Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
VBrick Rev® Cloud® Service (VRC)

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

for Charles Cutshall

TAHIRA MURPHY Digitally signed by TAHIRA MURPHY
Date: 2024.11.29 22:12:40 -05'00' 10/31/2024

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO VBrick Rev® Cloud® Service (VRC)

Unique Project Identifier: EIPL-EUS-05-00

Introduction: System Description

Provide a brief description of the information system.

VBrick Rev Cloud (VRC) is a United States Patent and Trademark Office (USPTO) information system that utilizes the VRC Service Federal Risk and Authorization Management Program (FedRAMP) authorized system. The FedRAMP VRC Service system is deployed and operated by VBrick as a multi-tenant Software as a Service (SaaS) product, and it is operated on top of the Amazon Web Services (AWS) cloud infrastructure. As an enterprise product, VRC Service includes the ability to interact and integrate with USPTO directory services and Single Sign On (SSO) capabilities to provide authentication for internal or confidential content. That integration occurs via USPTO's VRC system.

Address the following elements:

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

VRC is a major application and cloud-based Software-as-a-Service (SaaS) operating out of Amazon Web Services (AWS).

(b) System location

The VRC Service FedRAMP system is located in Herndon, Virginia. The USPTO VRC system is hosted on the VRC Service, which utilizes the AWS cloud. All data and any accompanying Personally Identifiable Information (PII) is stored in VBrick Rev SaaS cloud. There is no physical on-premise location for the VRC system.

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

VBrick VRC uses USPTO's Security Assertion Markup Language (SAML) 2.0 SSO system ICAM-IDaaS for all account provisioning and access authorization. ICAM-IDaaS requires that a USPTO user connect to VRC on an authorized USPTO's network system (NSI). VRC started using ICAM-IDaaS in September 2021.

VRC interconnects with the following systems:

Identity, Credential, and Access Management (ICAM) Identity as a Service (ICAM-IDaaS) System - provides an enterprise authentication and authorization service to all applications / Information Systems.

Network and Security Infrastructure (NSI) System - facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO applications.

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

VRC can directly serve video files or provide links to live webcasts, and is able to provide flexible deployment options for both generating and presenting content. VRC ties together devices located at customer sites to provide video experience to users who may be either in branch office locations or viewing remotely from home or from a mobile device.

(e) How information in the system is retrieved by the user

Name, IP (Internet Protocol) address, and email address information is retrieved by authorized USPTO staff and contractors via web browsers on authorized USPTO computer devices and networks connected to the VBrick SaaS cloud. Authorized USPTO staff and contractors via web browsers on authorized USPTO computer devices and networks retrieve USPTO internal video and live webcast content. Users via a web browser retrieve public video and live webcast content.

(f) How information is transmitted to and from the system

Information is transmitted to and from the system via an Internet connection to the VBrick SaaS Cloud.

(g) Any information sharing

Authorized USPTO staff and contractors have access to the data stored on the VRC System. VRC does not disseminate PII information to any other systems.

(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

Low

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):					

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): USPTO ICAM-IDaaS System via a SAML 2.0 connection to VRC.					

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.

For members of the public, they can choose to enter any name or email address (whether valid or not) into the system. Their name and email address are not verified or used for authentication. Due to the lack of verification and authentication, no members of the public can be definitively identified.

For USPTO employees and contractors, a background investigation is done by the USPTO Security Office prior as part of the onboarding process. Therefore, all employees and contractor's names and email addresses are already identified in USPTO ICAM-IDaaS via Security Assertion Markup Language (SAML) 2.0. VRC only uses this already existing data.

The non-sensitive PII in VRC is secured using appropriate administrative, physical and technical safeguards in accordance with the FedRAMP Low Impact (LI)-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.

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. PTO Form 2030 (Rev. 05/12). OMB 0651-0041 U.S. Patent and Trademark Office; U.S DEPARTMENT OF COMMERCE.
☐	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).

Federal Employees/Contractors: Name and email address are collected and maintained in audit logs, and that information is only used to capture the total number of users that are viewing a live or recorded video. The total number of users helps to improve Federal services online and as a way to measure employee satisfaction with the service.

