Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
KUDO Platform (UKP)

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: 2023.02.28 16:53:34 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO KUDO Platform (UKP)

Unique Project Identifier: EIPL-EUS-07-00

Introduction: System Description

Provide a brief description of the information system.

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 way the system operates to achieve the purpose(s) identified in Section 4
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.

(e) 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.

(f) 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.

(g) Any information sharing
Authorized USPTO staff and contractors have access to the data stored on the UKP System.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
The citation of the legal authority to collect PII and/or BII is 5 U.S.C 301, 35 U.S.C. 2, and E.O.12862.

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

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:					

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):					

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): Meeting files such as Power point slides, work documents and notes. Votes from polls, chat logs and meeting transcripts.					

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):					

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

PII in UKP is secured using appropriate administrative, physical and technical safeguards in accordance with the FedRAMP Moderate Impact Software as a Service (MI-SaaS) Authorization. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access and changes as part of verifying the integrity of data. Mandatory IT Awareness and role-based training is required for staff who have access to the system and addresses how to handle, retain, and dispose of data.

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).

The information in the system may contain PII about employees, contractors, other federal employees and members of the public. The information provided by virtual meeting participants is collected, maintained, or disseminated to promote information sharing initiatives, to improve employee or customer satisfaction, and to improve Federal services online. Meeting recordings (i.e., video and audio), files, notes, chat logs and transcripts, and any other information uploaded while using the Services is collected and maintained to promote information sharing. The list of meeting participants allows meeting hosts to forward translations of the meeting into different languages as requested by the meeting participants which promotes employee or customer satisfaction. Name and email address are collected and maintained in audit logs to improve federal services online.

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.)

The risks to the system are insider threats and adversarial entities. Mandatory IT awareness and role-based training is required for staff who have access to the system and addresses how to handle, retain, and dispose of data. Training is also provided to handle insider threats. UKP implements NIST security and management controls to prevent the inappropriate disclosure of sensitive information. Automated mechanisms are in place to ensure the security of all data collected. Security controls are employed to ensure information is resistant to tampering (Physical and Access Controls), the confidentiality of data in transit (Encryption), and that data is available for authorized users only (Access Control). Management controls are utilized to prevent the inappropriate disclosure of sensitive information. In addition, the Network and Security Infrastructure System (NSI) and Security and Compliance Services (SCS) systems provide additional automated transmission and monitoring mechanisms to ensure that PII is protected and not breached by any outside entities or insider threats. In the event of disposal, UKP uses degaussing to permanently remove data according to government mandate and security policy.

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: ICAM-IDaaS 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: Privacy Policy - KUDO (kudoway.com)
☐	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: Members of the public can choose to enter any name or email address to participate in the web conference thereby having the opportunity to decline to provide their real names. Their name and email address are not verified or used for authentication.
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: USPTO employees and contractors do not have the ability to decline to provide PII since the authentication process automatically passes the user's name and USPTO email address to UKP via ICAM.

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: UKP allows the user to submit their personal information voluntarily by not enforcing credential verification. When a user voluntarily submits information, it constitutes their consent to use the information for purposes stated at the time of collection.
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: UKP allows the user to submit their personal information voluntarily by not enforcing credential verification. When a user voluntarily submits information, it constitutes their consent to use the information for purposes stated at the time of collection.

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:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: USPTO employees and contractors may contact Human Resources to update their PII. Public users have an opportunity to review/update PII before submitting the information but they cannot update their information after submission.

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: The PII (from both members of the public and USPTO employees and contractors) is recorded and stored in a KUDO SaaS database. That PII is monitored and tracked by USPTO on an as-needed basis.
☒	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): 3/22/2022 ☐ 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):

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).*

UKP provides protection of PII in accordance with NIST 800-18 Rev. 1 and NIST 800-53 Rev. 4. The UKP System Security Plan (SSP) addresses the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment. The SSP is reviewed on an annual basis. In addition, annual assessments and Continuous Monitoring reviews are conducted for UKP. The USPTO Cybersecurity Division (CD) conducts these assessments and reviews based on NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations and NIST SP 800-53A Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations. The results of these assessments and reviews are documented in the UKP Security Assessment Package (SAP) as part of the system's Security Authorization process.

