Child Care Subsidy

Privacy Impact Assessment

June 10, 2019

POINT *of* CONTACT

Richard Speidel

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

Table of contents

SECTION 1.0 PURPOSE OF COLLECTION

1.1 Why is GSA collecting the information?

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

1.3 Is the information searchable by a personal identifier, for example a name or Social Security number? If so, what Privacy Act System of Records Notice(s) applies to the information being collected?

1.4 Has any information collection request (ICR) been submitted to or approved by OMB? If yes, provide the relevant names, OMB control numbers, and expiration dates.

1.5 Has a records retention schedule been approved by the National Archives and Records Administration (NARA) for the information system(s)? Explain how long and for what reason the information is retained.

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

SECTION 2.0 OPENNESS AND TRANSPARENCY

2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about them? If not, please explain.

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

SECTION 3.0 DATA MINIMIZATION

3.1 Whose information is included in the system?

3.2 What PII will the system include?

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

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

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

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

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

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?

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

SECTION 4.0 LIMITS ON USES AND SHARING OF 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?

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?

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 *Child Care Subsidy (CCS). The FM and HR IT division* may, receive and store and collect personally identifiable information ("PII") about the people who are requesting information and action from GSA. PII is any information[1] that can be used to distinguish or trace an individual's identity like a name and address.

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

Child Care Subsidy (CCS)

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.

System, application or project includes

- Full Name
- Personal address
- Personal or work Phone number
- Social Security Number
- Agency Name
- Spouse or Partner Full Name
- Child(ren) enrolled
- Power of Attorney (POA) or Guardian (if different than Parent / Spouse)
- Childcare Provider
    - Name, eg Kindercare Arlington
    - Address
    - E-mail Address

- Fax Number
- Phone number

Overview

The Child Care Subsidy Administration Program, Pegasys Financial Services Financial Information & Operations Division, USDA - Office of the Chief Financial Officer use Child Care Subsidy (CCS) to administer the child care subsidy program and pay invoices to child care providers for eligible Members/Employees participating in the child care subsidy program. USDA pays the difference between the actual costs and the family portion. The Eligibility and Invoice Processing subsystem is used to manage and maintain case files and process invoice payments for the US Coast Guard and GSA families participating in the Child Care Subsidy program. The FM and HR IT Services Division owns the application and manages all activities associated with the operations and maintenance of the IT solution.

Forms are submitted via email by the Members/Employees for the participating agencies requesting child care support and USDA CCS program administrators enter the documentation into the CCS Document Management subsystem. Upon approval, the data is hand-entered into the Eligibility and Invoice Processing subsystem to allow for invoices to be processed on behalf of the beneficiary.

Childcare Family Applicant Forms for GSA employees (link)

- OPM Form 1643 (link)
- Application Addendum

Childcare Family Form Attachments

- Current Employee Pay & Leave Statement
- Current Employee Federal Tax Return Form-1040
- Current Spouse/Partner Pay Statements for a minimum of 15 consecutive days and/or their most current student school schedule and the GSA Certification of Higher Education Form 2015-11 (Mandatory as applicable – Included within this package)
- Federal Tax Return Form-1040 for Spouse/Partner (Mandatory as applicable, if filed separately)
- Provider Application OPM 1644 (link)

- A copy of Child Care Provider's License, Letter of Registration or Accreditation Certificate

Childcare Provider Forms/ Attachments

- Provider Application OPM 1644 (link)
- Copy of Childcare Provider's License
- Letter/ Certificate of Accreditation

The system records the service information for Agency Employee and is available to them upon request. The records are retained for 7 years.

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 Why is GSA collecting the information?

The information collected by GSA with regards to Agency employees is minimum required for GSA to assist the employee in providing requested services. If errant documents are sent to GSA as a part of an application or family renewal, those documents are deleted as a matter of general practice.

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

CCS is not an external facing system; instead it is an internal system of record to track CCS team to review the records related to request to providing child care.

5 CFR 792.204 - Agency responsibilities; reporting requirement. Used by the Child Subsidy Program for tracking the utilization of funds. The SSN is captured to identify the Member/Employee and enable the reporting of the subsidy for GSA Employees on federal tax returns reported out of the GSA payroll system. The collection of information is also authorized by Section 643 of Public Law 106-58.

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?

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".

1.4. 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 CCS 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.

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.

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

Privacy Risk: The data collected is required for the program. Since the packages are submitted to USDA via e-mail, there is risk of interception, disclosure or mis-entry of the data on the application.

