GSA Privacy Impact Assessment (PIA): PIA-364

Created Date: 3/10/2022 3:45 PM Last Updated: 3/14/2022 2:54 PM

Instructions

Privacy Impact Assessment (PIA)

The Privacy Impact Analysis (PIA) questionnaire is applicable to information systems which store or process privacy data. The questionnaire collects information about the types of privacy data which are stored and processed, why it is collected, and how it is handled. A PIA is required based on the results of a Privacy Threshold Analysis (PTA) questionnaire that has been completed for the information system.

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the buttons at the bottom of the screen to save or exit the questionnaire. The 'Save and Close' button allows you to save your work and close the questionnaire. The 'Save and Continue' button allows you to save your work and remain in the questionnaire. The 'Cancel' button closes the questionnaire without saving your work.

00 Default Layout	**Workflow Status:**	99 Workflow Complete

PIA

General Information

PIA ID:	PIA-364	**PIA Status:**	Completed
Authorization Package (System Name):	Controlled Document Tracker (CDT)	**This is a RPA:**	No
Assessment Date:	3/14/2022	**Is Latest:**	Yes
FISCAL Year:	2022	**PIA Required (From Authorization Package):**	
Final FISCAL Year:		**PIA Expiration Date:**	3/14/2023
		Final PIA Expiration Date:	3/14/2023

Override / Reopen Explanation

Override FISCAL Year:		**Override PIA Expiration Date:**	
Reopened Explanation:			

Other Stakeholders

Stakeholders (not in Approval Process)

System Owner (SO):	McFerren, Chris A.	**Authorization Official:**	DelNegro, Elizabeth F

System Owner (eMail)

Name (Full)

Chris McFerren

Authorization Official (eMail)

Name (Full)

Elizabeth Delnegro

PIA Overview

A.System Name:	A. System, Application, or Project Name:	Controlled Document Tracker (CDT)
B.Includes:	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.Categories:	C. For the categories listed above, how many records are there for each?	There are a total of 44,000+- records in the system in its entirety. While some â€œmay contain PIIâ€, the majority of those records only contain information on GSA associates, as such is not considered PII.
D.Data Elements:	D. System, application, or project includes these data elements:	System information includes correspondences and documents and, in addition to work contact information, may also include the following specific types of data: â— Personal full name â— Personal physical address â— Personal phone number â— Personal email address â— Employer information and address, for example, for Federal employees or contractors regarding facility or employment concern â— Dun & Bradstreet and/or Tax ID numbers â— 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:		
PIA-0.1:	Is this a new PIA or Recertification request?	Annual Recertification
PIA-0.1Changes:	If you are reviewing this for annual recertification, please confirm if there are any changes in the system since last signed PIA?	Yes, there are changes

Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				

1.0 Purpose of Collection

PIA-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. Â§ 31.3101.
PIA-1.2:	Is the information searchable by a personal identifier, for example a name or Social Security number?		Yes
PIA-1.2a:	If so, what Privacy Act System of Records Notice(s) (SORN(s)) applies to the information being collected?		Existing SORN applicable
		PIA-1.2 System Of Record Notice (SORN) CR:	
PIA-1.2 System of Records Notice(s) (Legacy Text):	What System of Records Notice(s) apply/applies to the information?		Yes, SORN GSA/CIO-3, GSA Enterprise Organization of Google Applications and SalesForce.com applies to the information. Controlled document records (CDR) are each given a unique identifier (UI). Those UIs are the first of three primary methods for searching the system. The second primary search tool is for the GSA employee assigned to the CDR as the owner or assignee. The third primary search tool is by approver, which would also list only GSA employees. CDRs also contain a searchable summary field that contains a description of the issue and, if a Member of Congress made the request, will include the name of that Senator or Representative. CDT policy and practice prohibits the inclusion of any other name, whether member of the public or agency employee, to be contained in that field. Additionally, CDT documents, such as word docs and pdfs, may be titled with the last name of a Member of Congress. Salesforce permits searches of file names. As such, it is possible to create a listing of requests by Senator or Representative names.
PIA-1.2b:	Explain why a SORN is not required.		
PIA-1.3:	Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?		No
PIA-1.3 Information Collection Request:	Provide the relevant names, OMB control numbers, and expiration dates.		
PIA-1.4:	What is the records retention schedule for the information system(s)? Explain how long and for what reason the information is kept.		Several records retention schedules will be applied to content stored in this application. The common retention instruction is to retain these documents for 15 fiscal years and then accession them to NARA as permanent records. The information is retained as a record of the final document, letter, directive, report, or matter on the issue for later reference and as a record of approval or consensus or agreement

