



Federal Trade Commission
Privacy Impact Assessment

USAi Platform

September 2026

Table of Contents

1	System Overview	3
2	Data Type, Sources, and Use	4
3	Data Access and Sharing	6
4	Notice and Consent	7
5	Data Accuracy and Security.....	8
6	Data Retention and Disposal.....	10
7	Website Privacy Evaluation.....	10
8	Privacy Risks and Evaluation	10

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission (FTC, Commission, or Agency) is a federal law enforcement and regulatory agency with authority to promote consumer protection and competition through the prevention of unfair, deceptive, and anti-competitive business practices. The FTC pursues vigorous and effective law enforcement; advances consumer interests by sharing its expertise with federal and state legislatures and U.S. and international government agencies; develops policy and research tools through hearings, workshops, and conferences; and creates educational programs for consumers and businesses in a global marketplace with constantly changing technologies. The Commission enforces and administers a wide variety of competition and consumer protection laws.¹

To promote wider usage of artificial intelligence (AI) at the FTC, the Commission is utilizing the USAi platform, which was developed by the General Services Administration (GSA) for federal agencies to access and deploy secure leading commercial AI models. USAi is a FedRAMP-certified and multi-tenant platform that enforces strict separation without risking cross-agency data exposure. Each agency (or tenant) manages its own user stack, telemetry, and access parameters within an isolated architecture. USAi is hosted in secure FedRAMP-authorized federal cloud environments such as the AWS GovCloud and Microsoft Azure Government. The FTC has signed an MOU (Memorandum of Understanding) with GSA in order to access the USAi platform.

The platform is designed to enable FTC personnel to securely leverage the power of generative AI to improve law enforcement and regulatory activities, data analysis, research and business operations. USAi accomplishes this through the following components: USAi Chat – a web-based graphic user interface that allows authenticated users to engage in interactive, conversational sessions with various AI models; USAi API – a RESTful² application programming interface (API) that enables programmatic and automated integration of AI services into other agency systems and workflows; and USAi Console – a self-service management portal where users can manage their API credentials, review usage, and access documentation. The current models available in USAi are listed at <https://www.usai.gov/api-documentation/#models-and-endpoints>.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The information processed and maintained in USAi is collected pursuant to the Federal Trade Commission Act, 15 U.S.C. §§ 41-58 and [other laws and regulations](#) the Commission enforces.

¹ A list of the statutes enforced or administered by the FTC is available at <https://www.ftc.gov/legal-library/browse/statutes>.

² A RESTful API is an interface that two computer systems use to exchange information securely over the internet.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)³ may be collected or maintained in the system/project. Check all that apply.

<i>PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.</i>		
☒ Full Name	☒ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☒ Date of Birth	☒ Audio Recordings	☒ Internet Cookie Containing PII
☒ Home Address	☒ Photographic Identifiers (e.g., image, x-ray, video)	☒ Employment Status, History, or Information
☒ Phone Number(s)	☒ Certificates (e.g., birth, death, marriage, etc.)	☒ Employee Identification Number (EIN)
☒ Place of Birth	☒ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☒ Salary
☒ Age	☒ Vehicle Identifiers (e.g., license plates)	☒ Military Status/Records/ ID Number
☒ Race/ethnicity	☒ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☒ IP/MAC Address
☒ Alias	☒ Geolocation Information	☒ Investigation Report or Database
☒ Sex	☒ Passport Number	☒ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☐ Other (Please Specify): _____
☒ Work Address		
☒ Taxpayer ID		
☒ Credit Card Number		
☒ Facsimile Number		
☒ Medical Information		
☒ Education Records		
☒ Social Security Number		
☒ Mother's Maiden Name		

Note: The FTC may use USAi to process any information obtained as part of its law enforcement, regulatory and other activities, and which the FTC chooses to upload into the USAi platform. This may include all types of PII and sensitive information and is not limited to the data elements identified in the above table.

