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: 424
System Name: Control Document Tracker (CDT)
CPO Approval Date: 4/4/2023
PIA Expiration Date: 4/3/2026

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:
Control Document Tracker (CDT)

B: System, application, or project includes information about:
CDT includes information about Controlled Documents. Controlled Documents include official agency correspondence to Members of Congress, other governmental agencies, key stakeholders, and constituents.

Controlled documents also include agency-initiated documents, including spend plans, prospectuses, orders, delegations of authority, internal policy, Instructional Letters, memorandums of agreement or understanding, and proposed regulatory changes. The various documents may reference members of the public, Federal, State, local, and foreign government officials, vendors, and contractors.

C: For the categories listed above, how many records are there for each?
There are a total of 43,000+- records in the system in its entirety. While some “may contain PII”, the majority of those records only contain information on GSA associates, as such is not considered PII.

D: System, application, or project includes these data elements:
Full Name, Physical Address, Personal and Work Phone Number, Personal and Work Email Address, Employer Information and address, for example, For Federal employees and contractors regarding facility or employment concern, Dun & Bradstreet and/or Tax ID Numbers

Overview:

System information includes correspondences and documents and, in addition to work contact information, may also include the following specific types of data: Personal full name, Personal physical address, Personal phone number, Personal email address, Employer information and address, for example, for Federal employees or contractors regarding facility or employment concern, Dun & Bradstreet and/or Tax ID numbers, Names and email addresses (personal or work) may be stored in searchable data fields, but other data would be contained in documents attached to system records.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
There are many legal authorities that allow or require GSA to track controlled documents and collect the PII they may contain, including but not limited to 5 U.S.C. 301 and 41 U.S.C. § 31.3101.

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?
SORN GSA/CIO-3, GSA Enterprise Organization of Google Applications and SalesForce.com applies to the information.

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.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
General Legal Advice Presidential Records a. Files dealing with policy, advice, special access, and disposal. Permanent N01-0064-2005-0001 Item 5a PERMANENT. Cut off annually. Transfer to NARA when 15 years old. (N1-64-05-1, item 5a)

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.
There is no collection of information but instead, information is voluntarily provided by the individual involved or provided to GSA on behalf of the individual from a Congressperson or the White House, by mail or email. Individuals supply the information they believe is needed to resolve their inquiry and permit follow-up contact by the Government. Referrals on behalf of the individual routinely contain signed privacy release forms. Especially sensitive information is reviewed and redacted or reviewed and sequestered from the system.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
Contact information, such as name and address (email or other), are needed to resolve the inquiry and communicate with the individual who made the inquiry. GSA cannot provide an answer if the individual involved is unknown or there is no way to contact the individual who requested the answer.

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?
CDT does not aggregate or create new data about individuals that could be used to identify individuals. Each CDT package is managed separately. All access to CDT is granted via a request made by an Exec Sec Admin to the GSA IT Service desk (Service Now), which is then approved by the Google Cloud Platform minor application owner. Once approved, the user is then granted role-based access to the system by system administrators.

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

3.4 Explain: Please elaborate as needed.
No, the system does not monitor the public, employees or contractors.

3.5 What kinds of report(s) can be produced on individuals?
The only reports that can be produced on individuals are when the individuals are GSA employees or GSA contractors who are system users. Reports cannot be produced on individuals whose requests are being tracked in CDT. The requestor’s name is not included in any data field.

3.6 Will the data included in any report(s) be de-identified?
No

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?

3.6 Why Not: Why will the data not be de-identified?
Control Document Tracker reports do not contain data fields with PII, therefore, we will not be de-identifying any reports data.

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?
Yes

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?

As part of sharing resolution of the inquiry with the entity that had made the request on behalf of the individual, GSA may occasionally need to share personal information (such as a name of business at which the individual is employed) to the original congressional or White House requester. In this situation, GSA would actually be sharing such information only with the entity that had originally provided it to GSA.

