U.S. General Services Administration

GSA Implementation of USAi (GSA USAi) Privacy Impact Assessment (PIA)

June 2026

Point of Contact
Richard Speidel
Chief Privacy Officer
Office of Innovation, GSA IT
1800 F Street NW
Washington, DC 20405

Stakeholders

Name & Email of Information System Security Manager (ISSM):

- Nate Ciano, nathaniel.ciano@gsa.gov

Name & Email of System Owner:

- Ryan Palmer, ryan.palmer@gsa.gov

Signature Page

/Nate Ciano/, June 10, 2026

Nate Ciano, Information System Security Manager (ISSM)

/Ryan Palmer/, June 10, 2026

Ryan Palmer, System Owner

/Richard Speidel/, June 10, 2026

Richard Speidel, Chief Privacy Officer

Under the direction of the Senior Agency Official for Privacy (SAOP), the Chief Privacy Officer is responsible for ensuring the PIA contains complete privacy related information.

Table of contents

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

4.1 Is the information in the system, application or project limited to only the information that is needed to carry out the purpose of the collection?

4.2 Will GSA share any of the information with other individuals , Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

4.4 Will the system, application or project interact with other systems, either within GSA or outside of GSA? If so, what other system(s), application(s) or project(s)? If so, how? If so, is a formal agreement(s) in place?

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will the information collected be verified for accuracy and completeness?

5.2 Are there any privacy risks for individuals whose information is collected or used by the system, application or project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

SECTION 6.0 SECURITY

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technological, and managerial perspective?

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Document purpose

This document contains important details about the GSA Implementation of USAi. GSA-IT may, in the course of using the GSA Implementation of USAi, collect personally identifiable information ("PII") about the people who use such products and services. PII is any information[1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, uses, secures, and destroys information in ways that protect privacy. This PIA is comprised of sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles ("FIPPs"), a set of eight precepts that are codified in the Privacy Act of 1974.[2]

System, Application or Project

GSA implementation of USAi.

System, application or project includes information about

USAi does not specifically collect data from a defined population. However, information about agency employees, contractors, and the public may be present in inputs such as user prompts, uploaded files, the resulting generated outputs, and user-provided feedback on generated outputs. For example, GSA's AI Oversight Committee has approved general use cases related to drafting correspondence or summarizing documents, either of which may include incidental PII such as email addresses.

Models process prompts containing PII when the request focuses on a task and the PII is provided within the prompt. Models are not directed to discover or collect additional personal information.

API-based integrations with the GSA Implementation of USAi are responsible for obtaining use case approval and updating the Privacy Impact Assessment (or other privacy documentation) of any upstream (source) downstream (destination) data system.

System, application, or project includes

- User Information: Name, work email address, username, organization, user role

- Data Inputs: prompt content, uploaded files, feedback
- Data Outputs: generated responses
- Telemetry: usage logs, including user interaction and prompt response data

Overview

GSA Implementation of USAi provides agency personnel with access to generative AI chat and API capabilities for drafting, summarization, analysis, and related productivity tasks.

The system collects account and access data to authenticate authorized users and processes prompt, response, and file content submitted by those users.

Although the tool is not intended to serve as an official records repository, users may enter incidental PII in free text or uploads.

Any upstream system that utilizes the USAi-API must be evaluated separately under its own PTA, PIA, and/or SORN as appropriate.

Any downstream system that exports, ingests, stores, or analyzes raw interaction data must be evaluated separately under its own PTA, PIA, and SORN as appropriate.

SECTION 1.0 PURPOSE OF COLLECTION

1.1 Why is GSA collecting the information?

GSA is not specifically collecting information via the GSA Implementation of USAi.

A limited amount of PII is present in the system to provide authenticated agency users with AI chat capabilities, manage access, support security monitoring, troubleshoot service issues, and enable mission-related drafting, summarization, and analysis. Incidental PII may be processed when users include it in prompts, attachments, or feedback.

1.2 What legal authority and/or agreements allow GSA to collect the information?

Not Applicable - the purpose of the system is not directed to the collection of PII.

1.3 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information being collected?

Personally identifiable information is not regularly retrieved by personal identifier, therefore no System of Records Notice applies to the system.

