Privacy Office Contact Information

Please send any questions by email to gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, 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, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises 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 codified in the Privacy Act of 1974.[2]

[1]OMB Memorandum Preparing for and Responding to the 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.

General Information

PIA Identifier: 483
System Name: GSA Implementation of Google Workspace
CPO Approval Date: 8/6/2024
PIA Expiration Date: 8/6/2027

Information System Security Manager (ISSM) Approval

Nathaniel Ciano

System Owner/Program Manager Approval

Chris McFerren

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
GSA Implementation of Google Workspace

B: System, application, or project includes information about:
GSA Employees and Contractors

C: For the categories listed above, how many records are there for each?
Estimated a minimum of 500,000 records for the above categories.

D: System, application, or project includes these data elements:
Gmail Google, Meet Classic Hangouts, Google Chat, Google Calendar, Google Drive and Shared Drive . Google Docs, Google Sheets, Google Slides, Google Forms, Google Sites Google Keep Apps Script Chrome Browser,

Overview:

Google Workplace Enterprise is a collection of online messaging and collaboration applications offered as a Software as-a-Service (SaaS) in a cloud computing environment. There are 14 core applications in GWE and 55 non-core applications available in GWE. Please see the a list of Google services with implementation status here.
GSA is using the Google GWEWorkspace Enterprise Cloud to process and store data in Google production data centers. Machines supporting GWEdata are located in Google data centers and data at rest is encrypted using full disk encryption.GSA implementation of GWEGWE services consists of Gmail), Calendar, Chat, Meet , Directory, Drive and Docs,Vault, Groups for Business, Jamboard, Cloud Search, Keep & Sites. Google hosts the GWEGWE offering, including the underlying GCI. within Google data centers. providing it direct control over processing and storage of the core content. “Core content” means the following subsets of Customer Data with respect to these individual components of the Services.

- **Google GMail**: messages and attachments:
- **Google Calendar**: events and descriptions of events:
- **Google Directory (Contacts)**: content of the address book:
- **Cloud search**:
- **Google Drive and Docs**: content authored by the owner’s or collaborators of the doc. not including content hosted on (i) other Google products not referenced in Core Content or (ii) other third party websites:
- **Groups for Business(Google Groups)**: Google Groups for Business is a service from Google that supports mailing lists as well as collaborative inboxes for groups of users to access.Google Sites: content authored by the owners or collaborators of the site: not including content hosted on (i) other Google products not referenced in Core Content or (ii) other third party websites:
- **Google Vault**: Used to provide ediscovery related activities against GWE content.
- **Google Keep**: Content authored by die owner or collaborators of die note. except content embedded into the notes that is hosted on other Google products not referenced in this list.(e.g.. YouTube)
- **Chat and Classic Hangouts**: Conversations, both on the record and off—the-record Direct messages are removed after 24 Hours. Messages within rooms are retained indefinetly.
- **Google Meet**: Meeting details, including meeting creator. meeting code, phone access.

There are additional non core Google Services that are offered by Google that are available for use by GSA. For an accurate upto date list please visit the following Google help article:

https://support.google.com/a/answer/181865?hl=en

Google Cloud Directory Sync (GCDS) – GCDS automatically provisions users, groups, and nonemployee contacts based on the user data in GSA's LDAP, Microsoft Active Directory (AD). GCDS connects to GSA's GSuite directory and adds and suspends user accounts to match the existing organizational schema. The GCDS tool pushes members from GSA's LDAP (Active Directory) using a one-way push that reads the user data and pushes the information up to Google. There is a full Google Cloud Directory Sync Server on the dedicated servers inside GSA. The GCDS tool connects to GSA AD, gets users and their user attributes, and compiles the list on the server, connects to Google port 443 (secure SSL) and uses a one-way push to create, modify or suspend users in GSA's GSuite domain. This process is run on an hourly basis. If a user is no longer active in AD, the user is suspended in GSA's GSuite Domain.