Mitigation: The federal employee can submit the data from their government e-mail address and should use encryption methods provided by their government computers and e-mail systems to protect their sensitive information while it is in transit. Along with that, CCS practices least privilege permissions, where any user of the CCS Salesforce app will have only the minimum privileges necessary to perform their particular job function.

Also CCS application has 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.

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.

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 via email. This information is only accessed by those who need to review it.

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?

- Parent (the Member/Employee)
- Spouse or Partner
- Child(ren) enrolled
- Power of Attorney (POA) or Guardian (if different than Parent / Spouse)

The Eligibility and Invoice Processing subsystem also stores data on the child care provider companies, for example Child Care Provider Name, Address, Taxpayer Identification Number, Phone, Company Email.

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

The CCS application collects the following personal information that are stored on documents in the Document Management subsystem and as database fields in the Eligibility and Invoice Processing subsystem:

- Parent (the Member/Employee): SSN, Name, Work Address, Work phone, Work e-mail, Home Address, Home phone, and Home e-mail.

- Spouse or Partner: Name, Address, Phone, Email, Employer Name, Spouse/Partner's School Name
- Child(ren) enrolled: Name and Date of Birth
- Power of Attorney or Guardian (if different than Parent / Spouse): Name, Address, Phone, Email
- Childcare Providers: Provider: Name, Address, Taxpayer Identification Number, Phone, Email
- Historical documentation before July 2016 was collected and is stored in ImageNow (e.g. parents' tax returns) - this is outside of the Salesforce app and is not connected. There are no active deletes happening currently.
- Legal Documents with attributes including but not limited to name (e.g. Marriage License, Name Change, POA), to whom it applies (e.g. Parent, Child, Guardian), effective date and expiration date where applicable.

The Child Care Subsidy Program administrators determine the eligibility of the Member /Employee based on the data submitted.

The Child Care Subsidy program does not receive information from another system.

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

There are certain eligibility rules and prescribed child care programs involved with the Child Care Subsidy Program as defined on here - https://nfc.usda.gov/FSS/clientservices/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.

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

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

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.

- 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.

3.6 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?

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.

3.8 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?

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.

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

All information collected is necessary to provide service requested. 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.

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 is needed to process the request. 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?

Forms are submitted by the Members/Employees and then CCS program administrators enter the documentation into the CCS Document Management subsystem. Upon approval, the data is hand-entered into the Eligibility and Invoice Processing subsystem to allow for invoices to be processed on behalf of the beneficiary. Once an application or action request is received from a Member/Employee, the information from the documents

submitted is entered into the Eligibility and Invoice Processing subsystem by GSA Child Care Subsidy program administrators. When invoices are received by GSA staff, the invoice data is entered and it is shared with Pegasys for processing the payment and with PAR for recording the amounts in the employee record for the W-2 earning statement at the end of the year. The Social Security Number of the employee is required for this processing in order to process the earnings into PAR. The data is retained in CCS, Pegasys, and PAR per the financial management retention policies for at least six years. 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.

In addition, GSA may disclose system records in accordance with the routine uses listed in the GSA/CEO-1 SORN.

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. 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.

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?

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.

There are columns in the CCS database that are updated for the success/failure of the data being transmitted and these columns can be reset in order to send data again. The columns include the date and time the record was sent.

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?

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.

Access to the Salesforce Childcare Application is managed by a similar ticketing process. Access requests are submitted through the OCIO Task Tracking request form where they are routed to the application owner for approval. Upon approval, the user and related access permissions are provisioned. In the event that a user leaves GSA, their account is automatically disabled via a sync with Active Directory.

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. 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.

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. CCS applicants may re-submit information if the Program determines that documentation is incorrect or was errantly entered.

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?

- 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 CEO as well as one of the custom CCS Permission Sets in order to have access to this application.
- Designated app owner has 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 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.

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 3/20/2020.

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 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 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.

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

7.2 What procedures 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? If so, how?

Individuals do not have access to the application directly. They must obtain information from program administrators and each agency has a different path to obtaining the information. There are individual points of contact for assistance with the program. The POCs with phone numbers and e-mails are identified on GSA's intranet.

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. If a participant or applicant is concerned they can email or call their designated points of contact. All of the information is available on the public web site and a Contact Us page provides ways to get questions answered. There are individual points of contact for assistance with the program. The POCs with phone numbers and e-mails are identified on GSA's intranet.

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.

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 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.

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 CCS 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 CEO 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.