Controlled Document Tracker (CDT)

Privacy Impact Assessment

November 1, 2018

POINT *of* CONTACT

Richard Speidel

Chief Privacy Officer

GSA IT

1800 F Street, NW

Washington, DC 20405

richard.speidel@gsa.gov

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 the Controlled Document Tracker (CDT) application. The Office of Administrative Services (OAS) may, receive and store documents that may contain personally identifiable information ("PII") from individuals who are requesting information or action from GSA.

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

Controlled Document Tracker (CDT) EEO Salesforce Minor App.

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.

System, application or project includes

System information includes correspondences and documents and, in addition to work contact information, may also include the following specific types of private 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 concerns; and
- 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.

Overview

The Controlled Document Tracker (CDT) is a workflow management system used by the General Services Administration (GSA) to manage, track, and record the timely drafting and approval of official agency correspondence to Members of Congress, Federal, state, local, tribal, and foreign government entities, key stakeholders, and constituents, GSA also uses CDT for the timely drafting, tracking, and approval of agency-initiated documents. Such documents would include but not be limited to spend plans, prospectuses, orders, delegations of authority, Instructional Letters, memorandums of agreement or understanding, and proposed regulatory changes. System workflows forward the documents to the appropriate offices and people in GSA for edits, commentary, and approval. CDT serves as an official system of record for GSA's Executive Secretariat ("Exec Sec") and other offices in the Central Office and the regions.

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 Why is GSA collecting the information?

GSA receives and tracks all relevant information about a controlled document, as provided by the requestor. It is up to the discretion of the requestor to decide what information (personal or otherwise) is relevant to the request.

1.2 What legal authority and/or agreements allow GSA to collect 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.

CDT is not an external facing system; instead it is an internal system of record to track Administrator and Head of Service and Staff Office correspondence and records related to managing the functions of GSA: https://www.gsa.gov/cdnstatic/OAS_P_1820.1_Records_Management_Directive_%28signed_3-7-2014%29.pdf

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?

Data is routinely retrieved by control number or by document signer. Document signers are always Federal employees. Retrieval can also be performed using a text search, and using name or address as the search criterion. GSA-OCIO-3, "GSA Enterprise Organization of Google Applications and SalesForce.com" is the SORN covering this 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.

No, OMB's ICR process is not applicable to GSA's CDT as it is not an information collection activity.

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.

The life expectancy will vary as required by National Archive and Records Administration regulations and GSA Records and Retention Policy. In general, NARA requires records, including general correspondence and decision files accumulated by the Office of the Administrator and Heads of SSOs for any major subject in managing and carrying out the functions assigned to GSA other than office administration, to be stored permanently. The system allows the flexibility for the Application Owner to request that entire records be deleted by a Salesforce administrator. This is performed only after first ensuring the NARA records requirements are met.

Where there is not an approved records retention schedule, Exec Sec has consulted with the agency records officer to develop a records retention schedule for the minimum amount of time necessary to fulfill the project's needs.

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

No. There is no “collection” of data. Requestors voluntarily submit information attached to a request that they decide to initiate.

There are potential privacy risks due to the type of information being submitted. CDT will mitigate those risks in the following ways:

1.) 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.

2.) Assign a record owner to each controlled document whose responsibilities include reviewing and redacting unneeded information (SSNs, birth dates, birthplace, parent or children names, etc.) from documents where such information is not needed to resolve the inquiry or preventing the documents from being uploaded to the system altogether if the information is required.

3.) Assign a designated application owner. That application owner will:

● receive auto-generated emails from the GSA Helpdesk (ServiceNow) to review and either approve/reject or ask for additional clarification for any pending tickets regarding system modifications (including adding users to access the application);

● attend Security de-briefs, to review and then digitally sign updated security packages as appropriate and outlined by their respective Security team;

● work with release managers to determine appropriate date/timing of deployment and any communication or training surrounding those changes.

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.

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 (see response 1.6.2) is reviewed and redacted or reviewed and sequestered from the system.

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

No. As discussed above, 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.

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?

Names and email addresses for Federal employees, vendors, contractors, and members of the public may be included.

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

System information includes correspondences and documents and, in addition to work contact information, may also include the following specific types of private 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 concerns;
- Dun & Bradstreet and/or Tax ID numbers; and
- 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.

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

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.

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

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 Salesforce minor application owner. Once approved, the user is then granted role-based access to the system by system administrators.