on behalf of GSA. Decisions, Issuances, and Directives Legal Citation: DAA-0269-2016-0006-0001 (269.11/010) Description: This series covers decision papers, interpretation of laws and directives, and issuances issued by Heads of Staff and Services Offices and the Administratorâ€™s Office, and security directives issued under the Information Security Oversight Orders (ISOO). Retention Instructions: Permanent. Cut off at the end of the fiscal year when issued. Transfer to NARA 15 years after cutoff. Annual Significant Reports and Studies Legal Citation: DAA-0269-2016-0006-0003 (269.11/020) Description: This series includes documents created in reporting on management improvement goals, progress reports, and accomplishments for GSA internal and external Government-wide programs. Also included in this series are special studies conducted at the request of the Congress, the Office of Management and Budget (OMB), or the Office of Personnel Management (OPM), and the GSA Annual Report issued by the Administratorâ€™s Office and related records. Retention Instructions: Permanent. Cut off at the end of the fiscal year that the report has been issued. Transfer to NARA 15 years after cutoff. Strategic Evaluation and Planning Records Legal Citation: DAA-0269-2016-0006-0006 (269.11/030) Description: This series is concerned with all documents created in studying, proposing, reviewing, and assisting in changes in organization, function, and relationships of services, staff offices and regional offices. Included are organizational proposals, justifications, analyses of present and proposed arrangements, workloads, staffing patterns, current and proposed organization charts, functional statements, management studies, strategic plans, and related records. The files include disapproved proposals, comments on other organization studies, and records related to the changes to the GSA Organization. Retention Instructions: Permanent. Cutoff 1 year at the end of the fiscal year when issued, Transfer to NARA 15 years after cutoff. Significant Prepared Communications Records Legal Citation: DAA-0269-2016-0007-0001 (269.12/010) Description: Speeches and communications by Heads of Staff and Service Offices (HSSOs) as well as the Administratorâ€™s office, biographies of Administrator, Regional Administrators, HSSOs, and Commissioners. Also included are record copies of GSA press releases; record copies of internal and external newsletters, and related records. Retention Instructions: Permanent. Cut off at the end of the fiscal year when issued. Transfer to NARA 15 years after cutoff. Legislative and Congressional Affairs Program Reports Legal Citation: DAA-0269-2016-0008-0003(269.13/020) Description: Documents created in preparing and disseminating information reflecting content and status of the GSA legislative program, including reports of general information on, or status of, the legislative program, correspondence, and

		related records. Retention Instructions: Permanent. Cut off at the end of the fiscal year when the report is issued. Transfer to NARA 15 years after cutoff. Annual and Semiannual Management Reports to the Congress and GAO/IG Act Report and Response to OIG Semiannual Reports Legal Citation: DAA-0269-2016-0003-0001 (269.14/010) Description: This series comprises regular reports made to external agencies (such as the Congress, etc.). This report describes, for that specific reporting period, (1) the implementation of the recommendations by GSA Management contained in audit reports issued by the Office of the Inspector General (OIG), and (2) a report of cases where final action has not been taken on an audit one year after the date of the management decision. Retention Instructions: Permanent. Cut off at the end of the fiscal year after the report is issued. Transfer to NARA 15 years after cutoff.

