Template Version Number: 01-2020

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

Privacy Impact Assessment
for the
Rally Software: Rally Development System (RDS)

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 — 12/08/2021

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Rally Software: Rally Development System (RDS)

Unique Project Identifier: PTOC-029-00

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.

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

(e) 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.

(f) 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.

(g) Any information sharing conducted by the system

Data repositories allow information to be shared with internal stakeholders only. Rally Support Team has access to PII for technical support purposes upon customer request only. Rally Database Administrators have database access for technical support purposes only. The analytics team has access to performance-related data. Performance data does not contain PII. DevOps engineers have production-level access to metadata in the Mongo database. The metadata does not include PII.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

The legal authority to collect PII and/or BII derives from 5 U.S.C. 2, eGovernment Act, Clinger-Cohen, and Federal Information Technology Acquisition Reform Act (FITRA).

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

The Federal Information Processing Standard (FIPS) 199 security impact category for the system is 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): 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.

☐ 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.)*

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. Physical Characteristics	☐
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):					

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.

USPTO implements security and management controls to prevent the inappropriate disclosure of sensitive information. Security controls are employed to ensure information is resistant to tampering, remains confidential as necessary, and is available as intended by the agency and as expected by authorized users. Management controls are utilized to prevent the inappropriate disclosure of PII. Rally does not validate, manage, or share with 3rd party the USPTO user's data (First/Last Names and email addresses). The USPTO provides and manages PII on an individual basis or through a federated SSO. Rally does require an "email format" ID to procure the user onto the system. First/Last name is optional.

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):			

☒	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 data in RDS is about PTO employees as well as contractors. RDS must process PII to deliver its core features. RDS is responsible for setting up a Subscription with Subscription Administrator ID, email address, First and Last name. Rally Users login through their browser with a user ID (email format) and password. Also, the user's full name, persistent ID, and public IP address are processed. RDS uses personal information for setting up a USPTO Subscription with Subscription Administrator ID, email address, First and Last name. The USPTO is responsible to maintain subscription user base.

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.)

Insider threats and foreign entities are the main threat to the information system:
RDS Support Team has access to PII for technical support purposes upon customer request only.
RDS Database Administrators have database access for technical support purposes only.
RDS Super Administrators have subscription configuration access, including personal information for technical (procurement, licensing) support purposes.

The Segregation of Duties Policy is in place and enforced. RDS segregation of duties include logical access controls. Access logged and monitored. RDS storing data in PostgreSQL DB with AES-256 disk-level encryption. All data-in-transit is encrypted with TLS 1.2

RDS has Privacy and Data Protection Policy, PII Handling and Protection Policy
Annual Privacy and Data Protection training is mandatory for all employees and contractors.
Annual Security Awareness training is mandatory for all employees and contractors.

USPTO has implemented NIST security controls (encryption, access control, auditing) to reduce the insider threat risk. Mandatory IT Awareness and role-based training is required for staff who have access to Rally. Users are taught how to handle, retain, and dispose of data properly, and reporting requirements for potential insider threat, incidents, or breaches.

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: OKTA USPTO Active Directory for internal users (USPTO employees and contractors) is connected to the IT system. Technical controls are in place to address security concerns. Least privilege access policies and controls are in place. All information is encrypted during transmission and at rest, users and administrator are required to take security awareness training. Audit records are captured and

	periodically reviewed. Identity governance system is in place to manage and enforce security controls related to AC, AU, and IA.
☐	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: http://www.uspto.gov/privacy-policy	
☒	Yes, notice is provided by other means.	Specify how: See Appendix A
☐	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:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: USPTO Employees and Contractors do not have the opportunity to decline to provide their PII. They consent to providing their name (which is then used for the email address) and phone number as part of accepting employment at USPTO. That information is then used for the primary purpose of acquiring access to applications and the network during on boarding.

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:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: USPTO Employees and Contractors do not have the ability to consent to particular uses of their PII. They consent to providing their name (which is then used for the email address) and phone number as part of accepting employment at USPTO. That information is then used for the primary purpose of acquiring access to applications and the network during on boarding.