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

This control is implemented by the Salesforce Organization. Assigned authorizations for controlling access are enforced through Force.com Administration Setup Permission Sets & Public Groups.

1.) 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.

2.) Assign a designated application owner. That application owner will:

- receive auto-generated emails from the GSA Helpdesk (ServiceNow) to review and either approve/reject or ask for additional clarification for any pending tickets regarding system modifications (including adding users to access the application);

- attend Security de-briefs, to review and then digitally sign updated security packages as appropriate and outlined by their respective Security team;

- work with release managers to determine appropriate date/timing of deployment and any communication or training surrounding those changes.

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

No, the system does not monitor the public, employees or contractors. All logs of internal GSA associates who access the system are reviewed on a monthly basis per GSA policy.

3.7 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, as requestor name is not a data field.

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?

Controlled Document Tracker reports do not contain data fields with PII, therefore, we will not be de-identifying any reports data.

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

Exec Sec reviews all controlled documents before uploading to the system to redact unneeded information (SSNs, birth dates, birthplace, parent or children names, etc.) from documents where such information is not needed to resolve the inquiry or, if the data is needed to resolve the inquiry, Exec Sec stores the document outside the system, providing access only on an as-needed basis.

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?

Any PII is submitted voluntarily by the requestor, and not at the request of GSA. Therefore, any PII collected is deemed relevant to the request, by the requestor.

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?

No. 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 or is it taken from another source? If so, what is the other source(s)? 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.

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?

No. The CDT application has no internal or external connections to other systems.

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?

Not applicable as there is no external information sharing.

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?

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.

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?

No, as each GSA Program Manager and System Owner is responsible for maintaining the accuracy and completeness of the information under their control.

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?

- CDT users who have a designated responsibility and have been granted access to the application.
- Salesforce administrative staff also have access to the system. All Salesforce System Administrators are required to have a GSA Short Name Account (SNA). The SNA is used to grant administrative access to workstations, servers, or sensitive applications. Salesforce System Administrators need administrative access to Salesforce orgs and minor applications in order to provide support to Salesforce users and their associated permissions, groups and sharing rules. Additionally, they require administrative access in order to effectively perform Salesforce deployments and data loads. Salesforce System Administrators are required to login with a SNA token to keep their administrative duties separated from their regular duties. System changes made by these users will be tracked by Created By & Modified By fields. Login activity to the ORG is reviewed by the ISSO, per GSA Policy, on a weekly basis. Additionally logs are downloaded and archived/reviewed on a monthly basis. Any unauthorized activity is reported to the Information System Security Manager (ISSM) and the GSA IT Service Desk upon discovery.

All access is granted via a request made by the to the GSA IT Service desk (Service Now) which is then approved by the Salesforce minor application owner. Once approved, the user is then granted role-based access to the system by system administrators.

This application is hosted in the Employee Engagement Org (EEO) of Salesforce. All GSA employees and contractors who require access to this application must have either a Salesforce or Salesforce Platform license within EEO as well as one of the custom CDT Permission Sets in order to have access to this application

System Admins receive view/modify all access. A small group of Exec Sec Admins, representing the system owner, view all/modify some for control and monitoring. 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 with these 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 permission sets or processes.

Designated app owner has control over approving/denying user access requests (via ServiceNow).

- 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.

- Salesforce system administrators operating within the Salesforce EEO org are required to have Tier 2S clearance to be granted their designated SNA account/credential. All System Administrators are required to access the system with provided SNA credentials. Designated by OPM, Tier 2S clearance is a moderate risk (formerly MBI Level 5B) required for Non-Sensitive Moderate Risk (Public Trust) positions.

Using the aforementioned Profiles & Permissions the application allows users across GSA to set up primary controlled document records, and manage the collaboration, approval, and concurrence processes needed for the primary record. The application leverages a custom Salesforce.com data object to store information about the primary records, leverage Salesforce.com sharing settings and criteria-based sharing rules to control visibility and access to the primary records, and utilize a Visualforce user interface to allow users to add approvers and designate different approval types from one centralized approval step screen.

Users’ access to data is controlled by a combination of factors: alignment to an Exec Sec Admin Public Group, being owner or approver to a record, whether a record is manually shared with, etc. See the below paragraphs for detailed explanation on how this is restricted and controlled.

The primary data object, “Controlled Document”, is set as private in the organization-wide default setting. This will also be set irrespective of the role hierarchy. This ensures that records are private between users and offices. Role hierarchy is not in consideration since role hierarchy in the GSA EEO is not set up or maintained with authoritative data.

