Template Version Number: 01-2020

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

Privacy Threshold Analysis
for the
VBrick Rev Cloud (VRC)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO VBrick Rev Cloud (VRC)

Unique Project Identifier: PTOC-037-00

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 system (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).

VRC is a USPTO information system that utilizes the Vbrick Rev® Cloud® Service FedRAMP authorized system. The FedRAMP Vbrick Rev® Cloud® 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, Vbrick Rev® Cloud® Service includes the ability to interact and integrate with customer (USPTO) directory services and single sign on capabilities to provide authentication for internal or confidential content. That integration occurs via USPTO's VRC system.

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

VRC is a major application.

b) System location

The VBrick Rev® Cloud® Service FedRAMP system is located at 607 Herndon Parkway Suite 300, Herndon VA 20170. The USPTO VRC system is hosted on the hosted on the VBrick Rev® Cloud® Service, which utilizes the Amazon Web Services (AWS) cloud. All data and any accompanying 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)

VRC is a standalone system. VRC receives PII from USPTO RBAC via SAML 2.0.

d) The purpose that the system is designed to serve

VRC provides customers with the ability to serve live and on demand video to users.

e) The way the system operates to achieve the purpose

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

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

For public users, a display name, Internet Protocol (IP) address, and email address is collected and maintained; however, that information is not used to authenticate the public users (no authentication is required). The display name and email address that the public user enters is also not verified and it can be anything the user choses; such as:

- Display name: Fake Person
- Email address: fakeaddress@makebelieve.com

For USPTO internal users, name and email address are collected and maintained by the system. However, authentication occurs via Single-Sign-On once the user has previously authenticated to their PTONet account and only after the user acknowledges the USPTO warning banner. VRC does not use internal users' names and email addresses for authentication. VRC does not disseminate any information; rather, it provides a platform for webcast videos that disseminate information.

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

VRC administrators have access to the information collected and maintained from both public and USPTO internal users. However, as noted previously, the email addresses that public users enter do not have to be real email addresses and are not used to authenticate the users (no authentication is required). Internal USPTO and public users have access to live webcast videos and recorded videos.

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

Name and email address information is retrieved by VRC administrators via audit logs accessed through the VRC application. IP addresses are also collected via audit logs. USPTO internal and public users retrieve the videos via webcasts.

i) How information is transmitted to and from the system

Information is transmitted to and from the system via the VRC application. End users connect to VRC via their Internet Browser.

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): For members of the public, the interpretation of the data collected has resulted in a change to the determination of what constitutes PII. For USPTO employees, the collection of name and email address occurs due to the integration with USPTO Role-Based Access Control (RBAC); via Security Assertion Markup Language (SAML) 2.0.					

☐ 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 personally identifiable information (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 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 VBrick Rev Cloud (VRC) 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 VBrick Rev Cloud (VRC) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Randy Hill Office: Collaborative Services Division Phone: (571) 272-8983 Email: Randy.Hill@uspto.gov Signature: Users, Hill, Randy Digitally signed by Users, Hill, Randy Date: 2021.03.01 16:45:35 -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: DON R Watson Digitally signed by DON R Watson Date: 2021.03.02 11:11:35 -05'00' Date signed: _____
Privacy Act Officer Name: John Heaton Office: Office of General Law (O/GL) Phone: (571) 270-7420 Email: Ricou.Heaton@upsto.gov Signature: Users, Heaton, John (Ricou) Digitally signed by Users, Heaton, John (Ricou) Date: 2021.02.24 14:16:15 -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: 2021.03.03 11:54:19 -05'00' Date signed: _____
Co-Authorizing Official Name: N/A Office: N/A Phone: N/A Email: N/A Signature: _____ Date signed: _____	