Privacy Impact Assessment for the VA IT System called:

Child Care Records Management System (CRM)

EMPO Austin Information Technology Center (AITC)

Date PIA submitted for review:

09/09/2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rita K. Grewal	Rita.grewal@va.gov	(202) 632-7861
Information System Security Officer (ISSO)	Ahmed Tamer	Tamer.Ahmed@va.gov	(202) 461-9306
Information System Owner	Greg Watson	Gregory.Watson@va.gov	(512) 326-6889

Abstract

The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

The Child Care Records Management System provides Veterans Administration (VA) employees the ability to create an on-line application, via the VA intranet access, requesting childcare subsidy benefits and to scan in required documents to support that application.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The Child Care Records Management System (CRM) provides Veterans Administration (VA) employees the ability to submit an on-line application, via VA intranet access, requesting childcare subsidy benefits and to scan in required documents to support that application. VA employees will also be able to input their childcare provider's data into the system.

The program office that owns this system is Office of Human Resources and Administration.

CRM is operating under the legal authority of Public Law 1 06–58, Section 643, and Executive Order 9397: Numbering System for Federal Accounts Relating to Individual Persons, (https://www.federalregister.gov/articles/2008/11/20/E8-27771/amendments-to-executive-order-9397-relating-to-federal-agency-use-of-social-security-numbers) as stated in System of Records Notice (SORN) 165VA05CCSP-VA: VA Child Care Subsidy Program Records, (http://www.gpo.gov/fdsys/pkg/FR-2012-09-05/pdf/2012-21792.pdf)

CRM will provide control of records from creation, or receipt, through processing, distribution, organization, storage, and retrieval to ultimate disposition.

CRM uses web-based technologies that are hosted on virtual machines (VMs) in the Capitol Region Readiness Center (CRRC) VA datacenter to meet privacy and security standards established by VA guidelines. CRM does not conduct any information sharing.

CRM has the potential to be used by all VA employees. The current number of individuals whose information is stored in the system is up to 180,000 and growing. The system stores health and financial information about individuals.

CRM does not use cloud technology at this time.

The completion of this PIA will not result in the SORN, technology or business processes being changed.

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

☒ Name
☒ Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☒ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☒ Financial Account Information
☐ Health Insurance Beneficiary Numbers Account numbers
☒ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Current Medications
☐ Previous Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Other Unique Identifying Information (list below)

In addition, Child Care Records Management System (CRM) collects the following data:

Alias, Pay grade, total family income, names of children on whose behalf the parent is applying for subsidy, children's date of birth, childcare provider's tax identification numbers and copies of IRS Form 1040 and 1040A.

PII Mapping of Components

Child Care Records Management System (CRM) consists of 4 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Child Care Records Management System (CRM) and the functions that collect it are mapped below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

PII Mapped to Components

Components of the information system (servers) collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Production (database server)	Yes	Yes	Email Address, Provider Financial Account Information, Provider	Necessary for what the application does, provide	VA 6500 Controls in place Data is encrypted

			Certificate License Numbers, Alias, Pay Grade, SSN	childcare services	using FIPS 140-2 standard or equivalent
Production (database server)	Yes	Yes	Applicant's name, address, home phone	Necessary for what the application does, provide childcare services	VA 6500 Controls in place Data is encrypted
Production(database server)	Yes	Yes	Total Family Income, Names of children on whose behalf the parent is applying for subsidy, children's Date of Birth, including daycare provider's names & addresses	Necessary for what the application does, provide childcare services	VA 6500 Controls in place Data is encrypted
Production (database server)	Yes	Yes	provider license numbers and States where issued, and provider tax identification numbers and copies of IRS Form 1040 and 1040A	Necessary for what the application does, provide childcare services	VA 6500 Controls in place Data is encrypted

1.2 What are the sources of the information in the system?

List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

All information is received directly from the VA employee.

1.3 How is the information collected?

This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

All information is entered by the VA employee using the CRM application through a VA intranet web portal.

1.4 How will the information be checked for accuracy? How often will it be checked?

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

All information collected is for determining eligibility of participation in the program based on received financial data, qualified daycare, and parental information.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any

potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.
This question is related to privacy control AP-1, Authority to Collect

Public Law 1 06–58, Section 643. Executive Order 9397: Numbering System for Federal Accounts Relating to Individual Persons,
(https://www.federalregister.gov/articles/2008/11/20/E8-27771/amendments-to-executiveorder-9397-relating-to-federal-agency-use-of-social-security-numbers)
as stated in SORN 165VA05CCSP-VA: VA Child Care Subsidy Program Records,
https://www.govinfo.gov/

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk:

CRM collects both Personally Identifiable Information (PII) and a variety of other SPI, such as PHI. However, PHI is only used to for children participating in the program between the ages of 13 – 18 to provide medical documentation of a medical disability to continue participation in the program. This medical documentation information is provided by the parent from a medical doctor on a yearly basis to re-qualify for the program. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional or financial harm may result for the individuals affected.