Since “approval step” is a detail object to “controlled document” in a master-detail relationship, these records will inherit the access level from the master object “controlled document”. All Chatter feeds and files will also inherit the primary record’s access level.

There will be four permission sets (PS) for this application. One PS provides Create-Read-Edit (CRE) access to the majority of users. A second PS gives Exec Sec Users access to more fields than the office level users. The third PS will be used by the “ExecSec Admin” users, who will be allowed to delete records. The fourth permission set, “Controlled Document Tracker - OCIA - CRE”, is used by OCIA users to access only Contract Award Notification functionality which does not include any PII and is publicly available information. All users will need the Salesforce Platform license at the minimum. Users who are on Salesforce license do not need to be downgraded. However users who are on Chatter Free license need to get upgraded to a Platform license and profile in order to have access to this application.

Per GSA Salesforce Technical Guideline, profiles "GSA System Administrator", and “GSA System User” will receive access to all objects and fields at the profile level. These administrative profiles also will have modify all/view all access to all records in this application. This is an existing construct that will not be altered through this project.

There are three criteria-based sharing rules that grant access to Exec Sec users via public groups (PG).

- One sharing rule grants access to Exec Sec USERS (PG: Controlled Document Tracker-Exec Sec User) when “allow Exec Sec Access” is selected.
- The second sharing rule grants access to Exec Sec ADMINS (PG: Controlled Document Tracker-Exec Sec Admin) when “allow Exec Sec Access” is selected.
- The third rule shares CDT records that contain C in the Document ID with the "Controlled Document Tracker-Exec Sec Admin" group with the exception of offices B and C.

Read/Write is granted in all sharing rules.

The application allows record owners to share records to other users on an ad-hoc basis with those people that have a business need to know. This is needed to meet access needs that fall outside of the sharing rules and Apex sharing criteria. This also provides maximum flexibility to record access control.

The application shares records with users who are designated as approvers to the primary record. Approvers will receive read/write access to the primary record and related children/Chatter records.

Private records must be shared manually for anyone else to receive access.

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

Yes, Salesforce is an element in the Enterprise Application Services (EAS) SSP with an ATO expiration date of 3/21/2019.

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

As Salesforce is a cloud-based product, the minor application is protected by a multi-tiered security process. The cloud platform along with GSA's implementation of security controls provides a robust security profile. The data is protected by multiple access controls to the data, including login controls, profiles within the application and permission sets in the program. 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 suspected or confirmed security incidents and breaches of PII? If so, what are they?

Intrusion systems at the agency level provide a layer of security monitoring. Access to the GSA ORG unit is reviewed on a weekly basis, application permission sets are annually reviewed by the application owner.

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?

As with any application there are risks and GSA is required to follow all Federal mandates to secure information systems, regardless of PII status. By adhering to those mandates, GSA provides a high threshold of data security for data within its Information Systems.

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.

GSA does not actively solicit any information from individuals. Any information submitted by individuals (personal or otherwise) is completely voluntary.

7.2 What procedures 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.*.

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

Individuals supply the original information. If information relevant to the inquiry is incorrect, it would be amended as part of the inquiry resolution.

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?

Individuals who have submitted information have no access to data once it has been submitted since this is an internal application, but may be provided a copy as part of the inquiry resolution.

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.

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. High level system users receive annual role-based training for accessing systems with elevated rights. Those who fail to comply have access revoked.

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

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?

GSA employees and contractors who use 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. High-level system users receive annual role-based training for accessing systems with elevated rights. Those who fail to comply have access revoked. These trainings help users identify and report potential incidents and decrease the risk that authorized users will access or use the applicants' data for unauthorized purposes.

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?

Salesforce event monitoring is available for activity audits. Designated app owner has control over approving/denying stakeholder user access requests (via ServiceNow). Salesforce system administrators operating within the Salesforce EEO org are required to have Tier 2S clearance and use their designated SNA account. Access controls are monitored in accordance with GSA IT Policy.

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?

● Designated app owner has control over approving/denying stakeholder user access requests (via ServiceNow). App owners are required to conduct annual reviews of all users granted access to ensure continued/proper access it required.

● 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. App owners are required to conduct annual reviews of all users granted access to ensure continued/proper access is required

● Salesforce system administrators operating within the Salesforce PEO org are required to have Tier 2S clearance and use their designated SNA account.

[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.