Template Version Number: 01-2020

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

Privacy Threshold Analysis
for the
Rally Software: Rally Development System
(RDS)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Rally Software: Rally Development System (RDS)

Unique Project Identifier: PTOC-029-00

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 (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).

The Rally Development System (RDS) is a Contractor information system that serves as an Agile Platform and development tool for USPTO employees and projects. Rally allows USPTO developers to continuously track and prioritize work, reallocate development resources, collaborate between teams, and align strategy and development with the USPTO System Development Lifecycle (SDLC) and strategic roadmap. The RDS is externally hosted in GCP (Google Cloud Platform) and is available to USPTO users via a web interface.

a) ***Whether it is a general support system, major application, or other type of system***
The RDS is a major application.

b) ***System location***
Brocade Pkwy, Broomfield, CO 80021.

c) ***Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)***
RDS connects to OKTA. USPTO is leveraging OKTA IDaaS hosted within FedRAMP Certified Cloud to provide the enterprise services for the Identity and Access Management (IAM). The supporting components for the USPTO IAM services are located at the United States Patent and Trademark Office (USPTO). The system provides Identity Management (including user provisioning for the public), Authentication and coarse grained Authorization to the USPTO systems. This allows the USPTO user community, systems, and its employees to access the

resources provided by the organization while protecting those services from unauthorized access and/or individuals and systems.

d) ***The purpose that the system is designed to serve***
The RDS is an information system that serves as an Agile Platform and development tool for USPTO employees and projects.

e) ***The way the system operates to achieve the purpose***
RDS allows USPTO developers to continuously track and prioritize work, reallocate development resources, collaborate between teams, and align strategy and development with the USPTO System Development Lifecycle (SDLC) and strategic roadmap.

f) ***A general description of the type of information collected, maintained, used, or disseminated by the system***
The type of information collected, maintained, used, or disseminated by the system includes first and last names of USPTO personnel, project status and due dates, system requirements and milestones to complete project effort, and configuration settings.

g) ***Identify individuals who have access to information on the system***
Individuals who have access to the system are RDS administrators and USPTO End-Users.

h) ***How information in the system is retrieved by the user***
The RDS is externally hosted and is available to USPTO users via a web interface.

i) ***How information is transmitted to and from the system***
All data in transit is encrypted and all requests that are made will automatically be directed to HTTPS. Device management connections use SSH, PKI, and Secure ID VPN-based connections. User data connections use PKI and Secure ID VPN and SSL/TLS and only authorized USPTO systems may access the internal PTONet.

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): Collection of User ID, Names and Email addresses					

□ 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 PII?
As per OMB 17-12: “The term PII refers to information that can be used to distinguish or trace an individual’s identity either alone or when combined with other information that is linked or linkable to a specific individual.”

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

☒ DOC employees
☒ Contractors working on behalf of DOC
☐ Other Federal Government personnel
☐ Members of the public

☐ No, this IT system does not collect any PII.

If the answer is “yes” to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

☐ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

☒ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?
Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

☐ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☒ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ I certify the criteria implied by one or more of the questions above **apply** to the Rally Software: Rally Development System (RDS) 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 Rally Software: Rally Development System (RDS) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Melissa Rummel Office: Office of the Chief Information Officer (OCIO) Phone: (571) 270-0838 Email: Melissa.Rummel@uspto.gov Signature: Users, Rummel, Melissa Digitally signed by Users, Rummel, Melissa Date: 2021.09.23 16:14:21 -04'00' 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: 2021.09.27 13:43:09 -04'00' 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: 2021.09.10 08:48:13 -04'00' 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: Deborah Stephens Digitally signed by Deborah Stephens Date: 2021.09.27 14:32:37 -04'00' Date signed: ______________________________
Co-Authorizing Official Name: N/A Office: N/A Phone: N/A Email: N/A Signature: ______________________________ Date signed: ______________________________	