1.4. Has any information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.

Not Applicable

1.5. Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

GSA applies an approved records schedule for access logs, audit data, and any exported or retained official agency records created through use of the service:

- Raw Interaction Data (prompt & response): NARA GRS 5.2 (Transitory and Intermediary Records) – retained for 30 days to support troubleshooting, security monitoring, and operational continuity, after which data is deleted or sanitized consistent with approved disposition and contractual requirements.

- Redacted Interaction Data (prompt & response): NARA GRS 5.2 (Transitory and Intermediary Records) – retained for operational analytics and product improvement purposes.

- User Account and Access Data: Retained consistent with applicable GSA records schedules for IT administrative records.

Any downstream system that separately stores or analyzes interaction data should apply its own approved records schedule.

1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

Yes. The main risk is users entering more PII than necessary into free-text prompts or file uploads. The agency mitigates this through training, acceptable use rules, data handling

guidance, least-privilege access, limited retention, and review of use cases involving significant PII.

SECTION 2.0 OPENNESS AND TRANSPARENCY

2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about themselves? If not, please explain.

Yes. Users receive notice through:

- Internal Training Materials: Onboarding and periodic training on acceptable use and data handling.
- System Prompts: In-application guidance instructing users not to submit unnecessary sensitive information.
- Rules of Behavior: Acknowledgment of acceptable use policies prior to system access.
- Upstream (source) or Downstream (destination) system PIAs and SORNs.

Where information is entered about other individuals (such as names or contact details in prompts), GSA relies on existing privacy notices and agency policy as applicable.

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

Yes. Users may be unaware of the impact of specific uses of PII within the AI chatbot and incorrectly assume the USAi AI system is appropriate for all uses. GSA mitigates this through:

1. Training and Written Guidance: Periodic reminders on permitted and prohibited data types.

2. AI Oversight Committee: GSA AI Use Case approval requirements ensure review of appropriate uses.

3. Upstream/Downstream System Requirements: Rules of behavior and data handling requirements for any system integrating with USAi.

4. Published Privacy Documentation: This PIA is published at gsa.gov/privacy to provide transparency about data handling practices.

SECTION 3.0 DATA MINIMIZATION

GSA limits the collection of PII to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Whose information is included in the system, application or project?

Primary: Authorized GSA employees and contractors who use the system authentication data.

Incidental: Any individuals whose information users may include in prompts, uploaded files, or feedback (such as names, email addresses, et cetera).

3.2 What PII will the system, application or project include?

- User Account Data: Work email, username, organization, user role

- Interaction Data: Prompt content, uploaded documents, generated outputs, feedback

- Telemetry/Logs: Usage logs, timestamps, session identifiers, API activity

- Incidental PII: Names, email addresses, contact details, or other PII that users may include in prompts or uploads

3.3 Why is the collection and use of the PII necessary to the system, application or project?

- User Account Data: Required to authenticate users, assign roles, manage access, and support auditability.

- Interaction Data: Necessary to process user requests and generate responses for authorized productivity tasks.

- Telemetry/Logs: Required for security monitoring, troubleshooting, and operational support.

- Incidental PII: Not the purpose of the tool, but a reasonably foreseen byproduct of authorized use cases (such as drafting correspondence or summarizing documents).

3.4 Will the system, application or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

Yes. The system may generate metadata and derived outputs including:

- Usage History: Records of user interactions with the system.

- Timestamps: Date and time of interactions.

- Feedback Records: User-provided feedback on responses.

- Generated Outputs: Summaries, drafts, or analyses that reflect user interaction with the tool.

This data is maintained consistent with the retention schedules described in Section 1.5 and used only for authorized purposes including troubleshooting, security monitoring, and product improvement.

3.5 What protections exist to protect the consolidated data and prevent unauthorized access?

- Role-Based Access Controls (RBAC): Access limited to authorized personnel based on job function.

- Multi-Factor Authentication (MFA): Required through the GSA identity provider (SecureAuth).

- Encryption: Data encrypted in transit (TLS) and at rest.

- Audit Logging: All access and activity logged for security review.
- Privileged Access Controls: Administrative access restricted and monitored.
- Limited Retention: Raw interaction data retained for only 30 days.
- Separation of Environments: Any downstream system used to export, ingest, store, or review raw interaction data is addressed separately in that system's PTA/PIA.

