Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
SCS-SaaS-RegScale (RegScale)

Reviewed by: Deborah Stephens, 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

NICHOLAS CORMIER Digitally signed by NICHOLAS CORMIER Date: 2026.08.07 08:52:38 -04'00' 8/7/2026

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO SCS-SaaS-RegScale (RegScale)

Unique Project Identifier: EIPL-SCS-04-00

Introduction: System Description

Provide a brief description of the information system.

The RegScale system is a cloud-based Governance, Risk and Compliance (GRC) solution, hosted on Microsoft Azure Federal Risk and Authorization Management Program (FedRAMP) High Software-as-a-Service (SaaS) offering. It helps the United State Patent and Trademark Office (USPTO) automate and manage its cybersecurity and compliance requirements. It simplifies the Assessment and Authorization (A&A) process by providing a single platform where system stakeholders can track security controls, submit documentation, and monitor systems readiness for operation. RegScale supports traditional Authority to Operate (ATO) as well as USPTO Continuous Authorization to Operate (cATO) effort by automating tasks and providing nearly real-time system reports.

Address the following elements:

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

RegScale is a SaaS solution.

(b) System location

Alexandria, Virginia

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

RegScale system integrates internally with the following United States Patent and Trademark Office systems:

ICAM Identity as a Service (ICAM-IDaaS) - provides an enterprise authentication and authorization service to all applications.

Identity Management Authenticator (ID-AUTH) - personalizes the management of the smart card identification credentials under HSPD-12, issuance and management of the Rivest–Shamir–

Adleman (RSA) authentication tokens and issuance and management of Identity-based Public Key Infrastructure (IPKI) digital certificates.

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

Security and Compliance Services (SCS) - contains 5 subsystems which provide enterprise-wide security and compliance capability for all USPTO systems.

Enterprise Software Services (ESS)- is a major application and provides an architecture capable of supporting current software services at USPTO. ESS provides a centralized solution for assisting developers in building applications unique to the organization. The software implemented is intended to solve an enterprise-wide problem, rather than specific departmental issues. Enterprise level software aims to improve the enterprise's productivity and efficiency by providing business logic and support functionality, continuous collaborative and communication tools for organizational personnel to complete their everyday task.

UACS-USPTO AWS Cloud Services (UACS)- is an infrastructure platform used to support PTO Product Team Components hosted in the Amazon Web Services (AWS) East/West environment. The AWS East/West environment is comprised of several sub-components including, Virtual Private Cloud (VPC), Elastic Cloud Computing (EC2), Identity and Authentication Management (IAM), and Simple Storage Service.

Cyber Security Assessment and Management (CSAM)- is a Governance, Risk and Compliance (GRC) tool used to support the A&A process. It is utilized by USPTO to manage system security documentation, track risk posture, and ensure compliance with federal cybersecurity requirements.

Agile Delivery Platform (ADP)- is an integrated software engineering development solution that includes a central artifacts repository, version control, automated compile, build, test reporting, metering and analytics that can be built in AWS cloud. This allows for the continuous delivery of production ready codes to the various testing environments prior to promotion for the production.

Microsoft Office 365 (M365) - the M365 product of the Enterprise Infrastructure Product Line (EIPL) provides communication and collaboration tools and services using Microsoft Office 365. It provides support and is responsible for the core infrastructure of Office 365 including Exchange Online, SharePoint Online, OneDrive, TEAMS, and Office Services. Each Service Team is responsible for the configuration and feature settings within their perspective Service.

Service Management Platform (SMP)- is a cloud-based IT services management (ITSM) tool that provides a single system of record for IT services, operations, and business management by automating IT service applications and processes. USPTO uses the SMP to track and manage IT Service Desk incidents, problems, and change requests, with enhanced functionality to meet the growing IT service management requirements from across the enterprise. It specializes in ITSM by providing the infrastructure needed to perform data collection, storage, as well as application development on a single platform. The SMP capabilities include different cloud service models which are SaaS (Software as a Service), IaaS (Infrastructure as a Service) & PaaS (Platform as a Service). USPTO uses SMP as a SaaS.

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

RegScale operates as a secure, web-based platform accessed through a designated Uniform Resource Locator (URL) authenticated via ICAM-IDaaS. Once logged in, authorized USPTO employees and contractors navigate through an intuitive interface that allow them to review security data, monitor system security posture, and manage the A&A process through integrated workflows. Role-based access control ensure users can only view and modify information relevant to their roles, while encryption and comprehensive audit logging protect all activities and support accountability.

The system integrates with the USPTO Continuous Integration / Continuous Delivery (CI/CD) pipeline, Continuous Diagnostics and Mitigation (CDM) tools, Security Information and Event Management (SIEM) systems, vulnerability scanners, and the cloud platforms to automate and streamline both the A&A process and the System Development Life cycle (SDLC). These integrations eliminate redundancy, digitalize workflows, predict adherence to security control requirements and validate the security posture of systems. Additionally, the modular design of the system enables users to effectively document, track and manage key A&A artifacts to ensure continuous compliance and support for the cATO goals.

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

Information is retrieved by users through secure web interface and API integration. Authenticated users access the web interface by providing their credentials, enabling role-based access to data and system functionalities. Once logged in, users are able to navigate and view information in RegScale based on their role-based access.