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

USAi processes information that the FTC obtains as part of its law enforcement, regulatory and other activities, and which the FTC chooses to upload into the USAi platform. The data may include many types of sensitive information, including Controlled Unclassified

³ Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Information (CUI),⁴ that may be other than PII. For example, staff may use USAi for document summarization, condensing lengthy policy drafts and/or public comments into brief executive synopses. Other examples of USAi use may include code generation, managing and evaluating costs, and drafting language for contracts or Memorandums of Understanding (MOUs). Any and all information uploaded into the USAi platform would be processed and/or maintained by the system.

2.3 What is the purpose for collection of the information listed above?

The information processed in USAi includes information the FTC collects as part of its law enforcement and other activities. These activities may include investigating potential or alleged violations of anticompetitive practices; enforcing statutes and regulations that protect consumers against fraudulent, deceptive, or unfair practices in the marketplace; locating victims and potential witnesses; assisting with redress; investigating internal FTC matters; and defending the FTC in suits brought against the agency.

2.4 What are the sources of the information in the system/project? How is the information collected?

<i>Source of Data</i>	<i>Type of Data Provided & How It Is Collected</i>
FTC staff and contractors	The FTC obtains information directly from targets of its law enforcement activities and from individuals and entities with information that may be relevant to the FTC's investigations and other activities. The FTC may obtain this information voluntarily (e.g., from companies that wish to merge, or from consumers who file complaints with the FTC), through compulsory process (e.g., pursuant to an FTC-issued Civil Investigative Demand, subpoena, or other requests), or during formal discovery processes in federal or administrative litigation proceedings. The FTC also may forensically acquire electronic information directly from a defendant's business premises pursuant to federal court order. The FTC also obtains data created by its employees and contractors and is stored on the FTC's production network. In addition, the FTC obtains information from public sources such as the internet.

⁴ CUI is information the U.S. Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. See 32 C.F.R. § 2002.4(h).

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

<i>Data Will Be Accessed By and/or Provided To:</i>	<i>How and Why the Data Will Be Accessed/Shared</i>
FTC Staff and Contractors	FTC staff and contractors have access to USAi and may use it to support law enforcement, policy, and administrative activities. The FTC administrator can assign users to groups, which determines which users have privileged access to the USAi Admin, API, Group, and/or Model functions in the Console.
GSA and Cloud Service Provider Administrators	Authorized GSA staff and cloud service provider administrators manage platform-level operations and may have access to the data in the FTC tenant for system support, troubleshooting, and incident response purposes.

3.2 Do contractors and/or third-party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

Authorized GSA administrators and cloud service providers with privileged access accounts may have access to FTC tenant data for system support, troubleshooting, and incident response purposes. FTC data is maintained in the FTC's dedicated workspace and remains logically separate from other tenant data in USAi. USAi data is managed within secure FedRAMP-authorized federal cloud environments. The platform is designed specifically to provide federal agencies with a secure and compliant infrastructure to deploy and utilize generative AI models. USAi's secure architecture leverages multi-tenant cloud safety features such as encryption, identity management, and logging.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third-party service provider.

GSA employs multiple mechanisms to identify security incidents and breaches of PII on the USAi platform, and has established procedures for breach detection and response, including notifying affected agencies.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

- ☒ Notice is provided via (*check all that apply*):
- ☒ Privacy Act Statement (☒ Written ☐ Oral)
 - ☒ FTC Website Privacy Policy
 - ☒ Privacy Notice (e.g., on Social Media platforms)
 - ☒ Login banner
 - ☐ Other (*explain*): _____
- ☐ Notice is not provided (*explain*): _____

The information processed in USAi is from various systems that collect and maintain PII; refer to the system-specific [PIAs](#) for more information about how each system provides notice. Wherever possible, the FTC provides timely and effective notice to the public about activities that impact privacy, including the collection, use, and disclosure, and disposal of information at the time the information is collected. The FTC's Privacy Act notices are included on all forms, websites, and other instruments by which Privacy Act information is collected from individuals, either in written or oral form. For those occasions where the FTC cannot provide notice at the time the information is collected (e.g., when the information is collected by another law enforcement agency or another organization), the FTC provides notice via its privacy policy, its Privacy Act system of records notices ([SORNs](#)), and its [PIAs](#), including this one.

