Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Cloudflare

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

BRIAN ANDERSON Digitally signed by BRIAN ANDERSON
Date: 2025.10.29 07:22:15 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Cloudflare

Unique Project Identifier: EIPL-IHSN-10-00

Introduction: System Description

Provide a brief description of the information system.

The Cloudflare Domain Name Service[3] (DNS), which come with a wide variety of security features built-in, including Domain Name System Security Extensions (DNSSEC), Distributed Denial of Service (DDoS) mitigation and multi-DNS functionality presents the capability to stop attacks on the DNS infrastructure. Cloudflare DNS is protecting all USPTO owned domain names. Cloudflare DNS service provides protection for United States Patent and Trademark Office (USPTO) infrastructure by defending against DDoS attacks, ensuring data integrity through DNSSEC support using technology as well as providing content filtration and malware defense.

Address the following elements:

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

Cloudflare is a major application and a Software as a Service (SaaS) solution.

(b) System location

USPTO is using the DNS service from Cloudflare and the DNS zones are being hosted at all of Cloudflares global Points of Presence[4] (PoPs). Cloudflare's authoritative DNS service, which contains only publicly accessible information, is served globally for all of its customers, include FedRAMP customers. Cloudflare processes and stores information related to account configuration and logs within Cloudflare's U.S.-based data centers, with the disaster recovery site in Europe. For the USPTO's FedRAMP Cloudflare the traffic is only processed and decrypted in the FedRAMP Authorization Boundary which is located in the U.S.-based data centers.

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

[3] DNS – The system by which internet domain names and addresses are tracked and regulated as defined by IETF RFC 1034 and other related RFCs

[4] PoPs – Where a system connects to the internet

Cloudflare Authoritative DNS is an authoritative DNS service powered by Cloudflare's global network of datacenters that offers the fastest response time, unparalleled redundancy, and advanced security with built-in DDoS mitigation and DNSSEC. When an end user queries a client's domain, Cloudflare's authoritative nameservers receive those queries, look up the relevant DNS record information about that domain ("DNSRecord") and return a DNS response, which may include the domain's Internal Protocol (IP) address, for the requested domain back to the recursive resolver.

Cloudflare actively interacts with service providers who serve as sub-processors and agree to provide the same level of protection and security provided to customers and users by Cloudflare.

Cloudflare provides a list of these sub-processors, along with their location and a description of the products using those sub-processors. This list is available HERE.

Logs about activity on the Cloudflare network are stored in our data centers in the United States and Europe.

ICAM Identity as a Service (ICAM-IDaaS): provides authentication and authorization services for Cloudflare. See section 6.3 for systems authorized to process PII or BII.

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

Cloudflare Authoritative DNS is an authoritative DNS service powered by Cloudflare's global network of datacenters that offers the fastest response time, unparalleled redundancy, and advanced security with built-in DDoS mitigation and DNSSEC. When an end user queries a client's domain, Cloudflare's authoritative nameservers receive those queries, look up the relevant DNS record information about that domain ("DNSRecord") and return a DNS response, which may include the domain's IP address, for the requested domain back to the recursive resolver.

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

USPTO employees who have access to the system log in through the Cloudflare Dashboard via Cloudflare | Web Performance & Security.

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

The information is transferred through secure zone transfer from USPTO external DNS appliance to Cloudflare.

(g) Any information sharing

Cloudflare actively interacts with service providers who serve as sub-processors and agree to provide the same level of protection and security provided to customers and users by Cloudflare.

Cloudflare provides a list of these sub-processors, along with their location and a description of the products using those sub-processors. This list is available HERE.

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

M-22-09 and Executive Order 14028

(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): PII is being collected by Cloudflare					

☐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): Internal unique identifiers					
*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. 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):					

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)
DNS records if the website owner inserted personal data into such records

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.

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):			

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).

Personal Data Categories	Types of Personal Data	Purpose for Processing
DNS Records	DNS records are structured data entries that map domain names to various resources on the internet, such as origin IP addresses (the IP address of a website, not an end user), mail servers, or other services. DNS records would not contain personal data unless the website owner inserted personal data into such records. They only contain domain-related data and do not include information that can identify an end user trying to access a customer's domain.	To provide the DNS Service
Realtime DNS Lookups	Realtime DNS Lookups include the source IP address of the incoming request to the customer's domain. The source IP address is most often that of a recursive resolver but could be an	To provide the DNS service by responding to end user DNS queries with DNS responses in order to route t Customer's domain name.