The Google Cloud Directory Sync tool is used to provision/deprovision user accounts from AD LDS to Google. AD LDS is also used to provision the same information to the Salesforce platform.

GCDS is only used for the gsa.gov and test.gsa.gov domains of GWE. Apps.gsa.gov users are provisioned manually using the admin panel of GWE.

Access to Individual Email Accounts

Often requests are made that require access to individual emails within a client mailbox. These requests are for the purposes of investigations, security related alerts, containment of PII leakage incidents or other issues deemed necessary by the Office of General Counsel, Office of the Chief People Officer or the Office of the Senior Agency Information Officer. To access a user mailbox, a formal request must be made from OCPO, OGC, CISO or the ISSM with justification provided to the Enterprise Messaging and Collaboration Services Branch. The Enterprise Messaging and Collaboration Services Branch is the only authorized mechanism for the retrieval or deletion of a specific email.

Apps.gsa.gov

Apps.gsa.gov is the Google Workspace Enterprise implementation used to support Commissions and Boards who require collaboration service. These entities ususaly require between and 10-20 user accounts.

Apps.gsa.gov offers the same functionality and apps that gsa.gov provides for GSA. The underlying difference between the two plaforms is that authentication to apps.gsa.gov users 2 factor security key based and no integration with Active Directory.

Test.gsa.gov

Test.gsa.gov is the test instance of gsa.gov where new functionality that Google implements is vetted before implementation in gsa.gov

Gsa.gov

Gsa.gov in GSA's instance of Google Workspace Enterprise used to support collaboration among GSA associates.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
44 U.S. Code §3101. Records management by agency heads; general duties 5 U.S. Code §301. Departmental regulations

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?
Yes

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
Existing SORN applicable

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?
Yes, the system is searchable by a google account holder's name. Administrators can deactivate certain accounts; however, that does not preclude a user from searching a deactivated user's account for data that already exists in the system. Sources may vary widely as information is not collected by the system's applications specifically, but are used as a mechanism to store, collaborate and share information between users. The potential PII stored and shared using GWE comes from a varied source of extracts and sources. GSA primarily relies on GWE for storage, sharing or collaboration of mission-critical information at the FISMA moderate level. For example, Google and GSA have entered into a Business Associate Agreement (BAA) to allow GSA's Office of Evaluation Sciences to store HIPAA Limited Data Sets on Google Drive.

GWE is covered under GSA's Enterprise Organization of Google Applications SORN GSA/CIO-3 GSA Enterprise Organization of Google Applications and SalesForce.com.

1.2b: Explain why a SORN is not required.

1.3: Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

1.3: Information Collection Request: Provide the relevant names, OMB control numbers, and expiration dates.
GWE is not an information collection for Paperwork Reduction Act purposes. If a Google form requires an ICR, the form creator must adhere to procedures and policy.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
Records are maintained and verified while an employee has active employment. After a user leaves GSA, the email record will be available for 7 years and 15 years for high level officials. Records are disposed of as specified in the handbook, GSA Records Maintenance and Disposition System (CIO P 1820.1). The record retention period is indefinite this is part of GSA Number/Disposition Authority GRS 03.1/011 and DAAGRS-2013-0005-0008.

2.0 Openness and Transparency

2.1: Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? No

2.1 Explain: If not, please explain.

As a general rule, personal information is not collected by the system's applications. The system is a mechanism to collect, maintain, collaborate and share information between users.

In cases where personal information is collected by the system's applications, the application will present the applicable Privacy Act statement(s) to the user before they submit such information.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
GWE core apps (primarily Email, Sites, Groups and Docs) may contain PII stored there by users for the purposes of normal day to day work operations, operations collaboration or simple storage. A user could potentially enter PII into the system but the system itself does not collect it. None of the system's applications collect that information by default.

In cases where the system's applications collect personal information, that information is needed to comply with a legislative mandate (e.g., law, Executive Order, etc.)