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 update their information (name, preferred name) by submitting changes to Human Resources.
☐	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: Auditing and Monitoring is in place and enforced.
☒	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): 04/30/2021 ☐ 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).*

Access logged and monitored through Splunk. RDS storing data in PostgreSQL DB with AES-256 disk-level encryption. All data-in-transit is encrypted with TLS 1.2. All VM's has end-point protection, ClamAV and Symantec. Data backed up daily. Backups are securely replicated to an alternative location limiting data loss to no more than 24 hours in the event of primary data location disaster. Backups are stored locally and off-site with the same security and encryption mechanism. Backups are tested monthly. -RPO: 4 hours -RTO: 24 hours

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-25 Access Control and Identity Management System
☐	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 3.1: 001-051; General Technology Management Records GRS 6.3: 010; Information Technology program and capital investment planning records.

	GRS 6.3: 020; Enterprise architecture 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: Name, alias and work email address are PII that can be combined to identify individuals.
☒	Quantity of PII	Provide explanation: The PII collected is commensurate with the number of subscribed Rally users at USPTO, the number of which is in the thousands.
☒	Data Field Sensitivity	Provide explanation: Together, the fields of Subscription Administrator ID, email address, First and Last name is non-sensitive.
☒	Context of Use	Provide explanation: RDS uses PII for setting up a USPTO Subscription with Subscription Administrator ID, email address, First and Last name.
☒	Obligation to Protect Confidentiality	Provide explanation: This system is governed by The Privacy Act of 1974, which prohibits the disclosure of information from a system of records absent of the written consent of the subject individual.
☒	Access to and Location of PII	Provide explanation:

		Access to PII (user information, user ID and email address) is controlled through Segregation of Duties access controls vis role based access controls. Privileged users are the only one that have control to provision users within the system.
☐	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.)

Insider threats and foreign entities are the main threat to the information system:
RDS Support Team has access to PII for technical support purposes upon customer request only.
RDS Database Administrators have database access for technical support purposes only.
RDS Super Administrators have subscription configuration access, including personal information for technical (procurement, licensing) support purposes.

The Segregation of Duties Policy is in place and enforced. RDS segregation of duties include logical access controls. Access logged and monitored. RDS storing data in PostgreSQL DB with AES-256 disk-level encryption. All data-in-transit is encrypted with TLS 1.2

RDS has Privacy and Data Protection Policy, PII Handling and Protection Policy
Annual Privacy and Date Protection training is mandatory for ALL employees.
Annual Security Awareness training is mandatory for ALL employees.

Rally does require an "email format" ID to procure the user onto the system. First/Last name is optional.
Business Information collected for Support and Procurements purposes. The potential loss of this data will expose the current list of Rally users, including their email addresses and first and last names.

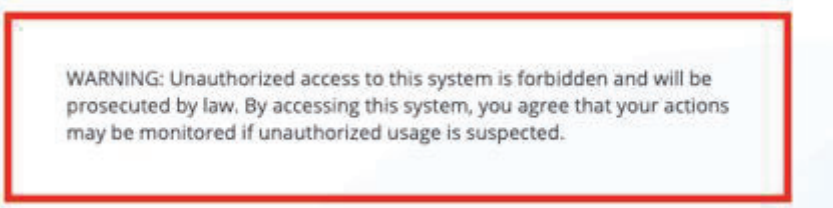
12.2 Indicate whether the conduct of this PIA results in any required business process changes.