4.3: Is the information collected:
Directly from the Individual

4.3Other Source: What is the other source(s)?

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?
Information is being directly provided by the individuals or indirectly provided by parties acting on behalf of the individual and whom the individual had contacted. It is the responsibility of the individual to assure the data provided is correct

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
The Program Manager and Application Owner are responsible for ensuring data is monitored for relevance and accuracy. In addition, the information is being directly provided by the individuals or indirectly provided by parties acting on behalf of the individual and whom the individual had contacted. It is the responsibility of the individual to assure the data provided is correct. When an inquiry cannot be resolved, Exec Sec personnel will contact the requester (the individual or the White House or congressional requester) to confirm the relevant search information is correct. As long as there is sufficient information to respond effectively, there is sufficient data. When a response cannot be provided because of insufficient data, as noted above, steps are taken to obtain sufficient information to respond or to determine that no response can be made.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
CDT users who have a designated responsibility and have been granted access to the application.

6.1b: What is the authorization process to gain access?
All GSA users will have access to the application with secure auth SSO to create a controlled record. Specific roles(A smallgroup of Exec Sec Admins, representing the system owner, view all/modify some for control and monitoring will require authorization by the CDT application owner. To get access to the application with a specific role, the user will have to submit a request via a servicenow ticket.

All other users receive access to controlled document records one record at a time, to either approve or collaborate on the drafting and clearance. Access is shared withthese users by one of the following: Exec Sec,the Record owner, or an approver or collaborator who has access to the record. However, they must already have access to the application via one of the aforementioned permissions or processes. Designated app owners have control over approving/denying user access requests (via ServiceNow).

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

No

6.2a: Enter the actual or expected ATO date from the associated authorization package.

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
Practice least privilege permissions, where any user of the CDT Salesforce app will have only the minimum privileges necessary to perform their particular job function. Google Cloud Platform cloud logging within the Google Cloud Platform is implemented and is monitored by the CDT application team. The cloud platform along with GSA's implementation of security controls provides a robust security roles. The data is protected by multiple access controls to the data, including login controls, roles within the application. Program management has authority to grant access to the application at all application levels. All higher level system support staff are granted access based upon need to know/requirement based needs.

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?
The CDT application is hosted on the Google Cloud Platform. The cloud platform along with GSA's implementation of security controls provides a robust security roles. The data is protected by multiple access controls to the data, including login controls, roles within the application. Access to the GSA ORG unit is reviewed on a weekly basis, application permission sets are annually reviewed by the application owner. The CDT application team follows the GSA IT Security Procedural Guide: Incident Response (IR) CIO-IT Security-01-02 for identifying, reporting and responding to security incidents and breaches of PII.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
GSA does not actively solicit any information from individuals. Any information submitted by individuals (personal or otherwise) is completely voluntary.

7.1Opt: Can they opt-in or opt-out?
Yes

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.

7.2: What are the procedures that allow individuals to access their information?
Should an individual request access to their information, it can and would be provided, in accordance with GSA's Privacy Act Rules at 41 C.F.R. 105-64 et seq..escribe any procedures or regulations that allow an individual access to information collected and/or the accounting or disclosures of that information. These procedures should include GSA's Privacy Act Rules. If an individual cannot access their information through the Privacy Act request process, state why.

7.3: Can individuals amend information about themselves?
Yes

7.3How: How do individuals amend information about themselves?
Individuals supply the original information. If information relevant to the inquiry is incorrect, it would be amended as part of the inquiry resolution.

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.
All GSA employees and contractors with access to this system are required to complete IT Security Awareness and Privacy Training on an annual basis. Users who fail to comply may have all access to GSA systems revoked.

Additionally, approved GSA associates who upload documents to CDT receive initial and refresher training on securing PII.

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?

As an application hosted on Google Cloud Platform. Google Cloud Platform cloud logging is available for activity audits. Designated app owners have control over approving/denying stakeholder user access requests (via ServiceNow).Access controls are monitored in accordance with GSA IT Policy.