3.6 Will the system monitor the public, GSA employees or contractors?

The system logs user activity for security, support, and administrative purposes. It is not deployed as an employee surveillance tool.

Logging is limited to what is necessary for:

- Security monitoring and incident response
- Troubleshooting and technical support
- Administrative oversight and compliance
- Product improvement and analytics (using aggregated/de-identified data where feasible)

3.7 What kinds of report(s) can be produced on individuals?

Administrative reports may show:

- User access and authentication records
- Usage volume and frequency
- Feedback submitted by users
- API activity associated with user accounts
- Troubleshooting logs tied to specific sessions or users

- Cost reporting

These reports are used only for security, support, and administrative purposes.

3.8 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

Where feasible, reporting for analytics and product improvement will use aggregated or de-identified data. De-identification processes include:

- Aggregation: Combining data across users to report trends without individual attribution

- Field Removal: Removing or masking direct identifiers (such as usernames and email addresses) from analytical datasets

- Tokenization: Replacing identifiable values with non-reversible tokens where individual-level analysis is required for operational purposes

Any downstream reporting environment that retains or analyzes raw interaction data must be addressed separately in that system's privacy documentation.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

Yes. The primary risks are:

1. Oversharing in Prompts: Users may enter more PII than necessary in prompts or uploads.

2. Unnecessary Retention: Interaction data could be retained longer than needed and PII may be exfiltrated from the GSA Implementation of USAi.

GSA mitigates these risks through:

- Data Minimization Guidance: Training and written guidance instructing users to limit PII in prompts.

- Prompt Warnings: In-application reminders about appropriate data handling.

- Use-Case Restrictions: GSA AI Oversight Committee review of use cases involving significant PII.
- Limited Retention: 30-day retention for raw interaction data.
- Periodic Review: Regular assessment of whether retention and access controls remain appropriate.
- Upstream & Downstream Separation: Any system that provides or ingests interaction data is evaluated separately, and the privacy rules of those systems apply.

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

4.1 Is the information in the system, application or project limited to only the information that is needed to carry out the purpose of the collection?

Yes. GSA limits required account data to what is needed for:

- Access management and authentication
- Administration and role assignment
- Security monitoring and incident response
- Technical support and troubleshooting

The system does not require or request sensitive PII to perform its core functions.

4.2 Will GSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?

GSA may share limited information under the following circumstances:

Recipient	Information Shared	Purpose	Safeguards
USAi Platform Provider (GSA IT)	User authentication data, interaction data	Platform operation, security, support	Agency agreement access controls, encryption

AI Service Providers	Prompt and response content	Model processing	Contractual restrictions, no training on government data
GSA Security Operations	Access logs, security events	Security monitoring, incident response	Role-based access, need-to-know

Additional sharing would be subject to GSA policy and applicable law. Aggregate or de-identified data may be shared for governance, oversight, or product improvement, and research purposes.

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

Data Type	Source
User Account Attributes	GSA identity provider GSAAuth
Prompt Content	Provided directly by the user
Uploaded Files	Provided directly by the user
Feedback	Provided directly by the user
Generated Responses	Created by the AI model based on user input

4.4 Will the system, application or project interact with other systems, applications or projects, either within or outside of GSA? If so, who, how and is a formal agreement(s) in place?

System	Interaction Type	Agreement/Documentation
GSA Identity Provider GSAAuth	User authentication via SAML/OIDC	Internal GSA system

USAi Core Platform (GSA IT)	Tenant services, API access	Interagency agreement
AI Model Providers (via USAi)	Model inference processing	Contractual agreements managed by GSA IT
GSA Security Operations Center	Security log ingestion	Internal GSA processes

Upstream/Downstream Systems: Any system that sends data to the USAi API (upstream) or receives exported interaction data (downstream) is documented separately in that system's PTA/PIA. Examples include:

- System to system interactions using the USAi-API e.g. Databricks
- Analytics platforms ingesting interaction logs
- Security tools receiving audit data

4.5 Are there any privacy risks for this system, application or project that relate to use limitation? If so, how will GSA mitigate these risks?