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

Information is transmitted to and from the RegScale system after user authentication through the web interface or via API communication. Authenticated users send and receive data securely,

while APIs handle system-system data exchange using tokens. There are no external or public users of the RegScale as the system can only be accessed while on the USPTO network via ICAM-IDaaS.

(g) Any information sharing

The RegScale system integrates with various internal systems to support the USPTO's cATO capability. All connected systems have been granted ATO by the USPTO, and data is protected through strict access control and encryption. The information that may be shared pertains to cATO data associated with any system leveraging RegScale to support its A&A process. This may include control implementation data, logging information, compliance data, among others. Additionally, information may be shared on a case-by-case basis within the bureau, with DOC to meet Continuous Diagnostic and Mitigation (CDM) requirements, and with Federal agencies.

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

Citation of the legal authority to collect PII is 5 U.S.C. 301 and 35 U.S.C.2; EO 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.

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

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):					

☐ 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):					

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.

RegScale ensures the information is accurate by obtaining the information directly from the individual with whom the information pertains. The system is secured using appropriate administrative physical and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, and auditing). Mandatory IT awareness and role-based training is required for staff who have access to the system and address how to handle, retain, and dispose of data. All access has role-based restrictions and individuals with privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random, periodic reviews (quarterly) to identify unauthorized access and changes as part of verifying the integrity of administrative account holder data and roles. Inactive accounts will be deactivated and roles will be deleted from the application.

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): 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): To support the A&A activities of USPTO systems.			

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 information in this system is about federal employees and contractors and is used for administrative matters. Information pertaining to the assigned Point of Contact (POC) for each USPTO systems utilizing the RegScale system as a GRC tool is recorded in the POC section of the tool. This information includes, but is not limited to, user IDs, work phone numbers, email addresses and job titles.

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.)

In the event of computer failure, insider threats, or attack against the system by adversarial or foreign entities, any potential PII data stored within the system could be exposed. To avoid a breach, the system has certain security controls in place to ensure the information is handled, retained, and disposed of appropriately. Access to individual's PII is controlled through the application, and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. These audit trails are based on application server out-of-the-box logging reports reviewed by the Information System Security Officer (ISSO) and System Auditor and any suspicious indicators such as browsing will be immediately investigated and appropriate action taken. Also, system users undergo annual mandatory training regarding appropriate handling of information.

NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

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: SMP M365 CSAM ICAM-IDaaS ID-AUTH ESS UACS NSI SCS NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.
☐	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 privacy policy. The privacy policy can be found at: https://www.uspto.gov/privacy-policy	
☒	Yes, notice is provided by other means.	Specify how: This PIA serves as a notice
☐	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: Users of USPTO systems do not have the opportunity to decline to provide PII as it is necessary for the operation of the system and as it is a part of their job duties.

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: Individuals do not have the opportunity to consent to particular uses of their PII/BII in this system as it is required for the purpose of this system.

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: The information collected is entered by the individuals themselves by their designated representatives, at which time, the information is reviewed and updated as necessary.

☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Some RegScale users are only granted access to perform specific functions. They do not have the privilege required to update their information. In such cases, a designated POC with the appropriate access right will assist in making the necessary update.

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: audit logs
☒	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): 10/29/2025 ☐ 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).*

The information within the RegScale system is secured using appropriate management, operational, and technical safeguards in accordance with NIST requirements. Such management controls include a review process to ensure that management controls are in place and documented in the System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII/BII data to a small subset of users. 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 system maintains an audit trail and the

appropriate personnel is alerted when there is suspicious activity. Data is encrypted in transit and at rest.

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)*: 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.)*

General Records Schedules (GRS) | National Archives

☒	There is an approved record control schedule. Provide the name of the record control schedule: GRS 3.1: General Technology Management Records Item - 020 Information technology operations and maintenance records. Which include access and audit logs.

	GRS 3.2. Information Systems Security Records, Item 010, 020, 035 031. 040, 050 Which include system security logs. and access logs
☐	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: The information collected by the RegScale system, including email address, phone members, user IDs, work address could be used to identify an individual.
☒	Quantity of PII	Provide explanation: The information is collected and entered by the user or a designated representative at which point it is validated for accuracy and completeness. At this time, the estimated number of users for the RegScale system is 150.
☒	Data Field Sensitivity	Provide explanation: The data collected is limited to work phone number, email addresses, user IDs and addresses, which are not considered sensitive PII and, therefore do not increase the

		sensitivity level of the data fields.
☒	Context of Use	Provide explanation: The PII data collected is used solely to identify the designated POCs for each system that utilizes the RegScale to support and facilitate its cATO activities.
☒	Obligation to Protect Confidentiality	Provide explanation: Based on the data collected, USPTO must protect the PII of each individual in accordance with 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: The servers are hosted within a high-sensitivity Azure zone protected with firewalls and network segmentation. Strict logical and physical access controls, including Access Control Lists (ACLs) and need-to-know restrictions, are enforced to prevent unauthorized access. Additionally, all data is encrypted at rest to protect sensitive information from unauthorized disclosure.
☐	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.)

In the event of computer failure, insider threats, or attack against the system, any potential PII data from USPTO employees or contractors stored within the system could be exposed. System users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zone within the cloud and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized accounts. USPTO monitors, in real-time, all activities and events within the servers storing the potential PII data and personnel review audit logs received on a regular bases and alert the appropriate personnel when inappropriate or unusual activity is identified.

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.