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: 372
System Name: Child Care Subsidy Case Management System (CCS)
CPO Approval Date: 6/2/2022
PIA Expiration Date: 6/1/2025

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:
Child Care Subsidy Case Management System (CCS)

B: System, application, or project includes information about:
Federal employees and their families that request financial assistance who have children enrolled, or who will be enrolled, in licensed or accredited family care homes or child care centers.

C: For the categories listed above, how many records are there for each?
8,290 Child Care Providers 17,443 Child Care Recipients/ Family Members (Spouse, guardian, etc) 309,682 Support Cases/ Applications/ Recertifications

D: System, application, or project includes these data elements:
Federal employees and their families that request financial assistance who have children enrolled, or who will be enrolled, in licensed or accredited family care homes or child care centers

Overview:

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
CCS is not an external facing system; instead it is an internal system of record to track CCS teams to review the records related to requests to provide child care.

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?
System of Records Notice (SORN) - GSA/CEO-1 80 FR 31905 July 6, 2015 Records may be retrieved by Agency employee names, Agency name, email address and case number. Retrieval can also be performed using a text search, and using name or email address as the search criterion. The Child Care Subsidy program is covered under FR-2008-04-25 (link). System is also covered under GSA-OCIO-3, "GSA Enterprise Organization of Google Applications and SalesForce.com".

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

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
Records will be archived in accordance with their disposition schedule. GSA records that do not have an approved disposition schedule will be retained until disposition authority is obtained from NARA in accordance with Implementing Schedules under 36 CFR 1226.14. Additionally for internal reporting and handling of records on these transactions with other agencies: GRS 04.2/130 (DAA-GRS-2013-0007-0012) Personally identifiable information extracts. Description: "System-generated or hardcopy print-outs generated for business purposes that contain Personally Identifiable Information. Legal citation: OMB M-07-16 (May 22, 2007), Attachment 1, Section C, bullet "Log and Verify." Temporary. Destroy when 90 days old or no longer needed pursuant to supervisory authorization, whichever is appropriate. GRS 04.2/140 (DAA-GRS-2013-0007-0013) Personally identifiable information extract logs Description: "Logs that track the use of PII extracts by authorized users, containing some or all of: date and time of extract, name and component of information system from which data is extracted, user extracting data, data elements involved, business purpose for which the data will be used, length of time extracted information will be used. Also includes (if appropriate): justification and supervisory authorization for retaining extract longer than 90 days, and anticipated disposition date.

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? Yes

2.1 Explain: If not, please explain.

Information is voluntarily provided by the individual involved or provided to GSA by the individual via email. Individuals supply the information they believe is needed to resolve their inquiry and permit follow-up contact by the Government.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
There are certain eligibility rules and prescribed child care programs involved with the Child Care Subsidy Program as defined here - https://www.opm.gov/policy-data-oversight/worklife/dependent-care/#url=Child-Care-Subsidy The application process requires the entry of the individual data in order to determine eligibility. In addition, the Social Security Number is required to report the subsidy on the employee's W-2 form. Each agency that offers child care subsidy benefits creates its own guidelines for administration. For example, USDA administers the programs on behalf of those agencies, following their established guidelines. GSA hosts the system that USDA uses to manage the program.

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?
CCS does not aggregate or create new data about individuals that could be used to identify individuals. All the data stored and provided by the requester is needed to process their request.

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 SalesForce.com Administration Setup Permission Sets & Public Groups.

- Practice least privilege permissions, where any user of the CCS Salesforce app will have only the minimum privileges necessary to perform their particular job function.
- 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.

3.4 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. All logs of internal GSA associates who access the system are reviewed on a monthly basis per GSA policy.

3.5 What kinds of report(s) can be produced on individuals?
CCS can create reports relating to service(s) requested by an Agency Employee. The record can include documents provided by the Agency Employee. For example, these reports can be used to measure GSA's timeliness when responding to requests, an accounting of the total number of applicants, and listing of current providers. Application activity logs can be produced when needed and are specific to users of the application. Such reports would include listing of records viewed or edited by a given user, timeliness of database transactions, etc.

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?
CCS aggregates data and de-identifies families and providers to produce metrics such as Number of Cases by Status and Number of Cases Received by Day. Other reports, such as those referenced above, do not de-identify families or providers.

