


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



Privacy Impact Assessment for the Google Analytics

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: 2025.11.04 12:04:32 -05'00'

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

Date

U.S. Department of Commerce Privacy Impact Assessment USPTO Google Analytics

Unique Project Identifier: Google Analytics

Introduction: System Description

Provide a brief description of the information system.

Google Analytics is a third-party server owned and managed by Google. It generates robust information about the public's interactions with United States Patent and Trademark Office (USPTO)'s public-facing website.

USPTO's use of Google Analytics is part of a paid contract and is subject to Google Analytics' [terms and conditions](#).

The primary account holder is the USPTO, which is responsible for ensuring appropriate use of Google Analytics. USPTO system product teams are responsible for ensuring appropriate use of Google Analytics on USPTO websites within their system boundary in accordance with applicable laws, regulations and USPTO policies. USPTO product teams are individuals assigned to ensure the overall management of the system they are assigned. Additionally, Google Analytics metrics are made publicly available through analytics.usa.gov, which is made available through General Services Administration (GSA). However, as this is not controlled by USPTO and it is up to GSA what data is displayed. USPTO makes no commitment that all Google Analytics data used by USPTO would be made available on this site.

Address the following elements:

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

Web analytics service. Software as a Service (SaaS)

(b) System location

Google's United States Cloud. Alexandria, VA

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

Interconnected to any USPTO:

TPS-ES (Trademark Processing System – external): is Major Application information system, and provides customer support for processing Trademark applications for USPTO.

OD/BD MS (Open Data/Big Data Master System): consists of subsystems which support the Big Data Portfolio.

RDMS (Reference Document Management System): is designed to serve as USPTO's enterprise-wide content management solution for reference and guidance documents – a critical tool for patent and trademark examiners and applicants.

OCCO-Web (Office Chief Communications Office Web): serves as the main web-based information dissemination channel for USPTO and provides links to public-facing, web-based applications used to conduct the Agency's day-to-day operations at www.uspto.gov.

SASE (Secure Access Service Edge): serves as an effective SASE solution at the USPTO for using Cloud Access Security Brokers (CASB), Secure Web Gateway (SWG) and Security as a Service (SecAAS) providers in keeping with the Trusted Internet Connection (TIC) 3.0 standard.

IPAS (Intellectual Property Assignment System): allows for electronic assignment of a patent or trademark via a website.

IDSS (Information Dissemination Support System): supports the Trademark and Electronic Government Business Division, the Corporate Systems Division, the Patent Search System Division, the Office of Electronic Information Products, and the Office of Public Information Services.

FPNG (Fee Processing Next Generation): is the fee management and revenue collection system at USPTO.

PC (Patent Center): is a next-generation Patents eCommerce application, used by patent practitioners, support staff, and independent inventors to file and manage patent applications.

TM-EXM (Trademark Exam): is a center where trademark attorneys and professional staff have the ability to securely login and complete end-to-end review and processing of trademark applications/registrations.

TTABC (Trademark Trial and Appeal Board Center): is an application information system, and provides an online interface for USPTO customers to submit forms to the Trademark Trial and Appeal Board (TTAB) electronically.

TMNG (Trademark Next Generation): is an application information system that provides support for the automated processing of trademark applications for the USPTO.

TM-External (Trademark External): is an electronic application filing system for USPTO Trademark. It provides the USPTO customers to electronically complete and submit a variety of trademark forms using a web-based user interface.

TPS-ES (Trademark Processing System – External): is a Major Application information system, and provides customer support for processing Trademark applications for USPTO.

MyUSPTO-C (MyUSPTO Cloud): is an external-facing web site application comprised of internal and external users. The purpose of the system is to reduce the number of logins for external USPTO customers and to provide a single location from where they can conduct their business with the USPTO.

IPLMSS (Intellectual Property Leadership Management Support System): provides capabilities and functionalities to support attorneys, litigation support personnel, USPTO staff, and the general public.

UGCS (USPTO Google Cloud Services): is a standard infrastructure platform used to support the USPTO's Patent Search Artificial Intelligence (AI) System, USPTO's future AI/Auto Machine Learning systems, and other USPTO Tenants, hosted in the Google Cloud Platform (GCP) us-east4, Northern Virginia, environment.

