Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
USPTO Google Cloud Platform Services (UGCS)

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

Digitally signed by BRIAN ANDERSON
Date: 2026.02.26 06:43:43 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO USPTO Google Cloud Platform Services (UGCS)

Unique Project Identifier: EIPL-IHSC-02-00

Introduction: System Description

Provide a brief description of the information system.

The United States Patent's and Trademark Office (USPTO), USPTO's Google Cloud Service, UGCS Infrastructure as a Service (IaaS) is a standard infrastructure platform, located in Google Cloud Platform (GCP) services used to support the USPTO's Platform as a Service (PaaS) Tenants. The GCP US-East4 environment is comprised of several sub-components including, Virtual Private Cloud (VPC networks), Cloud Computing (GCP Compute Engine), Identity and Authentication Management (IAM), and resilient cloud storage (GCP Cloud Storage).

Address the following elements:

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

UGCS is USPTO's UGCS IaaS cloud Platform, that is used to support the USPTO PaaS Tenants.

(b) System location

Primary location is GCP US East Region (McLean, VA)

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

UGCS hosts PaaS Tenants and maintains direct network connection and inheritance relationships with the following USPTO systems:

- **USPTO Azure Cloud Services (UMACS):** The UMACS is a cloud infrastructure platform used to support USPTO Application Information Systems hosted in the Azure East/West environment. The Azure East/West environment is comprised of several sub-components including, Virtual Private Network (vNet) Cloud Computing, Identity and Authentication Management (AAD), and Azure Managed Disks. These services are explained in greater detail below and further in the Azure East/West IaaS SSPPP.

- **Google Cloud Platform (GCP):** Google CSP (Cloud Service Provider), home of USPTO's UGCS offering for applications running in the Google Cloud.

- **ICAM Identity as a Service (ICAM-IDaaS):** The mission of the ICAM-IDaaS is to provide an enterprise authentication and authorization service to all applications/AIS's. As part of the enterprise services, it will also provide compliance for some of the NIST 800-53 controls (e.g. Access Control (AC), Audit and Accountability (AU)). The system provides following services to the enterprise: User Provisioning and Life Cycle Management, User Roles and Entitlement Management, User Authentication & Authorization to protected resources, application Integration/Protection, NIST controls compliance related to AU, AC, and Identification and Authentication (IA) family

- **Identity Management Authenticator (ID-AUTH):** Provides for PIV Card users network authentication. All USPTO users must use PIV card and/or equivalent multi-factor authentication. Privileged users access the USPTO network through authentication to the USPTO domain with the use of PIV Card + PIN, and the permissions to the application are role based and granted to the certificate on the user's PIV card. Authentication is performed using the PIV card. PIV Card and PIN are used for authentication to privilege accounts. These information systems inherit identification and authentication system remote access controls from AD accounts supplied by ESS. In order to gain access to privileged accounts, the administrator must have an AD username and an active RSA token. This provides multi-factor authentication for the system.

- **Enterprise Software Services (ESS):** ESS system provides an architecture capable of supporting current software services as well as providing the necessary architecture to support growth. ESS - EDS to serve the USPTO enterprise with use of System Center Configuration Manager (SCCM) drive accounts management issues with the Service Desk/Accounts Management team. The Accounts Management team reviews the report and creates ITSM tickets to manage accounts and equipment.

- **UACS-USPTO AWS Cloud Services (UACS):** The UACS General Support System (GSS) is an infrastructure platform, infrastructure as a service, used to support PTO Product Team Components, hosted in the 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), Simple Storage Service and other Fed Ramp approved services.

  These services are explained in greater detail below and further in the UACS System Description, UACS SSPP, and/or the AWS East/West IaaS SSPP.

- **Network and Security Infrastructure System (NSI):** The NSI system provides an architecture capable of supporting network and security infrastructure and services to USPTO systems, including routing, firewalls, and participation in the USPTO Security Monitoring stack with SCS.

- **Secure Access Service Edge (SASE):** The USPTO users of Netskope use their PIV credentials to authenticate to the NGC web administration console interface through strict enforcement of MFA on the system. The SASE system utilizes Security Assertion Markup Language (SAML) to prove SSO/PIV card authentication is enforced.

- **Security and Compliance Services (SCS):** SCS provides Security Incident and Event Management, Enterprise Forensic, Enterprise Management System, Security & Defense, Enterprise Scanner, Enterprise Cybersecurity Monitoring Operations, Performance Monitoring Tools, Dynamic Operational Support Plan, & Situational Awareness and Incident Response.