Yes. The primary risks are:

- Secondary Use: Chat data could be used beyond the original context if controls are not maintained.
- Downstream Expansion: Systems receiving exported data could use it for unintended purposes.
- Mission Creep: Authorized uses could expand without appropriate review.

GSA mitigates these risks through:

- Role-Based Access: Limiting access to authorized personnel with a need to know.
- Written Restrictions: Documented policies for systems receiving information via the System Security and Privacy Plan (SSPP) and related documentation.
- Governance Review: GSA AI Oversight Committee review for new use cases.

- Downstream Separation: Separate privacy review required for any downstream system that ingests raw interaction data.

- Contractual Controls: Agreements with service providers restricting use of government data.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected be verified for accuracy and completeness?

Data Type	Verification Method
User Account Data	Sourced from the GSA identity provider, which maintains authoritative employee/contractor records
Prompt and Uploaded Content	User-provided; not independently verified by the system
Generated Responses	AI-generated outputs are not independently verified unless validated by the business process using the output

GSA instructs users that AI-generated outputs should be reviewed for accuracy before use in official business processes.

5.2 Are there any privacy risks for individuals whose information is collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?

Yes. The primary risks are:

- Inaccurate User Input: Users may input inaccurate or outdated information about themselves or others.

- AI Hallucination: Model outputs may restate information incorrectly or generate inaccurate content.

- Outdated Information: Information in prompts or uploads may not reflect current status.

GSA mitigates these risks through:

- AI Use Case Review: AI Use Case review and requirements reliance on AI outputs for official decisions without human review and validation.

- Training: Educating users about AI limitations and the importance of verifying outputs.
- Acceptable Use Policy: Restricting use of the system for high-stakes decisions without appropriate oversight.

- Source System Authority: Corrections to personnel or official data must be made in authoritative source systems, not based solely on AI outputs.

- User Feedback: Users are trained to use the feedback mechanism to identify any inaccuracies provided by the system.

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who or what will have access to the data in the system, application or project? What is the authorization process to gain access?

Role	Access Level	Authorization Process
Authorized GSA Users	Own prompts, uploads, and responses	GSA identity provider authentication; role assignment by supervisor
Tenant Administrators	User management, configuration settings	Management approval; privileged access review
Technical Support Personnel	Troubleshooting logs, limited interaction data	Need-to-know basis; incident-driven access

Security Personnel	Audit logs, security events	SOC authorization; least-privilege access
USAi Platform Administrators (GSA IT)	Platform-level operations	Interagency agreement; role-based access

Access is granted through:

- GSA-approved identity federation GSAAuth
- Role assignment based on job function
- Least-privilege review
- Management approval for elevated access

Any downstream system access involving PII is managed separately under that system's security authorization and privacy documentation.

6.2 Has GSA completed a system security plan for the information system(s) or application?

Yes. The GSA implementation of USAi operates under an approved System Security and Privacy Plan (SSPP) consistent with GSA's authorization process. The system inherits controls from:

- USAi Core Platform (GSA IT)
- GSA Cloud Infrastructure (FCS)
- GSA Security Operations Center (GSA-IT)
- GSA Identity and Access Management (GSA-IT)

The SSPP is maintained as part of the Authorization to Operate (ATO) package and reviewed consistent with GSA Order CIO 2100.1.

6.3 How will the system or application be secured from a physical, technological, and managerial perspective?

Physical Controls:

- Cloud-hosted infrastructure in FedRAMP-authorized data centers

Technological Controls:

- Federated authentication via GSA identity provider
- Multi-factor authentication (MFA) required for all users
- Encryption in transit (TLS 1.2+) and at rest (AES-256)
- Role-based access controls (RBAC)
- Audit logging of all access and activity
- Network segmentation and monitoring
- Automated vulnerability scanning

Managerial Controls:

- Security awareness training for all users
- Acceptable use policies and rules of behavior
- Incident response procedures
- Regular security assessments
- Change management processes
- Privileged access management and review

6.4 Are there mechanisms in place to identify suspected or confirmed security incidents and breaches of PII? If so, what are they?

