GSA Implementation of Google (G) Suite

Privacy Impact Assessment (PIA)

June 06, 2019

POINT *of* CONTACT

Richard Speidel

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

Table of contents

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 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, 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 Google (G) Suite

System, application or project includes information about

GSA employees, Contractors

System, application or project includes

1. *App Scripts*
2. *Calendar*
3. *Chrome Browser*
4. *Drive and Team Drives*
5. *Email with Gmail*
6. *Groups*
7. *Hangouts Chat*
8. *Hangouts Classic*
9. *Hangouts Meet*

GSA uses G Suite for email, collaboration and sharing of information. As such, the applications (E-Mail, 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

GSA states its purpose and legal authority before collecting PII.

1.1 Why is GSA collecting the information?

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 collects that information as part of the processes.

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

44 U.S. Code § 3101. Records management by agency heads; general duties

5 U.S. Code § 301. Departmental regulations

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?

Yes, the system is searchable by a google account holder's name. Admins can deactivate certain accounts. That will not prevent a user from searching the deactivated users 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. Its primary purpose for being in G Suite is either for storage, sharing or collaboration. 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.

1.4. 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.

Yes, Contractor Information Worksheet; GSA Form 850, OMB Control Number: 3090-0283 with an expiration date of 7/31/2019.

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.

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 DAA-GRS-2013-0005-0008.

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

Controls have been put in place to prevent users from inadvertently sharing information with all members of the organization. Additionally, both employees and contractors are required to complete IT Security and Privacy Awareness training annually.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.

2.1 Will individuals be given notice prior to the collection and/or sharing 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.

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

The system is monitored, audited, and protected according to GSA IT policies and NIST requirements for IT systems. Additionally, scripts are in place for sites/groups to restrict Agency wide sharing of information and users are not allowed to create any new Groups or Sites.

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?

Federal employees and Contractors

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

The PII stored and shared using G Suite comes from a varied source of extracts and sources. Its primary purpose for being in G Suite is either for storage, sharing or collaboration. As the applications are not designed to specifically collect any specific information, it is up to users posting to ensure they only post such information as stated in SORN CIO-3 (http://www.gpo.gov/fdsys/pkg/FR-2013-06-11/pdf/2013-13813.pdf).

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

As users are the ones that can potentially cause an inadvertent sharing of information, it is the responsibility of the user to only share such information as required, on a need to know basis and only for the specified period required to support mission functions.

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?

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

3.5 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.

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

No, the system will not.

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

None.

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?

No.

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

G Suite provides auditing capability natively for G Suite core apps. Scripts are in place for sites/groups to restrict Agency wide sharing of information and users are not allowed to create any new Groups or Sites. GSA has implemented cloud lock to monitor drive data.

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

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. GSA may share data with DOJ, only for investigations 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)?

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, how and 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). Google form may be chosen by some at self discretion. If G Suite goes down, users won't have access. Moreover, GSA ENT accounts are part of AD team under Enterprise Infrastructure Operations (EIO) FISMA and if that goes down, users won't have access to G suite as well.

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?

*As users are the ones that can potentially cause an inadvertent sharing of information, it is the responsibility of the user to only share such information as required, on a need to know basis and only for the specified period required to support mission functions***.**

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?

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.

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?

The PII stored and shared using Google Apps comes from a varied source of extracts and sources. Its primary purpose for being in G Suite is either for storage, sharing or collaboration. This sharing and collaboration will be on a need to know basis and used only for Government related purposes in accordance with the GSA mission/tasks it supports.

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?

All GSA users including contractors use G Suite for email, collaboration and sharing of information. As such, the applications (E-Mail, 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.

6.2 Has GSA completed a system security plan 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, technological, 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 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.

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?

There is always some potential risk of unauthorized use or disclosure of PII. GSA mitigates the risk of breaches of PII by providing privacy and security training to GSA personnel on the appropriate use of information and implementing breach notification processes and plans.

In addition, access is limited on a need to know basis, with logical controls limiting access to data. GSA also automates protections against overly open access controls.

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 uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline 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. Access Logs are available for audit.

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

Yes, an individual's information can only be changed via authoritative systems such as HR Links and GCIMS.

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?

As users are the ones that can potentially cause an inadvertent sharing of information, it is the responsibility of the user to only share such information as required, on a need to know basis and only for the specified period required to support mission functions. Controls have been put in place to prevent users from inadvertently sharing information with all members of the organization.

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.

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.

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?

No. Privacy and security awareness training is provided to all GSA users. All new employees and contractors must sign rules of behavior. Role based training is also offered at GSA on Identifying and Reporting Incident and Breaches.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

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 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.

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, persons performing accountability and auditing will have elevated privileges in the G Suite system.

To mitigate this risk, GSA clearly identifies personnel with the capacity to audit G Suite and provides them with appropriate role-based training. Auditors perform their duties in collaboration with GSA supervisors and/or GSA's Privacy Office. In addition, access to PII information is curtailed or aggregated as needed for the specific purpose of the audit being performed.

[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.