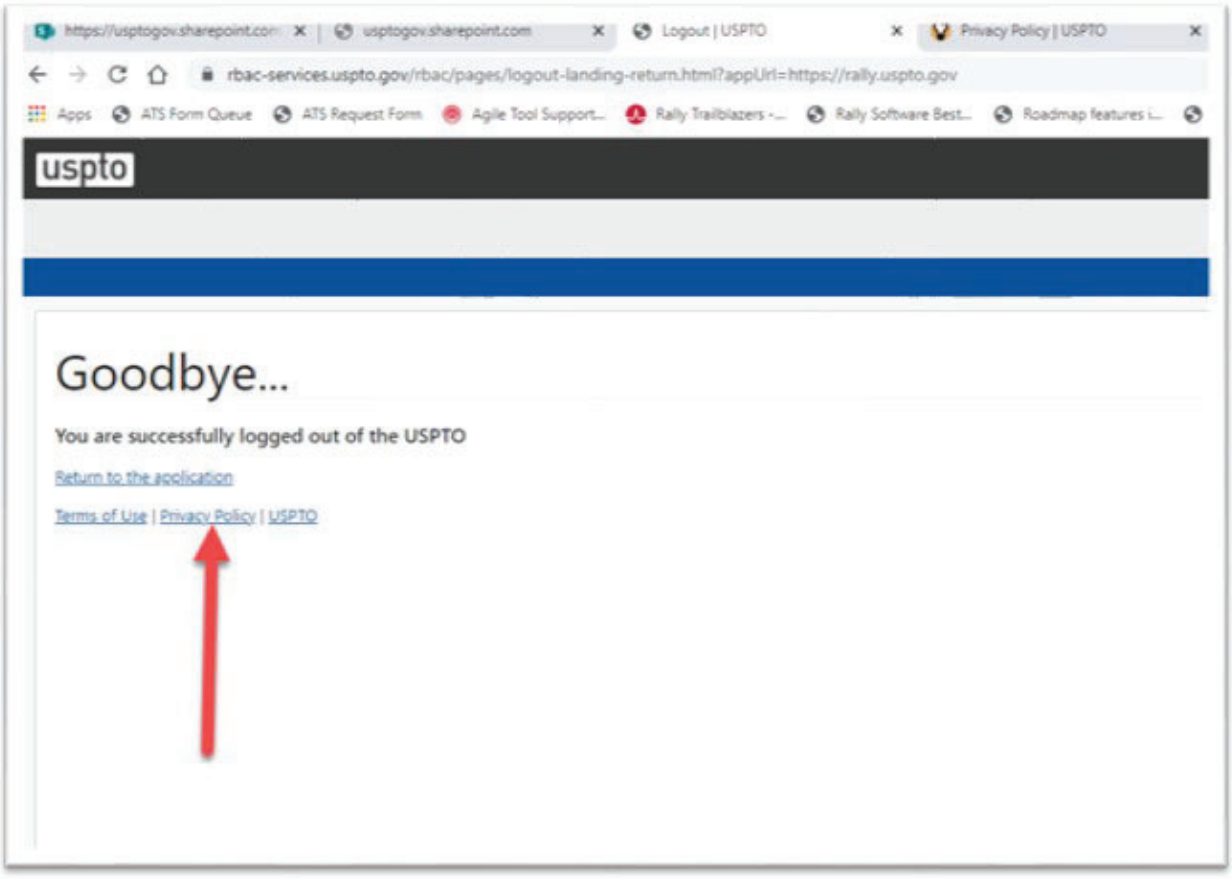
☐	Yes, the conduct of this PIA results in required business process changes. Explanation:
☒	No, the conduct of this PIA does not result in any required business process changes.

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.

Appendix A


WARNING: Unauthorized access to this system is forbidden and will be prosecuted by law. By accessing this system, you agree that your actions may be monitored if unauthorized usage is suspected.


usptogov.sharepoint.com
Logout | USPTO
Privacy Policy | USPTO
rbac-services.uspto.gov/rbac/pages/logout-landing-return.html?appUrl=https://rally.uspto.gov
Apps
ATS Form Queue
ATS Request Form
Agile Tool Support...
Rally Trailblazers -...
Rally Software Best...
Roadmap features i...
uspto
Goodbye...
You are successfully logged out of the USPTO
Return to the application
Terms of Use | Privacy Policy | USPTO