CFS (Consolidated Financial System): is a Master System composed of three (3) subsystems: Momentum, E-Acquisition (ACQ) and VendorPortal.

Momentum is a full-featured Commercial off-the-shelf (COTS) accounting software package that permits full integration of the processing of financial transactions with other normal business processes.

ACQ provides an automated solution for the procure-to-pay process in the acquisition community at the USPTO, allowing procurement users to create acquisition requests and track the life of procurement actions and documents associating with the plan.

The VendorPortal is a web-based COTS software based on the AEON platform developed by Distributed Solutions Inc. (DSI). The Vendor Portal provides a platform for interaction and information exchange between USPTO and the vendor community.

GPS (Global Patent Solutions System): is information system that provides support to USPTO patent review process. The purpose of this system is designed to support the USPTO international application or The Patent Cooperation Treaty (PCT) application process.

PPUBS (Patent Public Search): is a custom developed application information system provided by USPTO to replace legacy public search systems with a unified search system.

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

Google Analytics provides website traffic information through the use of first-party cookie(s) and a snippet of JavaScript on each webpage which transmits website traffic directly back to Google Analytics. The report Google Analytics provides USPTO only includes non-identifiable aggregated information. This allows the USPTO to view and analyze a variety of reports about how visitors interact on official websites without identifying visitors by their Internet Protocol (IP).

The USPTO privacy policy provides visitors with information on how to opt-out of having cookies dropped in the visitor's browser. The visitor will then be able to visit the USPTO website without information being processed on their visit.

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

USPTO employees and contractors who have been provided Google Analytics accounts will be able to log-in to Google Analytics to review and pull reports. Additionally, Google Analytics metrics are made publicly available through analytics.usa.gov, which is made available through General Services Administration (GSA). However, as this is not controlled by USPTO and it is up to GSA what data is displayed. USPTO makes no commitment that all Google Analytics data used by USPTO would be made available on this site.

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

IP addresses and log-in information for USPTO employees that have a Google Analytics account.

(g) Any information sharing

Google Analytics data is shared with GSA and is also made available to the public through GSA.

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

M-10-06, Open Government Directive (Dec. 8, 2009); M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies (June 25, 2010), and Memorandum on Transparency and Open Government (Jan. 21, 2009)

(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	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>	g. New Interagency Uses	<input type="checkbox"/>
b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input type="checkbox"/>	h. Internal Flow or Collection	<input type="checkbox"/>
c. Significant System Management Changes	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character of Data	<input type="checkbox"/>
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*	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
d. Employee ID	<input type="checkbox"/>	i. Credit Card	<input type="checkbox"/>	m. Medical Record	<input type="checkbox"/>
File/Case ID	<input type="checkbox"/>				
n. Other identifying numbers (specify): Property ID					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	<input type="checkbox"/>	h. Date of Birth	<input type="checkbox"/>	o. Financial Information	<input type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	i. Place of Birth	<input type="checkbox"/>	p. Medical Information	<input type="checkbox"/>
c. Alias	<input type="checkbox"/>	j. Home Address	<input type="checkbox"/>	q. Military Service	<input type="checkbox"/>
d. Gender	<input type="checkbox"/>	k. Telephone Number	<input type="checkbox"/>	r. Criminal Record	<input type="checkbox"/>
e. Age	<input type="checkbox"/>	l. Email Address	<input type="checkbox"/>	s. Marital Status	<input type="checkbox"/>
f. Race/Ethnicity	<input type="checkbox"/>	m. Education	<input type="checkbox"/>	t. Mother's Maiden Name	<input type="checkbox"/>
g. Citizenship	<input type="checkbox"/>	n. Religion	<input type="checkbox"/>		
u. Other general personal data (specify): Name of USPTO employees with an account to use Google Analytics, City and Country from where the site is being accessed, Language the browser or device accessing the site is set					