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

Individuals may not have the opportunity or ability to decline to provide information or consent to use of their information within the USAi platform. The opportunity or right depends on how the information is collected and the purpose for the collection. For example, those who provide information pursuant to compulsory process do not generally have a right to decline to provide the information. When information is provided voluntarily, the use of such information may also be governed by mutual agreement. If the individual has a right to consent to a particular use, this right will normally be exercised when determining whether to provide information to the FTC. Some uses of information are not subject to the consent of the individual providing the information (e.g., information provided pursuant to a court order or subpoena). In addition, uses of information may also be governed by specific laws (e.g., routine uses authorized under the Privacy Act of 1974).

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

Individuals seeking records about themselves do not have direct access to USAi. Instead, individuals may make a request under the Freedom of Information Act (FOIA) and Privacy

Act for access to information maintained about themselves in USAi or other FTC record systems. Individuals must follow the FTC's Privacy Act rules and procedures, which are published in the Code of Federal Regulations at 16 C.F.R. § 4.13, for requests for information. Privacy Act requests must be made in writing and submitted to the FTC's Office of General Counsel. The Privacy Act requires requesters to verify their identity, which can be done by digital authentication through Login.gov or by certifying by signature that the requester is the individual to whom the record pertains or is the parent or guardian of a minor or the legal guardian of the individual to whom the record pertains. *See the FTC [FOIA website](#).*

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

As stated above, individuals seeking records about themselves do not have direct access to the USAi platform. The FTC provides a process for individuals to correct or amend any inaccurate PII maintained by the Agency. The [FTC's privacy policy](#) provides links to the FTC's SORNs, which include information about how to correct or amend records. An individual may make a request under the Privacy Act for access to information maintained by the FTC about themselves in any FTC Privacy Act systems. Access to the information under the Privacy Act is subject to certain exemptions. Individuals may also file requests with the FTC under the FOIA for agency records that may be about them (if they are not exempt from disclosure to them under those laws).⁵ Additionally, individuals may contact the FTC with any complaints, questions or concerns via phone or email available on [www.ftc.gov](#) or contact the Chief Privacy Officer directly. Where appropriate, the FTC disseminates corrected or amended PII to other authorized users of that PII, such as external information sharing partners.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

Information that is used by the FTC as part of its law enforcement and other activities is reviewed for accuracy and timeliness as required by the particular activity. For example, staff performing an investigation based upon a "whistleblower" complaint may check the information that is obtained to ensure that it is timely and accurate. In other cases, the individual submitting the information may also be required to certify the accuracy of the information (e.g., witness or financial statements in court cases).

Information processed on the USAi platform is subject to appropriate security controls. In addition to protecting against unauthorized access, alteration, or dissemination, these

⁵ See 16 C.F.R. 4.11(a) (FTC FOIA rules), 4.13 (FTC Privacy Act rules).

controls reduce the risk of loss and assure the integrity of the evidentiary materials from the point at which they are included in the system.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

The FTC operates within a dedicated, logically isolated USAi tenant managed by the GSA. The tenant includes instances of USAi Chat, USAi API, USAi Console, dedicated data stores, and isolated logging infrastructure to ensure organizational separation from other agencies.

Access to USAi is restricted to authorized FTC employees and contractors using FTC-issued credentials. Authentication is integrated with the agency's identity management solution and requires multifactor authentication. Access is granted based on organization roles and principles of least privilege.

Administrative safeguards include user onboarding and offboarding procedures, periodic access reviews, security awareness training, Acceptable Use policy acknowledgements, and continuous oversight by the FTC Office of the Chief Information Officer (OCIO).

