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

JENNIFER GOODE Digitally signed by JENNIFER GOODE
Date: 2021.06.14 10:19:11 -04'00'

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

Unique Project Identifier: PTOC-037-00

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

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 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 Role-Based Access Control (RBAC) via Security Assertion Markup Language (SAML) 2.0.

(d) The way the system operates to achieve the purpose(s) identified in Section 4
VRC provides customers with the ability to serve live and on demand video to users. 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 in either 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 Software as a Service (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 conducted by the system
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.)

<table>
<thead>
<tr>
<th>Changes That Create New Privacy Risks (CTCNPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Conversions</td>
</tr>
<tr>
<td>b. Anonymous to Non-Anonymous</td>
</tr>
<tr>
<td>c. Significant System Management Changes</td>
</tr>
</tbody>
</table>

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.
☐ 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).

☐ 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).

**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.)*

<table>
<thead>
<tr>
<th>Identifying Numbers (IN)</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>b. Taxpayer ID</td>
<td>☐</td>
<td>g. Passport</td>
<td>☐</td>
<td>k. Financial Transaction</td>
</tr>
<tr>
<td>c. Employee ID</td>
<td>☐</td>
<td>h. Alien Registration</td>
<td>☐</td>
<td>l. Vehicle Identifier</td>
</tr>
<tr>
<td>d. Employee ID</td>
<td>☐</td>
<td>i. Credit Card</td>
<td>☐</td>
<td>m. Medical Record</td>
</tr>
<tr>
<td>e. File/Case ID</td>
<td>☐</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n. Other identifying numbers (specify):</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

<table>
<thead>
<tr>
<th>General Personal Data (GPD)</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Name</td>
<td>☒</td>
<td>h. Date of Birth</td>
<td>☐</td>
<td>o. Financial Information</td>
</tr>
<tr>
<td>b. Maiden Name</td>
<td>☐</td>
<td>i. Place of Birth</td>
<td>☐</td>
<td>p. Medical Information</td>
</tr>
<tr>
<td>c. Alias</td>
<td>☐</td>
<td>j. Home Address</td>
<td>☐</td>
<td>q. Military Service</td>
</tr>
<tr>
<td>d. Gender</td>
<td>☐</td>
<td>k. Telephone Number</td>
<td>☐</td>
<td>r. Criminal Record</td>
</tr>
<tr>
<td>e. Age</td>
<td>☐</td>
<td>l. Email Address</td>
<td>☒</td>
<td>s. Physical Characteristics</td>
</tr>
<tr>
<td>f. Race/Ethnicity</td>
<td>☐</td>
<td>m. Education</td>
<td>☐</td>
<td>t. Mother’s Maiden Name</td>
</tr>
<tr>
<td>g. Citizenship</td>
<td>☐</td>
<td>n. Religion</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>u. Other general personal data (specify):</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work-Related Data (WRD)</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Occupation</td>
<td>☐</td>
<td>e. Work Email Address</td>
<td>☒</td>
<td>i. Business Associates</td>
</tr>
<tr>
<td>b. Job Title</td>
<td>☐</td>
<td>f. Salary</td>
<td>☐</td>
<td>j. Proprietary or Business Information</td>
</tr>
<tr>
<td>c. Work Address</td>
<td>☐</td>
<td>g. Work History</td>
<td>☐</td>
<td>k. Procurement/contracting records</td>
</tr>
<tr>
<td>d. Work Telephone Number</td>
<td>☐</td>
<td>h. Employment Performance Ratings or other Performance Information</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>l. Other work-related data (specify):</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Distinguishing Features/Biometrics (DFB)

- Fingerprint☐
- Palm Prints☐
- Voice/Audio Recording☒
- Video Recording☐
- Photographs☐
- Other distinguishing features/biometrics (specify):

System Administration/Audit Data (SAAD)

- User ID☒
- IP Address☒
- Date/Time of Access☒
- Queries Run☐
- Contents of Files☐
- 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 Role Based Access 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.

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. 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.)

<table>
<thead>
<tr>
<th>Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Cards</td>
</tr>
<tr>
<td>Caller-ID</td>
</tr>
<tr>
<td>Other (specify):</td>
</tr>
</tbody>
</table>

☒ 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.)