too

Work-Related Data (WRD)					
a. Occupation	<input type="checkbox"/>	e. Work Email Address	<input checked="" type="checkbox"/>	i. Business Associates	<input type="checkbox"/>
b. Job Title	<input type="checkbox"/>	f. Salary	<input type="checkbox"/>	j. Proprietary or Business Information	<input type="checkbox"/>
c. Work Address	<input type="checkbox"/>	g. Work History	<input type="checkbox"/>	k. Procurement/contracting records	<input type="checkbox"/>
d. Work Telephone Number	<input type="checkbox"/>	h. Employment Performance Ratings or other Performance Information	<input type="checkbox"/>		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	<input type="checkbox"/>	f. Scars, Marks, Tattoos	<input type="checkbox"/>	k. Signatures	<input type="checkbox"/>
b. Palm Prints	<input type="checkbox"/>	g. Hair Color	<input type="checkbox"/>	l. Vascular Scans	<input type="checkbox"/>
c. Voice/Audio Recording	<input type="checkbox"/>	h. Eye Color	<input type="checkbox"/>	m. DNA Sample or Profile	<input type="checkbox"/>
d. Video Recording	<input type="checkbox"/>	i. Height	<input type="checkbox"/>	n. Retina/Iris Scans	<input type="checkbox"/>
e. Photographs	<input type="checkbox"/>	j. Weight	<input type="checkbox"/>	o. Dental Profile	<input type="checkbox"/>
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>	e. ID Files Accessed	<input checked="" type="checkbox"/>
b. IP Address	<input checked="" type="checkbox"/>	f. Queries Run	<input type="checkbox"/>	f. Contents of Files	<input type="checkbox"/>
g. Other system administration/audit data (specify): General information regarding the device, web browser, Country and operating system accessing the site.					

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	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input checked="" type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input checked="" type="checkbox"/>		
Other (specify):					

Government Sources					
Within the Bureau	<input checked="" type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>

State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		
Other (specify):					

Non-government Sources					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input type="checkbox"/>		
Other (specify):					

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

<p>The accuracy of the information in the system is ensured by obtaining it directly from the individual with whom the information pertains.</p> <p>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.</p>
--

2.4 Is the information covered by the Paperwork Reduction Act?

<input type="checkbox"/>	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify): Click or tap here to enter text.			

<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	For administering human resources programs	<input type="checkbox"/>
For administrative matters	<input type="checkbox"/>	To promote information sharing initiatives	<input type="checkbox"/>
For litigation	<input type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>
For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input checked="" type="checkbox"/>	For employee or customer satisfaction	<input type="checkbox"/>
For web measurement and customization technologies (single-session)	<input checked="" type="checkbox"/>	For web measurement and customization technologies (multi-session)	<input type="checkbox"/>
Other (specify): USPTO uses the aggregated information to improve website management and functionality, and to improve visitor experiences and online services. The improved functionality will increase USPTO's ability to disseminate information to the public and enhance communication, facilitate feedback on USPTO programs, promote public participation and collaboration, and increase government transparency.			

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).

All the information indicated in section 2.1 except name and email address is collected by Google Analytics. USPTO does not receive this information in an identifiable form but through an aggregated report.

USPTO does not receive any of the PII collected by Google Analytics. Google provides the USPTO with reports with non-identifiable aggregated information regarding visitors to USPTO websites, which cannot be used to identify individuals. USPTO uses this aggregated information to measure and analyze website traffic to fulfil the purpose as stated in section 4.1.

Regarding the name and e-mail address there are collected by Google Analytics on USPTO employees and contractors who create Google Analytics accounts. This information is used for account management.

- 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.)

USPTO only requests Google Analytics to collect certain information about USPTO website usage. USPTO does not have access to any PII collected or maintained by Google Analytics for which they provide USPTO non-identifiable aggregated information on visitor interaction with USPTO websites. USPTO Google Analytics accounts are maintained by the Web Management Group, only authorized USPTO employees and contractors are able to access the aggregated data, which is controlled through password protections. Google Analytics is owned and operated by Google Inc., which is responsible for the effectiveness of the Google Analytics opt-out browser add-on function. Google Inc. is responsible for securing the data they collect as stated in the terms of use.