UKP implements security and management controls to prevent the inappropriate disclosure of PII. Automated mechanisms are in place to ensure the security of all data collected. Security controls are employed to ensure information is resistant to tampering (Physical and Access Controls), the confidentiality of data in transit (Encryption), and that data is available for authorized users only (Access Control).

UKP is secured using appropriate administrative, physical and technical safeguards in accordance with the FedRAMP Moderate Impact-SaaS Authorization. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access and changes as part of verifying the integrity of data.

USPTO uses the Life Cycle review process to ensure that management controls are in place for UKP. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the SSP. The SSP specifically addresses the management, operational, and technical controls that are in place, and planned, during the operation of the enhanced system. Additional management controls include performing national agency checks on all personnel, including contractor staff. Additionally, USPTO develops privacy and PII-related policies and procedures to ensure safe handling, storing, and processing of PII.

UKP is secured by various USPTO infrastructure components, including the NSI and SCS systems and other OCIO-established technical controls to include SAML 2.0 authentication to UKP. Web communications leverages modern encryption technology such HTTPS and RTMPS connections.

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/DEPT-23 Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs. COMMERCE/PAT-TM-19 Dissemination Events and Registrations COMMERCE/DEPT-18 Employees Personnel Files Not Covered by Notices of Other Agencies COMMERCE/DEPT-20: Biographical Files and Social Networks
☐	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 5.1, item 020: Non-recordkeeping copies of electronic records GRS 5.2, item 020: Intermediary 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: The collection of names and email addresses can be used to identify an individual.
☒	Quantity of PII	Provide explanation: The quantity can vary since the information is limited to meeting participants.
☒	Data Field Sensitivity	Provide explanation: UKP system personnel consider the PII (name and email address for USPTO employees and contractors; potential real name and email address [unverified] for members of the public) to be low sensitivity.
☒	Context of Use	Provide explanation: USPTO Kudo Platform (UKP) enables business units to share vital knowledge through collaboration capabilities that incorporate data, multilingual voice, and video communication technologies. Name and email address are collected from USPTO employees, contractors, and meeting participants so that they will be able to participate in the collaborative meetings.
☒	Obligation to Protect Confidentiality	Provide explanation: In accordance with NIST 800-53 Rev. 4, UKP implements both AR-2 (Privacy Impact and Risk Assessment) and AR-7 (Privacy-Enhanced System Design and Development) security controls to ensure all user's confidentiality is protected. USPTO Privacy Policy requires the PII information collected within the system to be protected accordance to NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information. In accordance with the Privacy Act of 1974, PII must be protected.
☒	Access to and Location of PII	Provide explanation: Authorized USPTO staff and contractors have access to the data in UKP. UKP is secured using appropriate administrative, physical and technical safeguards in accordance with the FedRAMP Moderate-SaaS Authorization.
☐	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. USPTO has identified and evaluated potential threats to PII such as loss of confidentiality and integrity of information. Based upon USPTO's threat assessment, the Agency has implemented a baseline of security controls to mitigate the risk to information to an acceptable level. Controls that the bureau/operating unit have put into place to ensure that the information is handled, retained, and disposed appropriately include training, access restriction, password protection, and data retention policies.

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.

Points of Contact and Signatures

System Owner
Name: He, Gengshu Scott
Office: Collaborative Services Division
Phone: (571) 272-0038
Email: Ghe@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: Scott G He Digitally signed by Scott G He Date: 2023.02.27 08:31:53 -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: 2023.02.28 14:58:21 -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: 2023.02.24 11:17:56 -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

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: 2023.02.28 16:54:11 -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.