3.2: Will the system, application, or project create or aggregate new data about the individual?
No

3.2 Explained: If so, how will this data be maintained and used?

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?
Multi Factor Authentication (MFA) is used for access to the data, access controls are in place to ensure no inadvertent Agency wide exposure of the data is permitted, and users are trained on the proper handling of PII information when used with these applications.

3.4 Will the system monitor the public, GSA employees, or contractors?
None

3.4 Explain: Please elaborate as needed.
The system is a mechanism to collect, maintain, collaborate and share information between users and not used as a monitoring or surveillance tool.

3.5 What kinds of report(s) can be produced on individuals?
Using the audit logs provided by GWE as a part of it’s Cloud Audit Logs, reports can be produced on Admin Activity and Data Access activity by both privileged and non-privileged users.

Additionally, GWE administrators can filter and generate a report by event name, user, IP address, date, disk space and email address.

Finally, If a system's application (e.g., Google Forms) collects personal information about a user, that information can be accessed only by administrators and privileged users. That information can be filtered and reported by user/email address and other data elements that may be collected.

If a system's application (e.g., Google Forms) collects personal information about a user, that information can be accessed only by administrators and privileged users. That information can be filtered and reported by user/email address and other data elements that may be collected.

3.6 Will the data included in any report(s) be de-identified?
Yes

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?
Any reports that can be produced about the personal information are appropriate for those privileged users and do not require any aggregation or de-identification. However, in cases where information needs to be reported in the aggregate, privileged users should take care to de-identify all information prior to sharing with other audiences.

3.6 Why Not: Why will the data not be de-identified?
No, the reports that can be produced on Admin Activity and Data Access activity by both privileged and non-privileged users are appropriate for those audiences and do not require any aggregation or de-indentification.

4.0 Limits on Using and Sharing 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?
No

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?
Federal Agencies

4.2How: If so, how will GSA share the information?
For example, GSA may share data with the DOJ, only for investigation purposes. The full list of disclosures GSA is permitted to make under the Privacy Act is listed in the SORN under "routine uses":   https://www.federalregister.gov/d/2014-19071/p-26

4.3: Is the information collected:
From Another Source

4.3Other Source: What is the other source(s)?
Sources may vary widely as information is not collected by the system's applications specifically, but are used as a mechanism to store, collaborate and share information between users.

In cases where the system's application specifically collects personal information it would be collected directly from the individual.

BOT Name Vaccination Attestation GSA Roster Update: The narrative information in response to the Vaccination Attestation process is stored in Google Sheets. It is organized by employee name and GSA email address. Any attachments associated with the narrative information are stored in Google Drive.

4.4: Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?
No

4.4WhoHow: If so, who and how?

4.4Formal Agreement: Is a formal agreement(s) in place?
No

4.4NoAgreement: Why is there not a formal agreement in place?
GWE is not internally connected with any other systems with memoranda of understanding (MOU) or information sharing agreements (ISA). However, GWE does integrate with GSA's Active Directory (AD), which is under Enterprise Infrastructure Operations (EIO) FISMA and provides the access control list for GWE.

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?

Sources may vary widely as information is not collected by the system’s applications specifically, but are used as a mechanism to store, collaborate and share information between users.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
All GSA users including contractors use GWE for email, collaboration and sharing of information. As such, the applications (Email, Sites, Docs, Calendar, and Drive & Hangouts) do not collect any information, but it’s used as a means to store, share or house information of many types by all users in GSA. All personnel required to have background investigation completed before email access is granted. The GWE team verifies suitability of an employee or contractor before granting access to GWE from GSA Credential and Identity Management System (GCIMS) before granting access to email. To enable similar sharing and collaboration in Google with our non-GSA partners, these partners will use the GSA Affiliated Customer Accounts (GACA) process. GACA accounts allow GSA employees to share information on Google Drive or Google Sites with GSA external customers and business partners who do not have a gsa.gov email address.   Use of a GACA account has no impact on whether or to whom information can be shared. The determination of what can and cannot be shared using a GACA account is made on a case-by-case basis, looking at the type of information and the identity of the party with whom it is shared.

