International Affairs (OPIA), Global IP Academy (GIPA), Office of Undersecretary, and GIPA staff.

Address the following elements:

a) *Whether it is a general support system, major application, or other type of system*
UKP is a Software as a Service (SaaS).

b) *System location*

UKP is hosted in the cloud by KUDO, Inc. - KUDO Platform, FedRAMP Ready system.

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

UKP receives PII from the USPTO ICAM Identity as a Service (ICAM-IDaaS) system via Security Assertion Markup Language (SAML) 2.0.

ICAM Identity as a Service (ICAM-IDaaS): provides an enterprise authentication and authorization service to all applications/AIS's. As part of the enterprise services it will also provide compliance for some of the NIST 800-53 controls (e.g. AC, AU AP). The system provides following services to the enterprise:
-User Provisioning and Life Cycle Management
-User Roles and Entitlement Management
-User Authentication and Authorization to protected resources
-Application Integration/Protection
-NIST controls compliance related to AU, AC, and IA family

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

UKP provides multilingual web conferencing for internal and external customers.

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

UKP provides meeting links to meeting participants and interpreters. Meeting participants join the meeting via the meeting links from their device browser or KUDO Mobile App. Interpreters join meetings via the meeting links using their computer. Meeting content includes video, audio, and data from meeting participants and translated audio from interpreters.

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

UKP collects, maintains, or disseminates PII such as name, address and meeting content, e.g. video and audio, about DOC employees, contractors, other federal government personnel, and members of the public, or meeting participants.

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

USPTO employees and contractors have access to information in the system. Authorized internal USPTO and public users have access to web conferencing content and recorded videos.

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

Users are authorized USPTO staff, contractors, and public users, including public interpreters. Users connect to the KUDO SaaS cloud via authorized USPTO devices and networks, web browser, or KUDO mobile app. USPTO staff and contractors host and participate in multilingual web conferences and interpreters participate and perform language translation. Public users participate in the web conference.

i) How information is transmitted to and from the system

Users access KUDO through a browser using PTOnet or VPN. Users are authenticated via SAML 2.0. Data is transmitted to and from the system via Hypertext transfer protocol secure (HTTPS) and Real-Time Messaging Protocol (RTMPS) connection to the FedRAMP Ready KUDO Platform SaaS Cloud.

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

☒ The criteria implied by one or more of the questions above **apply** to the KUDO Platform (UKP) 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 KUDO Platform (UKP) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: He, Gengshu Scott Office: Collaborative Services Division Phone: (571) 272-0038 Email: Ghe@uspto.gov Signature: Scott G He Digitally signed by Scott G He Date: 2023.02.27 08:32:56 -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: 2023.02.28 14:56:29 -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: 2023.02.24 11:15:05 -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: 2023.02.28 16:51:30 -05'00' Date signed: _____
Co-Authorizing Official Name: N/A Office: N/A Phone: N/A Email: N/A Signature: _____ Date signed: _____	