Mitigation:

CRM employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. The VA's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. Many of the security controls are common security controls throughout the VA. These measures include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our security controls follow VA 6500 Handbook and NIST SP800-53 Moderate impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of the facility's common security controls. These are identified and described in the CRM system security plan.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained.
This question is related to privacy control AP-2, Purpose Specification.

All information collected is for determining eligibility to participate in the Child Care Subsidy Program (CCSP).
Full name: Used to identify the employee –Internal
Alias: Any alias used
Social Security Number (SSN): Used as an employee identifier and as a resource for verifying subsidy benefits received by participants throughout the calendar year to provide W-2 calculations are placed on correct Taxpayer Identification Number (TIN) which is used to identify child care provider taxes for the calendar year. -Internal
Date of Birth: Used to confirm employee identity -Internal
Maiden name: Used to confirm employee identity -Internal
Mailing address: Used to identify participate home mailing address and childcare vendor address. -Internal
Zip Code: Used to identify participate home mailing address and childcare vendor address. -Internal

Phone Number(s): Used to contact employees and childcare vendors, if necessary. -Internal
Fax Number: Used to contact employees and childcare vendors, if necessary. -Internal
Email address: Used to contact employees and childcare vendors, if necessary. -Internal
Financial account number: Used to identify account to transfer subsidy benefits to childcare provider on behalf of the VA employee. -Internal
Certificate/License number: Used to determine if the childcare provider is following state licensing and/or regulations pertaining to caring for children. -Internal
Pay Grade: Used as accounting data to measure the number of VA employees using the program in each grade group. -Internal
Total Family Income: Used to determine the percentage of total childcare costs VA will pay. -Internal
Names of Children: Used to determine the percentage of total childcare costs VA will pay. -Internal
Child(s) Date of Birth: Used to determine the percentage of total childcare costs VA will pay. -Internal
Name of Child Care Provider: Used to contact childcare vendors, if necessary. -Internal
Child Care Provider TIN: Used to ensure that W-2 calculations are placed on correct TIN which is used to identify childcare provider taxes for the calendar year. -Internal
IRS Tax Forms 1040 and 1040A: Used to determine the percentage of total childcare costs VA will pay. -Internal

2.2 What types of tools are used to analyze data and what type of data may be produced?

Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

CRM does not contain any tools to analyze data. CRM does not create or make available new or previously unutilized information about an individual.

2.3 How is the information in the system secured?

2.3a What measures are in place to protect data in transit and at rest?

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

Add answer here:

Formal, documented procedures to facilitate the implementation of the access control policies and associated access controls in: The VA Form 9957 process detailed in this SSP (Appendix A); and VA Handbook 6500.
Typical dissemination by the VA:
In order to gain access to the system, a 9957 must be filled out and sent to the Chief of Child Care Subsidy Program (CCSP). The Chief will review the 9957 and then add the user to the application with the role specified in the 9957.
The CRM PIA and SORN 165VA05CCSP-VA: VA Child Care Subsidy Program Records, are clear about the uses of the information. All Human Resource (HR) Specialists that use the system are granted access to enter the system and assist employees. The application administrator monitors and tracks access to PII. System training is held bi-annually to all point-of-contacts (HR Specialist) with access to CRM to ensure all system controls are in place. Routine uses of information in CRM through the SORN can be for purposes of Law Enforcement; Congressional Inquiry, Judicial/Administrative Proceedings; National Archives and Records Administration and General Services Administration; Statistical/Analytical Studies used by VA; Litigation;

Merit System Protection Board; Equal Employment Federal Labor Relations Authority and Non-Federal Personnel.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is retained by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

Full name, maiden name, mother's maiden name, alias, SSN, TIN, financial account number, mailing address, email address; date of birth, zip code, phone numbers, fax numbers, pay grade, telephone numbers, total family income, names of children on whose behalf the p arent is applying for subsidy, children's date of birth, information on child care providers used, including daycare provider's names, addresses, provider license numbers and States where issued, and provider tax identification numbers and copies of IRs Form 1040 and 1040A .

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

*The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.*

Information is retained until 3 years after leaving the program.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.
This question is related to privacy control DM-2, Data Retention and Disposal.

CRM records are retained in accordance with General Record Schedule 1 and the Office of Personnel Management Recordkeeping Manual as approved by NARA.
Yes, see below the items 120 & 121 where the CRM application is covered.
https://www.archives.gov/

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?
This question is related to privacy control DM-2, Data Retention and Disposal

After a 3-year period, the VA sanctioned destruction of paper and electronic records process in the form of shredding and program administrator the system for periodic purging.