6.1b: What is the authorization process to gain access?
All personnel required to have background investigation completed before email access is granted. GWE team verifies suitability of an employee or contractor before granting access to GWE from GSA Credential and Identity Management System (GCIMS) before granting access to email. To enable similar sharing and collaboration in Google with our non-GSA partners, these partners will use the GSA Affiliated Customer Accounts (GACA) process. GACA accounts allow GSA employees to share information on Google Drive or Google Sites with GSA external customers and business partners who do not have a gsa.gov email address.

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
Yes

6.2a: Enter the actual or expected ATO date from the associated authorization package.
7/9/2024

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
GSA assesses information and systems for compliance risk, reputational risk, strategic risk, situational/circumstantial risk, and operational risk. In order to mitigate these risks to an acceptable level, GSA implements extensive security controls for information collected or maintained on its behalf, and conducts third-party assessments of vendors and services it procures. GSA leverages FedRAMP instance of GWE and it has been approved to use as SaaS from FedRAMP. GSA implements controls relevant to third party vendors and services according to risks identified the following types of third party reviews: Third Party Security Assessment and Authorization (SA&A) Package; Statements on Standards for Attestation Engagements (SSAE) Review; Risk Assessments by Independent Organization; or a complete Risk Assessment by GSA.

6.4: Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?
Yes

6.4What: What are they?
GSA has procedures in place for handling security incidents. GSA monitors use of its systems and is responsible for reporting any potential incidents directly to the relevant Information Systems Security Officer (ISSO). This Officer coordinates the escalation, reporting and response procedures on behalf of GSA.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
No opportunities exist to consent, or decline. Sources may vary widely as information is not collected by the system's applications specifically, but are used as a mechanism to store, collaborate and share information between users.

For initial use cases with personal information, users are still required to respond, but they may choose the option that is equivalent to declining to provide any personal information.

7.1Opt: Can they opt-in or opt-out?
No

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.
No opportunities exist to consent, decline or opt out. Sources may vary widely as information is not collected by the system's applications specifically, but are used as a mechanism to store, collaborate and share information between users.

For initial use cases with personal information, users are still required to respond, but they may choose the option that is equivalent to declining to provide any personal information.

7.2: What are the procedures that allow individuals to access their information?
Only cleared individuals are granted permission to the system after a successfully completed background investigation. Individuals do not access their personal information in GWE directly. Instead, individuals may update their personal information via HRLink and GCIMS. Access Logs are available for audit purposes. GACA account holders can view their own account information in Google but do not have access to an account in HRLink and GCIMS. These non-GSA partners will use the GSA Affiliated Customer Accounts (GACA) process to create GACA accounts and those account holders can access their own profiles in Google.

7.3: Can individuals amend information about themselves?
Yes

7.3How: How do individuals amend information about themselves?
An individual's information (e.g. profile display name) can only be changed via authoritative systems such as HR Links and GCIMS.
In the case of users providing personal information via the system's applications, the user will have access to update their personal information via modification to a Document, Sheet, etc. or amending responses submitted via Google Form.

8.0 Awareness and Training

8.1: Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.
GSA requires annual privacy, security training & collaboration sharing for all personnel and has policies in place that govern the proper handling of PII. This is managed through the CIO and Online Learning University (OLU) system.

9.0 Accountability and Auditing

9.1: How does the system owner ensure that the information is used only according to the stated practices in this PIA?
GSA requires privacy and security training for all personnel, and has policies that govern the proper handling of PII. GSA has also implemented security and privacy controls for its systems, including those that support design research, and has limited access to those personnel with a need to know. Further, OMB requires the GSA to document these privacy protections in submissions for Information Collection Requests processed under the Paperwork Reduction Act. All GSA systems are subject to periodic audits to ensure that GSA protects and uses information appropriately. As discussed above, GSA takes automated precautions against overly open access controls.