Technical safeguards include:

- Encryption of data in transit using TLS and encryption of data at rest using FIPS 140- validated cryptographic modules;
- Role-based access controls (RBAC) and tenant isolation;
- Audit logging and monitoring of user activity and administrative actions;
- Secure API authentication and authorization controls;
- Continuous vulnerability management and security monitoring;
- Dedicated storage and logging for the FTC tenant.

User-submitted prompts and generated responses remain within the secure USAi environment. Users may only access conversations and content that they create or are explicitly authorized to access through system functionality.

5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

☒ Not Applicable.

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

Information received in the system for purposes of creating prompts or generating responses is retained and destroyed/deleted in accordance with General Records Schedule 5.2, Transitory and Intermediary Records, and, to the extent applicable, the instructions in the FTC Rules of Practice Section 4.12, Disposition of Documents Submitted to the Commission. User login information, technical logs, access control, and other authentication records related to user login and session management are retained and destroyed/deleted in accordance with General Records Schedule 4.2, Information Access and Protection Records.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

FTC personnel access USAi through the GSA-managed web application available only to authorized users. The FTC implementation of USAi does not employ website tracking technologies for public-facing purposes, such as advertising, web analytics, or user profiling. Any cookies or similar technologies used by the application are limited to those necessary to support authentication, session management, security, and system functionality. These technologies are temporary, expire when the user session ends or after the defined inactivity period, and are not used to track users across websites or for marketing purposes. Any website privacy practices related to the underlying GSA hosted platform are governed by GSA.

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

<i>Risk</i>	<i>Mitigation Strategy</i>
Unauthorized access to the USAi platform	Access is limited to authorized FTC personnel using FTC-issued credentials with multifactor authentication. Role-based access controls, tenant isolation, logging, and periodic access reviews reduce the likelihood of unauthorized access.

<i>Risk</i>	<i>Mitigation Strategy</i>
The output from Generative AI tools may misrepresent information, generate inaccurate content, and incorrectly summarize information	To address this risk, FTC staff are prohibited from relying on AI-generated output without thoroughly reviewing it. FTC personnel are required to independently review, validate, and verify AI-generated outputs before relying upon or distributing them. FTC staff are required to include a disclosure note that AI was used to generate any work product that they share with others internally and to obtain supervisory approval before sharing outside the agency.
Data leakage	User prompts and agency data are processed within the secure USAi environment. Customer data is logically isolated, encrypted in transit and at rest, and protected by access controls.
Collection or disclosure of PII through user prompts	User prompts are transmitted from USAi Chat/API backend to authorized AI service endpoints, including GCP Vertex AI, Azure AI, and AWS Bedrock over HTTPS using TLS 1.2 or higher. Access to these services is limited to those with authorization to use them, network restrictions, and tenant managed identities or API credentials. AI responses are returned through the same encrypted channel.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

USAi is configured so that customer prompts and generated outputs remain within the authorized environments. These controls reduce the likelihood of unauthorized disclosure or secondary use of agency information.

Privacy protections are supported through administrative safeguards including user training, acceptable use requirements, access reviews, and governance processes that require human review of AI-generated outputs before they are relied upon for official FTC business.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

USAi is not considered a Privacy Act system of record of its own accord. However, the data processed by USAi may come from a Privacy Act system of record. Such data, to the extent such data are about an individual and retrieved by that individual's name or other personal identifier, are covered by the Privacy Act of 1974, 5 U.S.C. 552a, under one or more applicable FTC SORNs. A complete list and copies of these SORNs is available online at www.ftc.gov.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

The collection, use, and disclosure of information in this system are consistent with the [FTC's Privacy Policy](#). In addition, FTC staff must adhere to the USAi System Rules of Behavior and the FTC guidance on the use of Generative AI. Furthermore, FTC staff are required to review and sign the FTC Rules of Behavior on an annual basis.