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA 6500.1 HB Electronic Media Sanitization.

Disposition of Printed Data:
Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks and disposed of properly (when the approved records schedule permits destruction) by shredding or similar VA approved methods in accordance with VA Directive 6371. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

For training purposes, Human Resources (HR) Point of Contacts (POCs) do not use PII information of VA employees.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk:

The risk to maintaining data within CRM is the longer time frame information is kept, the greater the risk that information possibly will be compromised or breached.

Mitigation:

To mitigate the risk posed by information retention, CRM adheres to the VA RCS schedules for each category of data it maintains. When the retention data is reached for a record, CRM will carefully dispose of the data by the VA approved method.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.10 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Office of Finance	Financial Services Center (FSC	Personally, Identifiable Information (PII)	Encrypted email and access authorization using Network Identification (NTID) are all measures that are utilized within the facilities.

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk:

There is a risk that information may be shared with an unauthorized VA program, system, or individual.

Mitigation:

Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need to know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization using Network Identification (NTID) are all measures that are utilized within the facilities.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.11 on Privacy Threshold Analysis should be used to answer this question.
Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are shared/received with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

In order to protect Veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:
1. The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.
2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.
4. Internal protection is managed by access controls such as user IDs and passwords, authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:
Privacy Risk:

N/A

Mitigation:
N/A

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.

If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

At the beginning of the application process, employees receive notice of the use of information to determine program eligibility.

Additional notice is provided through this PIA, which is available online, as required by the eGovernment Act of 2002, Public Law 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs and the following VA SORN which is published in the Federal Register and available online:

SORN 165VA05CCSP-VA: VA Child Care Subsidy Program Records - Routine use of information in CRM through the SORN can be used for purposes of Law Enforcement; Congressional Inquiry, Judicial/Administrative Proceedings; NARA and General Services Administration; Statistical/Analytical Studies used by VA; Litigation; Merit System Protection Board; Equal Employment Federal Labor Relations Authority and Non-Federal Personnel.
https://www.oprm.va.gov/docs/Current_SORN_List_08_17_2021.pdf

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached.
This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress

Failure to submit required documentation to determine eligibility to participate in the program would result in denial of service. This is an opt-in program.
VA participants are allowed to make changes or corrections within his/her file by doing a formal change within the CRM to address any issues. All changes within the application establish a second review of the participant's application to ensure information added still maintains the individual's qualification to remain in the program.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use?
This question is related to privacy control IP-1, Consent

Failure to submit required documentation to determine eligibility to participate in the program would result in denial of service. This is an opt-in program. Only the VA employee is allowed to have direct access to the contents of his/her application information.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:

Privacy Risk:

Only assigned role users for the system are allowed access to participant's data in the system. There is a risk that VA employees, employee veterans and other members of the public will not know that the CRM exists or that it collects, maintains, and/or disseminates PII and other SPI about them.

Mitigation:

If an assigned user no longer requires access to the system, the user account can be de-activated by the program administrator.
CRM mitigates this risk by ensuring that it provides individuals notice of information collection and notice of the system's existence through the methods discussed in question 6.1.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

CRM is a Privacy Act System and not exempt from the access provisions of the Privacy Act. Any VA employee with an active VA network account may access CRM, via the VA intranet, to apply for childcare subsidy. A VA network user identification and password are issued only after proper clearance is verified and all VA required training is complete. The VA ensures that these requirements are met for each user on an annual basis.

Failure to submit required documentation to determine eligibility to participate in the program would result in denial of service. Childcare subsidy benefits is an opt-in program. VA participants are allowed to make changes or corrections within his/her file by doing a formal change within CRM to address any issues. All changes within the application establish a second review of the participant's application to ensure information added still maintains the individual's qualification to remain in the program.

SORN 165VA05CCSP states: Individuals wishing to request access to records about them should contact the system manager indicated. Individuals must provide the following information for their records to be located and identified: a. Full name b. Social Security Number. Individuals requesting access must also follow the Office of Personnel Management's Privacy Act Regulations regarding verification of identity and amendment of records (5 CFR, Part 297).

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

VA participants are allowed to make changes or corrections within his/her file by doing a formal change within CRM to address any issues. All changes within the application establish a second review of the participant's application to ensure information added still maintains the individual's qualification to remain in the program.
SORN 165VA05CCSP states: Individuals wishing to request amendment of records about them should contact the system manager indicated. Individual must furnish the following information for their records to be located and identified: a. Full name b. Social Security Number. Individuals requesting amendment must also follow the Office of Personnel Management's Privacy Act Regulations regarding verification of identity and amendment of records (5 CFR part 297).