2.0 Openness and Transparency

PIA-2.1:	Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them?	Yes
PIA-2. 1Explain:	If not, please explain.	

3.0 Data Minimization

PIA-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.
PIA-3.2:	Will the system, application, or project create or aggregate new data about the individual?	No
PIA-3. 2Explained:	If so, how will this data be maintained and used?	
PIA-3.3:	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.
PIA-3.4:	Will the system monitor the public, GSA employees, or contractors?	None
PIA-3. 4Explain:	Please elaborate as needed.	No, the system does not monitor the public, employees or contractors.
PIA-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 requestorâ€™s name is not included in any data field.
PIA-3.6:	Will the data included in any report(s) be de-identified?	No
PIA-3. 6Explain:	If so, what process(es) will be used to aggregate or de-identify the data?	
PIA-3.6Why Not:	Why will the data not be de-identified?	Controlled 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

PIA-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
PIA-4.2:	Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?	Other Individuals
PIA-4.2How:	If so, how will GSA share the information?	Yes. 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.
PIA-4.3:	Is the information collected:	Directly from the Individual
PIA-4.3Other Source:	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.
PIA-4.4:	Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?	No
PIA-4.4Who How:	If so, who and how?	
PIA-4. 4Formal Agreement:	Is a formal agreement(s) in place?	
PIA-4.4No Agreement:	Why is there not a formal agreement in place?	There are no internal or external connections to other systems.

5.0 Data Quality and Integrity

PIA-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

PIA-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.
PIA-6.1b:	What is the authorization process to gain access?	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. All access is granted via a request made 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 owners have 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. Usersâ€™ 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. Manually in this context means that no one can see any documents unless they are in the process chain or given explicit access to a document. That assignment would be granted within the system and would be exclusive to internal GSA associates/contractors. The "users" in question are all GSA individuals as this is an internal use system. See the below paragraphs for detailed explanation on how this is restricted and controlled. The primary data object, â€œControlled Documentâ€, 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 â€œapproval stepâ€ is a detail object to â€œcontrolled documentâ€ in a master-detail relationship, these records will inherit the access level from the master object â€œcontrolled documentâ€. All Chatter feeds and files will also inherit the primary recordâ€™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 â€œExecSec Adminâ€ users, who will be allowed to delete records. The fourth permission set, â€œControlled Document Tracker - OCIA - CREâ€, 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 â€œGSA System Userâ€ will receive access to all objects and fields at the profile level. These administrative profiles also will 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). â— One sharing rule grants access to Exec Sec USERS (PG: Controlled Document Tracker Exec Sec User) when â€œallow Exec Sec Accessâ€ is selected. â— The second sharing rule grants access to Exec Sec ADMINS (PG: Controlled Document Tracker-Exec Sec Admin) when â€œallow Exec Sec Accessâ€ is selected. â— 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.
PIA-6.2:	Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?	Yes
PIA-6.2a:	Enter the actual or expected ATO date from the associated authorization package.	3/25/2023
PIA-6.3:	How will the system or application be secured from a physical, technical, and managerial perspective?	As Salesforce is a cloud-based product, the minor application is protected by a multitiered security process. The cloud platform along with GSAâ€™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.
PIA-6.4:	Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?	Yes
PIA-6.4What:	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.

7.0 Individual Participation

PIA-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.
PIA-7.1Opt:	Can they opt-in or opt-out?	Yes
PIA-7. 1Explain:	If there are no opportunities to consent, decline, opt in, or opt out, please explain.	ISSO is to fill
PIA-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 GSAâ€™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 GSAâ€™s Privacy Act Rules. If an individual cannot access their information through the Privacy Act request process, state why.
PIA-7.3:	Can individuals amend information about themselves?	Yes
PIA-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

PIA-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

PIA-9.1:	How does the system owner ensure that the information is used only according to the stated practices in this PIA?	Controlled Document Tracker is identified as a Minor Application within Salesforce. Salesforce event monitoring is available for activity audits. Designated app owners have 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.