<table>
<thead>
<tr>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio recordings</td>
</tr>
<tr>
<td>Video surveillance</td>
</tr>
<tr>
<td>Other (specify):</td>
</tr>
</tbody>
</table>

☐ 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.)

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>For a Computer Matching Program</td>
</tr>
<tr>
<td>For administrative matters</td>
</tr>
<tr>
<td>For litigation</td>
</tr>
<tr>
<td>For civil enforcement activities</td>
</tr>
<tr>
<td>To improve Federal services online</td>
</tr>
</tbody>
</table>
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 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) and EMSO systems provide 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.

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.)

<table>
<thead>
<tr>
<th>Recipient</th>
<th>How Information will be Shared</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Case-by-Case</td>
</tr>
<tr>
<td></td>
<td>Bulk Transfer</td>
</tr>
<tr>
<td></td>
<td>Direct Access</td>
</tr>
</tbody>
</table>
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:

VRC connects with USPTO RBAC via SAML 2.0 via the ESS system, as described in the ESS System Security Plan.

☐ 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.)*

<table>
<thead>
<tr>
<th>Class of Users</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>General Public</td>
<td>☐</td>
</tr>
<tr>
<td>Government Employees</td>
<td>☒</td>
</tr>
<tr>
<td>Contractors</td>
<td>☒</td>
</tr>
<tr>
<td>Other (specify)</td>
<td></td>
</tr>
</tbody>
</table>

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: __________________________. |
| ☐ | Yes, notice is provided by other means. Specify how: |
| ☒ | No, notice is not provided. Specify why not: The vendor (V Brick) 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 on boarding when they accept their USPTO PTONet credentials. For members of the public, the information provided is voluntary and not validated. |
| ☐ | 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. Public users have an opportunity to review/update PII before submitting the information. |
| ☐ | 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 FISMA requirements.
  Provide date of most recent Assessment and Authorization (A&A): 9/24/20
- ☐ 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 supporting 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 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.)*

The information system provides protection of resources in accordance with NIST 800-18 Rev. 1 and NIST 800-53 Rev. 4; the EVES 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 on the ESS data. 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 EVES Security Assessment Package as part of the system’s Security Authorization process.

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.
VRC is secured using appropriate administrative, physical and technical safeguards in accordance with the FedRAMP 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.

USPTO uses the Life Cycle review process to ensure that management controls are in place for EVES. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the System Security Plan. The System Security Plan 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 sensitive data.

EVES 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 TLS 1.2 over 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 and number (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.)

☒ 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:
10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

<table>
<thead>
<tr>
<th>Disposal</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Shredding</td>
<td></td>
<td>☒</td>
</tr>
<tr>
<td>Overwriting</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>Degaussing</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>Deleting</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>Other (specify)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels**

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.)*

<table>
<thead>
<tr>
<th>Impact Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>☒ Low</td>
<td>The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td>☐ Moderate</td>
<td>The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td>☐ High</td>
<td>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.</td>
</tr>
</tbody>
</table>

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>☒ Identifiability</td>
<td>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 boarding process. Therefore, all employees and contractor’s names and email addresses are already identified in USPTO Role-Based Access Control (RBAC) via Security Assertion Markup Language (SAML) 2.0. VRC only uses this already existing data.</td>
</tr>
<tr>
<td>☒ Quantity of PII</td>
<td>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.</td>
</tr>
<tr>
<td>☒</td>
<td>Data Field Sensitivity</td>
</tr>
<tr>
<td>☒</td>
<td>Context of Use</td>
</tr>
<tr>
<td>☒</td>
<td>Obligation to Protect Confidentiality</td>
</tr>
<tr>
<td>☒</td>
<td>Access to and Location of PII</td>
</tr>
<tr>
<td>☐</td>
<td>Other:</td>
</tr>
</tbody>
</table>

**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. |
## USPTO Points of Contact and Signatures

### System Owner
Name: Randy Hill  
Office: Collaborative Services Division  
Phone: (571) 272-8983  
Email: Randy.Hill@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:  
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:  
Date signed:  

---

### Privacy Act Officer
Name: John (Ricou) Heaton  
Office: General Law Office (GLO)  
Phone: (571) 270-7420  
Email: Ricou.Heaton@uspto.gov

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

Signature:  
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:  
Date signed:  

---

### Co-Authorizing Official (if applicable)
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.