- **Patent Search AI (PSAI):** combines Artificial Intelligence (AI) Technologies that are specifically custom-made machine learning (ML) models, cloud-based deployments and user experience development integrated with Patent End to End (PE2E) Search.

- **Trademark Next Generation (TMNG)**: application information system that provides support for the automated processing of trademark applications for the USPTO. Patent Search AI (PSAI): combines Artificial Intelligence (AI) Technologies that are specifically custom-made machine learning (ML) models, cloud-based deployments and user experience development integrated with Patent End to End (PE2E) Search

- **Website Management Branch (WMB)**: application information system that provides support for the management and updating of Websites for the USPTO.

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

The UGCS Infrastructure-as-a-Service (IaaS) provides administrative efficiency and improved security to the USPTO Platform-as-a-Service (PaaS) Tenants that are hosted on the UGCS IaaS platform. The system provides a central location for where all USPTO GCP baseline infrastructure services used by the USPTO PaaS Tenants can be operated, managed, and monitored. UGCS also provides the ability to improve the facilitation of application development by offloading developers' non-core competencies to the operations and maintenance team supporting UGCS. Essential services such as user account administration, access control, networking infrastructure, logging and the UGCS platform and their support team will address monitoring, standardized server images, and the support of those components.

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

Cleared USPTO/UGCS IaaS personnel access their work space through the UGCS console. Individual product teams have segregated access and interaction methods that exist in separate ATO boundaries. UGCS does not have any direct retrieval of the information within the PaaS tenants.

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

Cleared USPTO/UGCS IaaS personnel work through access to the UGCS console. Any transmission of information between user and the applications/databases is segregated and handled at the PaaS level by individual Product Teams with separate ATOs.

(g) Any information sharing

UGCS IaaS support personnel work in the UGCS boundary, which does not have applications or databases that transact sensitive BII or PII. Applications and databases are hosted in Tenant PaaS system boundaries, where they have their own ATO and FISMA reporting requirements.

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

Please refer to the PIAs of the systems listed in the interconnections, section c of this PIA.

(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 system is getting a PIA due to an agreement with DOC and USPTO on a new understanding of when a					

system needs a PIA.

☒ 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): UGCS host PaaS Tenants who have their own PTA/PIA and FISMA reporting responsibilities, UGCS PIA has been conducted to account for their migrations.					
UGCS IaaS is a standard infrastructure platform located in Google Cloud Platform Services (GCP), is a Cloud Services Provider (CSP) used to support the USPTO's Platform as a Service (PaaS) Tenants. Sensitive BII/PII data is handled at the Tenant's application (component) level.					

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. Sex	☐	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): UGCS IaaS is a standard infrastructure platform located in Google Cloud Platform Services (GCP), is a Cloud Services Provider (CSP) used to support the USPTO's Platform as a Service (PaaS) Tenants. Sensitive BII/PII data is handled at the Tenant's application (component) level.					

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	☐		
Other work-related data (specify): UGCS IaaS is a standard infrastructure platform located in Google Cloud Platform Services (GCP), is a Cloud Services Provider (CSP) used to support the USPTO's Platform as a Service (PaaS) Tenants. Sensitive BII/PII data is handled at the Tenant's application (component) level.					

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): UGCS IaaS is a standard infrastructure platform located in Google Cloud Platform Services (GCP), is a Cloud Services Provider (CSP) used to support the USPTO's Platform as a Service (PaaS) Tenants. Sensitive BII/PII data is handled at the Tenant's application (component) level.					

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):
Please refer to the PIAs of the interconnected systems listed in section c of this PIA.

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): Please refer to the PIAs of the interconnected systems listed in section c of this PIA.					

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	☐	Other Federal Agencies	☐
State, Local, Tribal	☐	Foreign	☐		
Other (specify): Please refer to the PIAs of the interconnected systems listed in section c of this PIA.					

Non-government Sources					
Public Organizations	☐	Private Sector	☐	Commercial Data Brokers	☐
Third Party Website or Application			☐		
Other (specify): Please refer to the PIAs of the interconnected systems listed in section c of this PIA.					

2.3 Describe how the accuracy of the information in the system is ensured.

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. For the audit data that the UGCS system collects, access control restrictions are in place and principle of least privilege in maintained to ensure only authorized individuals have access to audit log files.

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.

Additionally, UGCS is an IaaS that is used to support USPTO. Access to the systems hosted in UGCS is handled at the application (component) level. The data stored within Tenant boundaries is not visible by UGCS Administrators and is based on the application (component) that sits on the UGCS IaaS rail for its services. The UGCS Administrators manage IaaS operating systems, systems software, image builds, patching, and the availability of services. Tenant teams manage their own BII/PII requirements, in segregated environments.