USPTO employees and contractors undergo annual mandatory training regarding appropriate handling of information.

USPTO systems that use Google Analytics have 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 adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.

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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
DOC bureaus	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private sector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

<input type="checkbox"/>	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?

<input type="checkbox"/>	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input checked="" type="checkbox"/>	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	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.

<input checked="" type="checkbox"/>	<p>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:</p> <p>List all systems that it interconnects with/pulls data from</p> <p>TPS-ES OD/BD MS OCCO-Web SASE IPAS IDSS FPNG PC TM-EXM TTABC TMNG TM-External TPS-ES MyUSPTO-C IPLMSS CFS GPS PPUBS</p> <p>USPTO systems that use Google Analytics have 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 adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.</p>
<input type="checkbox"/>	<p>No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.</p>

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	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
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.)*

<input type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input checked="" type="checkbox"/>	Yes, notice is provided by the privacy policy. The privacy policy can be found at: https://www.uspto.gov/privacy-policy	
<input checked="" type="checkbox"/>	Yes, notice is provided by other means.	Specify how: This PIA serves as notice.
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Members of the public can opt-out by blocking the websites cookies. The information on how to block cookies is provided by usa.gov: Block website cookies instructions
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: USPTO employees and contractors that require a Google Analytics account can not decline to provide their PII/BII as it is required for them to complete their work.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

<input type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: USPTO does not control cookie site management, these are browser dependent controls. Some browsers may allow particular consents to use PII/BII by websites. Users should follow the instructions provided in section 7.2 to determine if particular consent by the browser is provided. USPTO employees and contractor's information is required for them to complete their work. They are not provided the opportunity to consent to particular uses of their PII/BII.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: USPTO employees and contractors can log-in to their google analytics accounts and review and update PII pertaining to them.
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: For visitors to USPTO websites, USPTO does not have access to the PII/BII pertaining to individuals. USPTO only has the

		non-identifiable aggregated data. The user is not able to update the PII pertaining to them but may update the data on them if they have a google account.
--	--	--

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

<input checked="" type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input type="checkbox"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
<input type="checkbox"/>	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): <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<input type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input type="checkbox"/>	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).
<input type="checkbox"/>	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input type="checkbox"/>	Contracts with customers establish DOC ownership rights over data including PII/BII.
<input checked="" type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input type="checkbox"/>	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).*

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. 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."

<input type="checkbox"/>	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i>
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input checked="" type="checkbox"/>	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.)*

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule: GSA -3.1 – 40: Information Technology oversight and compliance Records
<input type="checkbox"/>	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:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	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	<input type="checkbox"/>	Overwriting	<input type="checkbox"/>

Degaussing	<input type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
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.)*

<input checked="" type="checkbox"/>	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	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.)*

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: The information available to USPTO is not identifiable for users to USPTO websites. If it was available, the information has a possibility to identify the individual, however it would only identify the IP address and information about the device not necessarily the user of the device. For USPTO employees and contractors logging into Google Analytics only their name and USPTO employee would be available to identify the individual.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: The quantity of PII for USPTO employees and contractors will fluctuate but should be less than 100 users. For the public the quantity of PII will be based on the visits to USPTO websites. There are usually between 5,000 and 10,000 users active every 30 minutes.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: The data collected about individuals is not sensitive.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: The data used by USPTO is non-identifiable aggregated data used to improve USPTO services. USPTO uses the aggregated information to improve website management and functionality, and to improve visitor experiences and online services. The improved functionality will increase USPTO's ability to disseminate information to the public and enhance communication, facilitate feedback on USPTO programs, promote public participation and collaboration, and increase

		government transparency
<input checked="" type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation: The obligation to protect confidentiality of the information is defined in the agreement that GSA negotiated on behalf of all government agencies. USPTO does not handle any PII that Google Analytics may collect and process.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: The PII is not accessible to USPTO users and is only available to Google Analytics.
<input type="checkbox"/>	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. 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.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required business process changes. Explanation:
<input checked="" type="checkbox"/>	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.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required technology changes. Explanation:
--------------------------	--

<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.