Members of the Public: Display Name, email address, and IP address are collected and maintained in audit logs, and that information is only used to capture the total number of connections that are viewing a live webcast. The total number of connections helps to improve Federal services online and as a way to measure the public's satisfaction with the service.

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.)

VRC implements 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 Perimeter Network (NSI) system provides additional automated transmission and monitoring mechanisms to ensure that PII is protected and not breached by any outside entities. In the event of disposal, VRC uses degaussing to permanently remove data according to government mandate and security policy.

The security safeguards for the VRC meet the NIST SP 80-53 (Rev. 5) requirements set forth in the System Security and Privacy Plan (SSPP) and in the USPTO IT Security Handbook. The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the enhanced system. All systems are subject to monitoring that is consistent with applicable regulations, agency policies, procedures, and guidelines. The system is implemented with encryption (Secure Socket Layer (SSL)). Authorized users have role-based permissions. VRC is continually monitored to provide "near real-time" risk reporting and mitigation activities.

PII in VRC is secured using appropriate administrative, physical and technical safeguards in accordance with the applicable federal laws, Executive Orders, directives, policies, and standards. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening.

Data is maintained in areas accessible only to authorized personnel. 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. Information is protected through a layered security approach which incorporates the use of secure authentication, access control, mandatory configuration settings, firewalls, Virtual Private Network (VPN), and encryption, where required. Internally within USPTO, data transmission confidentiality controls are provided by PTONet.

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: • USPTO ICAM-IDaaS • NSI The security safeguards for the VRC meet the NIST SP 80-53 (Rev. 5) requirements set forth in the System Security and Privacy Plan (SSPP) and in the USPTO IT Security Handbook. The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the enhanced system. All systems are subject to monitoring that is consistent with applicable regulations, agency policies, procedures, and guidelines. The system is implemented with encryption (Secure Socket Layer (SSL)). Authorized users have role-based permissions. VRC is continually monitored to provide "near real-time" risk reporting and mitigation activities. PII in VRC is secured using appropriate administrative, physical and technical safeguards in accordance with the applicable federal laws, Executive Orders, directives, policies, and standards. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. 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. Information is protected through a layered security approach which incorporates the use of secure authentication, access control, mandatory configuration settings, firewalls, Virtual Private Network (VPN), and encryption, where required. Internally within USPTO, data transmission confidentiality controls are provided by PTONet.
☐	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:
☒	No, notice is not provided.	Specify why not: The vendor (VBrick) will not permit a link to the USPTO privacy policy on the webpage where the PII is entered.

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: For members of the public, they can choose to enter any name or email address (whether valid or not) into the system. 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: For USPTO employees, the authorization process automatically passes the users name and USPTO email address to VRC via the USPTO computer used to access content.

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: USPTO employees and contractors consent to providing information for the primary purpose of acquiring access to applications and network during onboarding when they accept their USPTO PTONet credentials. VRC no longer collects PII from the public.
☐	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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: USPTO employees and contractors may login to MyUSPTO and update their PII held in their Account Profile. VRC no longer collects PII from the public.
☐	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

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 VBrick 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): 6/11/2024 ☐ 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 5 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).*

PII in VRC is secured using appropriate administrative, physical, and technical safeguards in accordance with the applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorize personnel. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access.

The security safeguards for the VRC meet the NIST SP 800-53 (Rev. 5) requirements set forth System Security Plan (SSP) and in the USPTO Cybersecurity Baseline Policy. The Security Plan specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the enhanced system. All systems are subject to monitoring that is consistent with applicable regulations, agency policies, procedures, and guidelines. The system is implemented with encryption (SSL). VRC is continually monitored to provide "near real-time" risk reporting and mitigation activities.

Management Controls:
a) The USPTO uses the Life Cycle review process to ensure that management controls are in place for VRC. During the enhancement of any component, the security controls are reviewed, reevaluated, and updated in the Security Plan. The Security Plans specifically address 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.

b) The USPTO uses the Personally Identifiable Data Extracts Policy. This means no extracts of sensitive data may be copied on to portable media without a waiver approved by the DOC Chief Information Officer (CIO).