	end user's IP address.	
Customer DNS Logs	DNS query data as described above is included in service logs made available to customers.	• To provide customers with Customer Logs (i.e., DNS logs and DNS Analytics) for custom reporting and analytics purposes • Customers can view aggregate analytics in the dashboard / via API • Troubleshooting purposes
The following information is processed when customers sign up for a Cloudflare account and remains consistent across all of our products unless otherwise noted:		
Customer Account / Contact Information	• Administrator email address • Administrator name • Password • Billing contact names • Billing address • Internal unique identifiers	• Access to service • Configuration • Access controls • Security • Auditing and other data capture of service use • Billing • Contact: Marketing, T&S, configuration, support escalation
Administrative User Audit Logs	Administrative users are those with login credentials for a Cloudflare account and/or those who administer any of the Services for a Customer. Administrative user logs include Configuration information such as: • Administrator name • Policy settings (administrator name, IP address) • User Agent • Unique account ID	• Configuration Information is processed to log what policies were implemented and/or changed and who made the change • Provide information about the account
Support information	If a customer submits a support ticket related to our services, we may process the following information associated with the ticket: • First and last name • Email address • Phone number • Customer account information (Company name, street, city, state/region, country, Unique account ID)	• Remote access support • Review support service quality • Troubleshooting • Analysis of service

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.

Cloudflare has in place data processing addendums (DPAs) with vendors and sub-processors who process personal information on Cloudflare's behalf. Cloudflare chooses vendors and sub-processors carefully, conducting thorough assessments of their privacy and security practices before contracts are entered. Once a contract and DPA is in place, the extent of oversight of their compliance varies depending on the nature of the information being processed, the systems to which a sub-processor or vendor may have access, and other factors.

Vendors must also sign NDAs prior to engaging with Cloudflare.

Customers can subscribe to an RSS feed to receive alerts when Cloudflare adds or removes sub-processors. For more information on how RSS Feeds work, please see the following article: https://www.businessinsider.com/what-is-rss-feed .

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): Cloudflare sub-processors, as described here: https://www.cloudflare.com/gdpr/subprocessors/professional-services	☐	☐	☒

☐	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: ICAM-IDaaS 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: https://www.uspto.gov/privacy-policy	
☒	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.	Specify why not: The USPTO employee or contractor and any member of the public cannot decline to provide their PII/BII as it is needed to protect USPTO systems.

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: The USPTO employee or contractor and any member of the public cannot consent to particular uses of their PII/BII as it is needed to protect USPTO systems.

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 can review and update their PII within their Cloudflare account
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Members of the public do not have an opportunity to review/update PII/BII pertaining to them directly in this system as the information passes through Cloudflare but is not stored within Cloudflare.

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): 6/18/2024

	☐ 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).*

Cloudflare implements encryption to adequately protect personal data using state-of-the-art encryption protocols designed to provide effective protection against active and passive attacks with resources known to be available to public authorities, trustworthy public-key certification authorities and infrastructure, effective encryption algorithms and parameterization, such as a minimum of 128-bit key length of symmetric encryption, and at least 2048-bit RSA or 256-bit ECC key lengths for asymmetric algorithms.

Cloudflare enhances the security of processing systems and services in production environments by employing a code review process to increase the security of the code used to provide the Services and testing code and systems for vulnerability before and during use, maintaining an external bug bounty program, using checks to validate the integrity of encrypted data, and employing preventative and reactive intrusion detection. Additionally, Cloudflare deploys high-availability systems across geographically- distributed data centers. Cloudflare implements input controls measures to protect and maintain the confidentiality of personal data including an authorization policy for the input, reading, alteration and deletion of data, authenticating authorized personnel using unique authentication credentials (passwords) and hard tokens, automatically signing-out user IDs after a period of inactivity, protecting the input of data as well as the reading, alteration ad deletion of stored data, and requiring the data processing facilities are kept locked and secure.

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.

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: DAA-GRS-2013-0006-0003: System access records nor requiring special accountability for access
☐	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: Minimal PII is collected about members of the public, such as IP address the other PII mentioned in section 2.1 is regarding account provisioning.
☒	Quantity of PII	Provide explanation: Cloudflare has about 50 unique USPTO employee and/or contractor user accounts. For member of the public, USPTO has about 100,000 visitors a day to USPTO websites that would pass through Cloudflare.
☒	Data Field Sensitivity	Provide explanation: The PII being collected is not sensitive with most of it being publicly available PII.
☒	Context of Use	Provide explanation: The PII is being used for account management and to minimize USPTOs cybersecurity risk.
☒	Obligation to Protect Confidentiality	Provide explanation: USPTO privacy policy requires that PII information collected within the system to be protected in accordance with NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information.
☒	Access to and Location of PII	Provide explanation: The PII is restricted to select USPTO employees and contractors with Cloudflare accounts, Cloudflare and their sub processors. The PII for USPTO's Cloudflare instance is located in the United States with some of the PII located in countries that have substantially equivalent Privacy rights.
☐	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.)

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 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.