



Child Care Subsidy

Privacy Impact Assessment (PIA)

April 20, 2020

POINT of CONTACT

Richard Speidel

gsa.privacyact@gsa.gov

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

Instructions for GSA employees and contractors:

This template is designed to help GSA employees and contractors comply with the E-Government Act of 2002, Section 208. GSA conducts privacy impact assessments (PIAs) for electronic information systems and collections in accordance with CIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices. The template is designed to align with GSA business processes and can cover all of the systems, applications, or projects logically necessary to conduct that business.

The document is designed to guide GSA Program Managers, System Owners, System Managers, and Developers as they assess potential privacy risks during the early stages of development and throughout the system, application, or project's life cycle.

The completed PIA shows how GSA builds privacy protections into technology from the start. Completed PIAs are available to the public at gsa.gov/pia.

Each section of the template begins with a statement of GSA's commitment to the Fair Information Practice Principles (FIPPs), a set of eight precepts that are codified in the Privacy Act of 1974.

Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response. Please note the instructions, signatory page, and document revision history table will be removed prior to posting the final PIA to GSA's website. **Please send any completed PIAs or questions to gsa.privacyact@gsa.gov.**

Stakeholders

Name of Information System Security Manager (ISSM):

- Matt Reagan, matthew.regan@gsa.gov
- Donald Gehl, donald.gehl@gsa.gov

Name of Program Manager/System Owner:

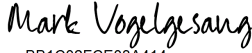
- Mark Vogelgesang - Mark.vogelgesang@gsa.gov

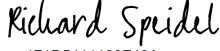
Signature Page

Signed:

DocuSigned by:

92526A8616CB470...
Information System Security Manager (ISSM)

DocuSigned by:

BB1C02FCE03A414...
Program Manager/System Owner

DocuSigned by:

171D5411183F40A...
Chief Privacy Officer (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

Document Revision History

Date	Description	Version of Template
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Added questions about third-party services and robotics process automation (RPA)	2.0
6/26/2018	New question added to Section 1 regarding Information Collection Requests	2.1
8/29/2018	Updated prompts for questions 1.3, 2.1 and 3.4.	2.2
11/5/2018	Removed Richard's email address	2.3
11/28/2018	Added stakeholders to streamline signature process and specified that completed PIAs should be sent to gsa.privacyact@gsa.gov	2.4
4/15/2019	Updated text to include collection, maintenance or dissemination of PII in accordance with e-Gov Act (44 U.S.C. § 208)	2.5
9/18/2019	Streamlined question set	3.0
2/20/2020	Removed email field from signature page	3.1

Table of contents

SECTION 1.0 PURPOSE OF COLLECTION

- 1.1 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
- 1.2 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?
- 1.3 Has an 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.
- 1.4 What is the records retention schedule for the information system(s)? Explain how long and for what reason the information is kept.

SECTION 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? If not, please explain.

SECTION 3.0 DATA MINIMIZATION

- 3.1 Why is the collection and use of the PII necessary to the project or system?
- 3.2 Will the system create or aggregate new data about the individual? If so, how will this data be maintained and used?
- 3.3 What controls exist to protect the consolidated data and prevent unauthorized access?
- 3.4 Will the system monitor members of the public, GSA employees, or contractors?
- 3.5 What kinds of report(s) can be produced on individuals?
- 3.6 Will the data included in any report(s) be de-identified? If so, how will GSA aggregate or de-identify the data?

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, maintenance, use, or dissemination?
- 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 GSA verify the information collection, maintenance, use, or dissemination for accuracy and completeness?

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 (SSP) for the information system(s) supporting the project?
- 6.3 How will the system be secured from a physical, technical, and managerial perspective?

6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, 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?

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system owner ensure that the information is being used only according to the stated practices in this PIA?

Document purpose

This document contains important details about *[system, application, or project]*. To accomplish its mission *[GSA office]* must, in the course of *[program name]*, 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]

A. System, Application, or Project Name:

Child Care Subsidy (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:

[Name and other biographic, demographic or biometric information (e.g., date of birth, age, gender, race, height, fingerprints, photos, or video);

Contact information (e.g., address, telephone number, email address);

Social Security Number (SSN), Driver's license number, passport number, or other government-issued identifiers or images of documents, etc.;

Financial Information (credit card/Payment Card Information (PCI), bank routing, tax identification number (TIN), etc.);

User and online information: a device or software-based information (including mobile device location, Global Positioning System (GPS), passwords, IP address, cookies and third-party services);

Information about individuals provided by third parties (e.g. credit reports, background investigation);

Other Information (health, medical information).]

- 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, e.g. 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

Child Care 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

Child Care 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 Employees 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 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.

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.

1.2 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?

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".

1.3 Has an 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.

1.4 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.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects, maintains, uses or disseminates as well as how it protects and shares it. It provides straightforward ways for individuals to learn how GSA handles PII.

2.1 Will individuals be given notice before the collection, maintenance, use or dissemination 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.

SECTION 3.0 DATA MINIMIZATION

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

[State why the collection of PII is necessary for the mission. For example, an explanation that the system collects name, date of birth, and biometrics in order to identify those individuals who enter GSA premises is adequate. However, merely stating that the above data will be collected to verify identity is insufficient.

When answering the question, explain why a collection of non-PII will not suffice.]

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? If so, how will this data be maintained and used?

[Today's systems and applications can often derive new data or create previously unavailable data about an individual through aggregation. The [mosaic theory](#) posits that disparate pieces of information, though not individually sensitive, can become sensitive when combined with other pieces of information that could result in unforeseen harm to individuals if misused.

Put another way, aggregation is taking various data elements and turning them into a composite to form another type of data, e.g., tables or data arrays. This composite may be different from the source information. Discuss whether the system will aggregate or derive data. In addition, discuss how this information will be maintained and used. If any new data should be considered PII, include those fields. For example, explain any new, unique identifier that is linkable back to a user.]

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?

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? 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.

SECTION 4.0 LIMITS ON USING AND SHARING 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 and how? Is a formal agreement(s) in place?

[Describe what this system, application, or project will interact with, either within or outside GSA. Describe how the data is transmitted. Is the data transmitted electronically, in bulk, by paper, direct access, or by some other means? Discuss whether access controls ensure appropriate sharing of information. State whether there is an MOU, contract, or agreement in place and define its sharing parameters.]

If data is being shared externally, discuss whether the receiving system or application has undergone a Security Assessment and Authorization (A&A). For sharing with non-Federal agencies, discuss how the relevant privacy protections have been expressed and documented to ensure the privacy and security of the information once it is shared. Discuss how external entities will notify GSA of a suspected or confirmed security incident or breach of PII.]

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.

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, 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.

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 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.

6.2 Has GSA completed a System Security Plan (SSP) for the information system(s) or application?

Child Care Subsidy is a Salesforce Minor application in the CEO ORG which falls under EAS (Enterprise Application Services); EAS SSP authorization expires March 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? 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.

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 do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, 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 emails 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.

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 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.

^[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.