GSA Implementation of Google (G) Suite

Privacy Impact Assessment (PIA)

September 24, 2020

POINT *of* CONTACT

Richard Speidel

gsa.privacyact@gsa.gov

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Instructions for GSA employees and contractors:

This template is designed to help GSA employees and contractors comply with the E-Government Act of 2002, Section 208. GSA conducts privacy impact assessments (PIAs) for electronic information systems and collections in accordance with CIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices. The template is designed to align with GSA business processes and can cover all of the systems, applications, or projects logically necessary to conduct that business.

The document is designed to guide GSA Program Managers, System Owners, System Managers, and Developers as they assess potential privacy risks during the early stages of development and throughout the system, application, or project's life cycle.

The completed PIA shows how GSA builds privacy protections into technology from the start. Completed PIAs are available to the public at gsa.gov/pia.

Each section of the template begins with a statement of GSA's commitment to the Fair Information Practice Principles (FIPPs), a set of eight precepts that are codified in the Privacy Act of 1974.

Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response. Please note the instructions, signatory page, and document revision history table will be removed prior to posting the final PIA to GSA's website. Please send any completed PIAs or questions to gsa.privacyact@gsa.gov.

Stakeholders

Name of Information System Security Manager (ISSM):

- Nathaniel Ciano

Name of System Owner:

- Chris McFerren

Signature Page

Signed:

DocuSigned by:

Nathaniel Ciano

113E72276281433...

Information System Security Manager (ISSM)

DocuSigned by:

Chris McFerren

2961993077FB404...

Program Manager/System Owner

DocuSigned by:

Richard Speidel

171D5411183F40A...

Chief Privacy Officer (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

Document Revision History

Date	Description	Version
06/05/2020	Initial version on current template	1.0
8/20/2020	Updated	2.0
9/4/2020	Minor Update to Question 3.5	3.0
9/24/2020	All comments were addressed including Section D.	4.0

Table of Contents

SECTION 3.0 DATA MINIMIZATION

3.1 Why is the collection and use of the PII necessary to the project or system?

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

3.3 What controls exist to protect the consolidated data and prevent unauthorized access?

3.4 Will the system monitor members of the public, GSA employees, or contractors?

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

3.6 Will the data included in any report(s) be de-identified? If so, how will GSA aggregate or de-identify the data?

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, maintenance, use, or dissemination?

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 GSA verify the information collection, maintenance, use, or dissemination for accuracy and completeness?

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 (SSP) for the information system(s) supporting the project?

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

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

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, 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?

SECTION 8.0 AWARENESS AND TRAINING

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

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system owner ensure that the information is being used only according to the stated practices in this PIA?

Document purpose

This document contains important details about GSA's implementation of Google (G) Suite. GSA Office of Corporate Service may, in the course of G Suite, 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]

System, Application, or Project Name:

GSA Implementation of Google (G) Suite

B. System, application, or project includes information about:

- GSA Employees
- Contractors

C. For the categories listed above, how many records are there for each?

We estimate 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

GSA uses G Suite for email, collaboration and sharing of information. As such, the applications (Gmail, Sites, Docs, Calendar, Hangouts, and Drive) are used as a means to store, share or house information of many types by all users in GSA.

SECTION 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? If so, 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 G Suite comes from a varied source of extracts and sources. GSA primarily relies on G Suite 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 the Google Drive.

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

1.3 Has an 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.

No, G Suite is not an information collection for Paperwork Reduction Act purposes. If a Google form requires an ICR, the form creator must adhere to Regulatory Secretariat Division procedures and policy.

1.4 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.

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.

SECTION 2.0 OPENNESS AND TRANSPARENCY

2.1 Will individuals be given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

No, 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.

SECTION 3.0 DATA MINIMIZATION

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

G Suite 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, collaboration or simple storage. An employee could potentially enter PII into the system but the system itself does not collect it. None of these apps collect that information as part of the processes.

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

No, the system will not create or aggregate new data about the individuals.

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

Two factor authentication (2FA) 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?

No, the system will not.

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

Using the audit logs provided by G Suite 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, G Suite administrators can filter and generate a report by event name, user, IP address, date, disk space and email address.

3.6 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?

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.

SECTION 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. 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.

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?

Yes. For example, GSA may share data with DOJ, only for investigations 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 directly from the individual or is it taken from another source? If so, what is the other source(s)?

No, 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.

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

G Suite is not internally connected with any other systems with memoranda of understanding (MOU) or information sharing agreements (ISA). However, G Suite does integrate with GSA's Active Directory (AD), which is under Enterprise Infrastructure Operations (EIO) FISMA and provides the access control list for G Suite.

SECTION 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.

SECTION 6.0 SECURITY

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?

All GSA users including contractors use G Suite 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. G Suite team verifies suitability of an employee or contractor before granting access to G Suite 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.

6.2 Has GSA completed a System Security Plan (SSP) for the information system(s) or application?

Yes, GSA has completed a system security plan (SSP) for the systems that support and maintain the information used in G Suite. GSA categorizes all of its systems using Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems (FIPS 199). G Suite operates on systems rated “moderate impact.” Based on this categorization, GSA implements security controls from NIST Special Publication 800-53, “Recommended Security Controls for Federal Information Systems and Organizations” to secure its systems and data.

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 G Suite 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? If so, 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.

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? 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.

7.2 What procedures 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 G Suite 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, these 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? If so, how?

Yes, an individual's information (e.g. profile display name) can only be changed via authoritative systems such as HR Links and GCIMS.

SECTION 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.

SECTION 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.

[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.