Operational Controls:
a) Access to all PII/BII data is for users on PTONet who have verified access to VRC. Additionally, access to PII/BII data is restricted to a small subset of VRC users.

b) Manual procedures are followed for handling extracted data containing sensitive PII which is physically transported outside of the USPTO premises. In order to remove data extracts containing sensitive PII from USPTO premises, users must:

1. Maintain a centralized office log for extracted datasets that contain sensitive PII. This log must include the date the data was extracted and removed from the facilities, a description of the data extracted, the purpose of the extract, the expected date of disposal or return, and the actual date of return or deletion.
2. Ensure that any extract which is no longer needed is returned to USPTO premises or securely erased and that this activity is recorded on the log.
3. Obtain management concurrence in the log, if an extract aged over 90 days is still required.
4. Store all PII data extracts maintained on a USPTO laptop in the encrypted My Documents directory. This includes any sensitive PII data extracts downloaded via the USPTO VPN.
5. Encrypt and password-protect all sensitive PII data extracts maintained on a portable storage device (such as CD, memory key, flash drive, etc.). Exceptions due to technical limitations must have the approval of the Office Director and alternative protective measures must be in place prior to removal from USPTO premises.

USPTO is using the following compensating controls to protect PII data:

a) No extracts of sensitive data may be copied on to portable media without a waiver approved by the DOC CIO. The request for a waiver must include specifics as to how the data and device are protected, how long the data will be maintained, and how the data on the device will be deleted when no longer required.

All laptop computers allowed to store sensitive data must have full disk encryption.
VRC is secured by various USPTO infrastructure components, including the Network and Security Infrastructure (NSI) system and other OCIO established technical controls to include SAML 2.0 authentication to VRC. Web communications leverages modern encryption technology such as Transport Layer Security (TLS) 1.2 over Hypertext Transfer Protocol Secure (HTTPS).

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)*:
☐	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.)*

General Records Schedules (GRS) | National Archives

☒	There is an approved record control schedule. Provide the name of the record control schedule: GRS 3.2:010 Information Systems Security Records Systems and data security 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: For members of the public, they can choose to enter any name or email address (whether valid or not) into the system. Their name and email address are not verified or used for authentication. Due to the lack of verification and authentication, no members of the public can be definitively identified. For USPTO employees and contractors, a background investigation is done by the USPTO Security Office prior as part of the onboarding process. Therefore, all employees and contractor's names and email addresses are already identified in USPTO ICAM-IDaaS via Security Assertion Markup Language (SAML) 2.0. VRC only uses this already existing data.
☒	Quantity of PII	Provide explanation: VRC system personnel consider the quantity of PII (name and email address for USPTO employees and contractors; potential real name and email address [unverified] for members of the public) to be limited.
☒	Data Field Sensitivity	Provide explanation: VRC 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 non-sensitive PII.
☒	Context of Use	Provide explanation: Name and email address are collected and maintained in audit logs, and that information is only used to capture the total number of users that are viewing a live webcast or recorded video. The total number of users helps to improve Federal services online and as a way to measure employee satisfaction with the service. Members of the Public: Name, email address, and IP address are collected and maintained in audit logs, and that information is only used to capture the total number of connections that viewed a live webcast. The total number of connections helps to improve. Federal services online and as a way to measure satisfaction with the service.
☒	Obligation to Protect Confidentiality	Provide explanation: In accordance with NIST 800-53 Rev. 5, VRC implements both AR-2 (Privacy Impact and Risk Assessment) and AR-7 (Privacy-Enhanced System Design and Development) security controls to ensure all stakeholder's confidentiality is protected.
☒	Access to and Location of PII	Provide explanation: The non-sensitive Personally Identifiable Information in VRC is secured using appropriate administrative, physical and technical safeguards in accordance with the FedRAMP Li-SaaS Authorization. Authorized USPTO staff and contractors have access to the data stored on the VRC System. VRC does not disseminate PII information to any other systems.

☐	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.)

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 sensitive information to an acceptable level.

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.