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are notified of the procedures for correcting their information by SORN 165VA05CCSP

The SORN is published in Federal Registry and linked on the VA public website: https://www.oprm.va.gov/privacy/systems_of_records.aspx

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

VA participants are allowed to make changes or corrections within his/her file by doing a formal change within CRM to address any issues. All changes within the system establish a second review of the participant's application to ensure information added still maintains the individual's qualification to remain in the program.

Formal redress is provided in SORN 165VA05CCSP.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

<u>Principle of Individual Participation:</u> If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

<u>Principle of Individual Participation:</u> Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

<u>Privacy Risk:</u>

There is a risk that the employee provides inaccurate information that is required in order for their application to be approved.

<u>Mitigation:</u>

Information provided during the application process is verified by the employees HR department. If data is found to be missing or inaccurate, the HR employee working on the application will contact the employee and notify them, this will provide the employee the opportunity to resubmit the required documentation.

CRM mitigates the risk of incorrect information in an individual's records by authenticating information when possible using the resources discussed in question 1.5.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

Describe the process by which an individual receives access to the system.

Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Only a CCSP staff member with Administrator functionality in CRM can assign roles and or add/change role assignment.

This feature allows Program Analysts and CCSP Admins to maintain Admin users. Using the fields provided, users shall be added and assigned a Role. User information can also be updated or deleted using the icons within the action column. Note: Only CCSP Admins can add other CCSP Admins. The CRM application is role-based and consists of the following roles, which cannot be combined:

• HR Specialist – users assigned this role can complete application forms (0730a), upload supporting documents, enter childcare provider information, complete the HR checklist, and complete submit payment requests.
• Processor – users assigned this role can do everything an HR Specialist can, plus determine eligibility, approve/deny applications, process monthly payment request forms (0730h), and send out announcement emails. • Budget Analyst – users assigned this role can verify the subsidy payment information on the monthly payment request forms (0730h), manage actual payment amounts, and run reports.
• Program Analyst – users assigned this role can run reports (except audit reports), manage actual payment amounts, and manage user accounts (except CCSP Admin accounts).
• Program Support Specialist – users assigned this role can view all records in the system in order to research participant questions but cannot make changes. This is a read-only role.

• CCSP Admin – users assigned this role can perform all tasks of other roles in the system, manage CCSP Admin accounts, and generate audit reports.

• VA Employee – This is not an assigned role in the application, but noted in this PIA because all VA Employees, with an active directory ID, have access to submit an application for childcare subsidy through the User Interface.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes, VA contractors access CRM. The majority of the development team is comprised of contractors. The System Administrator team is also comprised of contractors. Access to the system for both teams is required for ongoing software development work to continue as well as for day to day maintenance of the systems and their networks.

Contractors can be granted access to CRM if their VA manager and local Information Security Officer approve. They are required to follow the same procedures VA employees do for access, which is to submit a 9957 form as specified in section 8.1. In addition, in accordance with the contract between the contractor and the government, all contractors with access to CRM information are required to meet the VA/CRRC contractor security requirements. Contracts are reviewed annually by the Contracting Officers Representative (COR).

VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Training is provided to all HR Specialist whom service as point-of-contact to assist employee's locally with the CCSP application process. Each HR Specialist is instructed to use his/her Network facility identifier to pull their participants out the system and within the provided "User Manual" describing security elements for the system.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the VA Privacy and Security Awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information. System administrators are required to complete additional role-based training. Users with access to PHI are required to complete HIPAA privacy training annually

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*

4. *The Authorization Date,*
5. *The Authorization Termination Date, .*
6. *The Risk Review Completion Date*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Authority to Operate was granted on April 25, 2019 for 3 years expiring April 24, 2022.

The FIPS 199 classification of the system is MODERATE

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517.

This question is related to privacy control UL-1, Information Sharing with Third Parties.

No

9.2 Identify the cloud model being utilized.

Example: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

N/A

9.3 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

9.4 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

N/A

9.5 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

9.6 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

N/A

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2021.09.29 16:28:21 -04'00'

Privacy Officer, Rita K. Grewal

Tamer F. Ahmed 531244

Digitally signed by Tamer F. Ahmed 531244
Date: 2021.09.29 13:02:30 -04'00'

Information Systems Security Officer, Ahmed Tamer

Watson, Greg E.

Digitally signed by Watson, Greg E.
Date: 2021.09.29 11:00:08 -05'00'

System Owner, Greg Watson

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

http://www.gpo.gov/fdsys/pkg/FR-2012-09-05/pdf/2012-21792.pdf

https://www.oprm.va.gov/docs/Current_SORN_List_08_17_2021.pdf