Yes. GSA employs multiple mechanisms to identify security incidents and breaches of PII:

- Audit Logging: Comprehensive logging of user access, authentication events, and administrative actions
- Security Monitoring: GSA Security Operations Center (SOC) monitoring of security events
- Automated Alerts: Threshold-based alerting for anomalous activity
- Incident Reporting Procedures: Established processes for reporting and responding to security incidents per GSA IT Security Policy
- Coordination with GSA-IT: Incident response coordination with the USAi platform provider
- Regular Log Review: Periodic review of access and activity logs

6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?

Yes. The primary security-related privacy risks are:

- Accidental Disclosure: Users may inadvertently include sensitive PII in prompts shared with the AI model.
- Overbroad Access: Excessive access permissions in downstream systems that ingest interaction data.
- Data Exfiltration: Unauthorized extraction of interaction data containing PII.

GSA mitigates these risks through:

- Training: Security awareness and data handling training
- Monitoring: Continuous security monitoring and anomaly detection
- Least Privilege: Role-based access with regular access reviews
- Incident Response: Established procedures for breach detection and response

- Encryption: Data protected in transit and at rest

- Downstream Review: Separate security and privacy review for systems that ingest exported interaction data or use the API

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities are available for individuals to consent to specific uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline or opt out, please explain.

Use of the GSA Implementation of USAi is limited to authorized GSA employees and contractors operating under GSA policy.

Consent and Participation:

- Users acknowledge acceptable use policies and rules of behavior prior to accessing the system

- Users may decline to enter optional information in prompts

- Users are instructed not to include unnecessary PII in prompts or uploads

Limitations:

- Basic account data (work email, username, organization) is required for authentication and access management

- Users who choose not to provide required account information cannot access the system

- Audit logging for security and oversight purposes is mandatory and cannot be opted out

7.2 What procedures allow individuals to access their information?

The system does not maintain records about individuals. Individuals can only view information that they have put into the system themselves, including their chat history.

7.3 Can individuals amend information about themselves? If so, how?

No, the system does not maintain records about individuals. Individuals can only view information that they have put into the system themselves, including their chat history.

7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?

Not Applicable

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application or project.

General Privacy and Security Training:

- All GSA employees and contractors complete annual privacy awareness training as required by GSA policy
- All GSA employees and contractors complete annual IT security awareness training per GSA Order CIO 2100.1

USAi-Specific Training:

- Onboarding Guidance: New users receive orientation on acceptable use, data handling, and prohibited data types before accessing the system
- Acceptable Use Policy: Users acknowledge rules of behavior that include privacy and data handling requirements

8.2 Are there any privacy risks for this system, application or project that relate to awareness and training? If so, how will GSA mitigate these risks?

Yes. The primary risks are:

- Informal Treatment: Users may treat chat interactions as informal and ignore data handling rules.

- Unfamiliarity with AI: Users may not understand how AI systems process information or the implications of including PII in prompts.

- Complacency: Over time, users may become less attentive to privacy requirements.

GSA mitigates these risks through:

- Mandatory Training: Required training

- Periodic Reminders: Regular communications and refresher guidance

- In-Application Prompts: Contextual reminders about appropriate data handling based on system prompts

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system, application or project ensure that the information is used in accordance with the stated practices in this PIA?

GSA ensures compliance through technical controls, administrative controls, and auditing.

The GSA AI Oversight Committee reviews and approves use cases, including those involving PII. The Privacy Office maintains oversight of the administration of privacy documentation and practices. The GSA Implementation of USAi system team provides technical and process information in order to support the development of privacy documentation. Technical controls include role-based access, audit logging, and configuration management with change control.

Administrative controls include acceptable use policies, rules of behavior, documented use cases, and periodic review of system use and compliance. Auditing includes log review, access reviews, PIA updates aligned to the ATO cycle, and regular security assessments.

9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Yes. Without ongoing review, system uses may expand beyond documented purposes, data may be repurposed without appropriate oversight, and downstream systems may use exported data in unanticipated ways. GSA mitigates these risks through AI Oversight Committee review of new use cases, formal documentation of approved uses, periodic review of use cases within the USAi console, PIA updates when significant changes occur, approval requirements before expanding functionality, and requiring separate PTA/PIA review for downstream systems that ingest interaction data.

---

[1]OMB Memorandum *Preparing for and Responding to a Breach of Personally Identifiable Information* (OMB M-17-12) defines PII as: "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." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.