3.6 Why Not: Why will the data not be de-identified?
No

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?
Information is being directly provided by the individuals. Members/Employees submit applications to USDA following the procedures outlined in the application form identified in the Overview. Once the data is received in documentation format, Child Care Subsidy staff enter the individual fields into the system. The individual member/employee provides the information, but not directly into the application. Any PII is submitted voluntarily by the requestor and is needed to process the request. Therefore, any PII collected is deemed relevant to the request, by the requestor.

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?
Yes

4.4WhoHow: If so, who and how?
Yes. GSA staff access CCS information and the data is shared with GSA's Pegasys financial management system. Each month, the child care provider and the employee sign and submit the invoice. The GSA Child Care Subsidy Program administrators will enter the invoice data into the system. The actual invoice is archived in the ImageNow system and the invoice data is transferred to Pegasys for processing after approval by the CCS Invoice Administrator in the system (this portion of the process does not take place on Salesforce). The Invoice Administrator may reject the invoice and in that case, it would not be entered into CCS or sent to the GSA financial system. The only disclosure that the CCS application makes outside of GSA is sending the payment file containing accepted CCS invoice records to GSA's financial system for processing via the back end automated process. The data in the payment file transmitted to the financial system contains the parent's last name as part of the invoice number to ensure proper payment.

4.4Formal Agreement: Is a formal agreement(s) in place?
Yes

4.4NoAgreement: Why is there not a formal agreement in place?

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. It is the responsibility of the individual to assure the data provided is correct. If an individual mis-entered information, they may resubmit forms and attachments as necessary. As a matter of practice, old form attachments are kept but underlying system data is overwritten to reflect the accurate state. The information is also peer reviewed by CCS Program administrators along with the following error checks.
- The CCS provider vendor code and address code are checked against the USDA financial system to include whether the provider is in an active status. Each GSA employee's SSN will be validated in the exchange with the PAR system. If the SSN or name is incorrect, the data exchange with PAR will fail and a person will have to review and correct the data manually.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?

- Application roles are granted to individuals after the submission of an Enterprise Access Request System (EARS) form. EARS captures the request for the individual including the role they are requesting in the application. The request is processed through a workflow including approval by authorized personnel. After the EARS request is approved, a database administrator will create the user account and assign the appropriate roles based on the EARS request. This process ensures that users only gain access to the data and operations that they require to perform their job in the process. Per GSA requirements, an annual review of accounts is performed to confirm the users with access are still valid. There are less than ten users who have access to this data.

- 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 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 Customer Engagement Org (CEO) of Salesforce. All GSA employees and contractors who require access to this application must have either a Salesforce or Salesforce Platform license within the CEO as well as one of the custom CCS Permission Sets in order to have access to this application.

- Designated app owners have control over approving/denying user access requests (via ServiceNow).

- Practice least privilege permissions, where any user of the CCS Salesforce app will have only the minimum privileges necessary to perform their particular job function.

- Salesforce system administrators operating within the Salesforce CEO 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.

- 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 modify all/view all access to all records in this application. This is an existing construct that will not be altered through this project.

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 17 Version 3.1: February 20, 2020 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.

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

6.2a: Enter the actual or expected ATO date from the associated authorization package.
3/31/2021

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 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 and respond to suspected or confirmed security incidents and breaches of PII?
Yes

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

7.1: What opportunities do individuals have to consent or decline to provide information?
Disclosing information to CCS is voluntary, as stated in the application package. Individuals who have questions or concerns about the submission requirements can contact the CCS: https://insite.gsa.gov/topics/hr-pay-and-leave/worklife-programs/child-care-for-gsa-employees contains contact information for the program administrators. After an employee contacts the program, the program administrator will send application packet and additional information is available in the System of Records Notice (SORN):
https://www.gsa.gov/portal/getMediaData?mediaId=124926

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?
The SORN requires the individuals to address requests to the system manager of the application for access to their own information. Individuals may reach out to the GSA Child Care Subsidy point of contact via this website, https://insite.gsa.gov/topics/hr-pay-and-leave/worklife-programs/child-care-for-gsa-employees

7.3: Can individuals amend information about themselves?
No

7.3How: How do individuals amend information about themselves?

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

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?
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 CEO org are required to have Tier 2S clearance and use their designated SNA account. Access controls are monitored in accordance with GSA IT Policy.