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.

	Some of the systems that use UGCS may be subject to the Paperwork Reduction Act. To obtain more information on these systems Paperwork Reduction Act please refer to the PIAs of the systems listed in the interconnection section c of this PIA.

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): Please refer to the PIAs of the interconnected systems listed in section c of this PIA.

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).

UGCS IaaS is a standard infrastructure platform hosted in Google Cloud Platform Services (GCP), is a Cloud Services Provider (CSP) used to support the USPTO's Platform as a Service (PaaS) Tenants. Sensitive BII/PII is handled at the application (component) level. UGCS host PaaS Tenants who have their own PTA/PIA at FISMA reporting responsibilities, UGCS PIA has been conducted to account for their migrations. For more information on how each system uses the PII/BII, please refer to the PIAs of the interconnected systems listed in section c of this PIA.

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 attach 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):	☐	☐	☐
UGCS host PaaS Tenants who have their own PTA/PIA and FISMA reporting responsibilities, UGCS PIA has been conducted to account for their migrations. For more information on how information is shared for systems using UGCS, please refer to the PIAs listed in the interconnections section c of this PIA.			

☐	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: UGCS hosts PaaS Tenants and maintains direct network connection and inheritance relationships with the following USPTO systems: • **UMACS** • **GCP** • **ICAM-IDaaS** • **ID-AUTH** • **ESS** • **UACS** • **NSI** • **SASE** • **SCS** • **PSAI** • **TMNG** • **WMB** * UGCS Product Team does have visibility into sensitive BII/PII in other FISMAs. This above is simply a list of UGCS interconnections. Please refer to the interconnections section c of this PIA to learn more information regarding the systems that utilize UGCS. 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 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: This PIA serves as 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.	UGCS host PaaS Tenants who have their own PTA/PIA and FISMA reporting responsibilities, UGCS PIA has been conducted to account for their migrations.

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.	UGCS host PaaS Tenants who have their own PTA/PIA and FISMA reporting responsibilities, UGCS PIA has been conducted to account for their migrations.

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: Tenants implement at the individual Product team level
☐	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: 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): 11/14/2025 ☐ 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): UGCS host PaaS Tenants who have their own PTA/PIA and FISMA reporting responsibilities, UGCS PIA has been conducted to account for their migrations.

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).*

PII within the 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)*:
☐	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. The applications (components) that UGCS provides services for may collect sensitive PII and/or BII in their own respective ATO boundaries. Please refer to the PIAs of the systems listed in the interconnections, section c for each system's applicable SORNs.

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:
☒	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: The applications (components) that UGCS provides services for may collect PII and/or BII and have it in UGCS. Please refer to the PIAs of the systems listed in the interconnections section c for the specific record retention schedules.
☐	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): The USPTO's UGCS IaaS does not own or transact data with physical disposal requirements. UGCS does not have visibility into the data disposal methods of USPTO's PaaS tenants that reside on UGCS. Please refer to the PIAs of the systems listed in the interconnections section c for the specific disposal methods of the PII/BII.			

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 combination of data from different sources and systems within the UGCS environment that contain PII or BII information.
☒	Quantity of PII	Provide explanation: UGCS stores large quantities of data that may contain PII from across the USPTO network
☒	Data Field Sensitivity	Provide explanation: PII stored in the system is data collected from applications (components) within UGCS. The information is confidential and unique to those systems.
☒	Context of Use	Provide explanation: UGCS IaaS is a standard infrastructure platform located in Google Cloud Platform Services (GCP), is a Cloud Services Provider (CSP) used to support the USPTO's Platform as a Service (PaaS) Tenants.
☒	Obligation to Protect Confidentiality	Provide explanation: Sensitive data is located across different sections of the UGCS environment. As an environment for

		applications across the USPTO network, UGCS must ensure only authorized systems and individuals have access to their information.
☒	Access to and Location of PII	Provide explanation: Data that may be used, stored, and transmitted by the Application Systems is centrally stored by UGCS. UGCS must ensure that only authorized systems and individuals have access to their data from this central storage system.
☒	Other:	Provide explanation: UGCS IaaS is a standard infrastructure platform located in Google Cloud Platform Services (GCP), is a Cloud Services Provider (CSP) used to support the USPTO's Platform as a Service (PaaS) Tenants.

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.)

The PII in this system poses a risk if 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 protected 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.