US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/03/2016

OPDIV:

ACF

Name:

Customer Inquiry Management

PIA Unique Identifier:

P-8441654-683956

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

Yes

Identify the operator.

Contractor

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

No

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The mission of the U.S. Department of Health and Human Services (HHS) is to enhance the health and well-being of Americans by providing for effective health and human services and by fostering sound, sustained advances in the sciences underlying medicine, public health, and social services. As an Operating Division (OPDIV) of HHS, the mission of the Administration for Children and Families (ACF) is to promote the economic and social well-being of children, youth, families, and communities, focusing particular attention on vulnerable populations such as children in low-income families, refugees, and Native Americans. ACF directly supports HHS' Strategic Goal 3: Advance the Health, Safety and Well-Being of the American People, further supporting the three Secretary's Priorities: 1) Put Children and Youth on the Path for Successful Futures, 2) Promote Early Childhood Health and Development, and 3) Ensure Program Integrity, Accountability and Transparency. The Office of Child Support Enforcement (OCSE) is the federal government agency that oversees the national child support program. We help child support agencies in states and tribes develop, manage and operate their programs effectively and according to federal law, through partnering with state, tribal and local child support agencies and others to encourage parental responsibility so that children received financial, emotional, and medical support from both parents, even when they live in separate households. We promote effective child support enforcement tools coupled with family-centered customer service.

The Customer Inquiry Management (CIM) System manages public inquiries about child support for different divisions across OCSE.

Describe the type of information the system will collect, maintain (store), or share.

The Customer Inquiry Management (CIM) system collects, maintains (stores) and shares the following data with State Child Support Agencies: First and Last Name, Social Security Number (SSN), Driver's License Number, e-mail address, phone number, Date of Birth, location (mailing address), financial account information, case numbers, employment status, user credentials, and any additional information the public chooses to share when completing their inquiry. Users that have login credentials include HHS employees and direct contractors.

The system contains questions and information about child support cases, stores inquiries from the public (received either directly or through the Executive Branch or Congress), and notes that the OCSE specialists make in order to manage public inquiries about child support for different divisions across OCSE.

There is a public facing website with an inquiry form that allows members of the public to submit their inquiry. Members of the public do not have login access to the CIM System and only see their own information provided on the inquiry form. Data within the CIM System, including submitted inquiries, is accessed by system users (HHS employees and direct contractors) through authorized and access-controlled user accounts.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The Customer Inquiry Management (CIM) system collects, maintains (stores) and shares the following data with State Child Support Agencies: name, Social Security Number (SSN), Driver's License Number, e-mail address, phone number, Date of Birth, location (mailing address), case numbers, employment status, and any other information the public might provide in their inquiries (Personally Identifiable Information (PII) and Non-PII) for identifying child support cases with state agencies and locating individuals. The system contains questions and information about child support cases, also stores inquiries from the public (received either directly or through the Executive Branch or Congress) and notes that the OCSE specialists make about the inquiry in order to manage public inquiries about child support for different divisions across OCSE.

When a login account needs to be created for system end users and administrators (includes HHS Employees and Direct Contractors), the name and email address is collected to create the login credentials. Public users are not required to login to submit an inquiry.

Since the system is only 2 years old, the data is kept in the system permanently. However, in the future there will be a discussion of possibly having a retention period of 5-7 years.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number

Date of Birth

Name

Driver's License Number

E-Mail Address

Mailing Address

Phone Numbers

Financial Accounts Info

Employment Status

User Credentials (username and password)

Case number

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Public Citizens

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The primary purpose for the CIM System collecting PII is for identifying child support cases with state agencies and locating individuals who owe child support.

Describe the secondary uses for which the PII will be used.

Not Applicable (N/A)

Describe the function of the SSN.

The purpose of the CIM System collecting social security numbers is to track down and to locate individuals who owe child support.

Cite the legal authority to use the SSN.

42 U.S.C. 9858i, 9858j

https://www.federalregister.gov/articles/2015/04/02/2015-07440/privacy-act-of-1974-system-of-records-notice

Identify legal authorities governing information use and disclosure specific to the system and program.

42 U.S.C. 9858i, 9858j

https://www.federalregister.gov/articles/2015/04/02/2015-07440/privacy-act-of-1974-system-of-records-notice

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

ACF System of Record Notification 09-80-0385 OCSE Federal Case Registry of Child Support

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Email

Online

Other

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

OMB CONTROL NUMBER: 0970-0177
EXPIRATION DATE: 09/30/2017
TITLE: OCSE-157 Child Support Enforcement Annual Data Report

OMB CONTROL NUMBER: 0970-0181
EXPIRATION DATE: 05/31/2017
TITLE: Child Support Enforcement Program Financial Report Child Support Enforcement Program Quarterly Report of Collection

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

State or Local Agencies

The PII will be shared or disclosed with State Child Support Agencies to locate individuals who owe child support.

Describe any agreements in place that authorizes the information sharing or disclosure.

The system does not integrate or have direct interface with any information technology systems for data and information exchange, necessitating establishment of any Computer Matching Agreements (CMA). Data is directly entered into the system by the system end user and is not derived from interface or upload from another information technology system or database. The system does not interface, integrate, or share data with any other information technology system or databases. Data is accessed by end users through authorized and access controlled user accounts. There is one page with an inquiry form that is made public so members of the public can submit their inquiry, however, the members of the public do not have access to any of the data or other functions of the system. Information is not shared outside of the system. No disclosure or sharing of PII is permitted or performed that is not governed by a formal agreement.

Describe the procedures for accounting for disclosures.

Any disclosure of PII outside of the system (e.g. sending names through email) is recorded and a report is generated. This report describes the date, nature, and purpose of each disclosure; and the name and address of the recipient.

Every time HHS makes an authorized disclosure of a record outside HHS for a reason other than the Freedom of Information Act (FOIA), the CIM System under HHS policy is required to and does document this disclosure within a system log providing the following information: The date, nature, and purpose of each disclosure; and The name and address of the recipient. HHS shall keep that document for five years after the disclosure occurred or the life of the record (whichever is longer). If the individual named in the record requests an accounting of disclosures, HHS shall provide the details of all disclosures except for certain ones which relate to civil or criminal law enforcement.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

The Customer Inquiry Management (CIM) system users will be notified that their information is collected for the purpose of creating a system user account to access the system. This notification will occur prior to the user account being created.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

When CIM System users (members of the general public) initiate a system inquiry the system prompts them for fields that contain their personal information. At this time the user can either choose to continue filling out the inquiry, and in doing so provide PII to the system, or choose to cancel the request thereby opting-out.

After access approval for system end-users and administrators (including direct contractors), the name and e-mail address is collected from end users for access control, and is based upon consent of the end users for creating an end user account. If the user is required to have a system account as part of their job duties, then they will not be able to opt-out of providing their name and email as these are required for account creation. Once the account has been created, the user then can choose whether to provide further personal information or not.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

The CIM System collects the following PII data from end users for access control: name, e-mail address, location (mailing address) and phone number and is based upon consent of the end users for creating an end user account. End users are notified by the system administrator via email and their consent is obtained from the individuals whose PII is in the CIM System when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection)

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

OSCE Customer Inquiry Management system collects the following PII data from end users for access control: name, e-mail address, location (mailing address) and phone number and is based upon consent of the end users for creating an end user account. There are processes in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. System users contact the system program manager or system administrator with concerns about their user account. At that time, the program manager and system administrator will work together to evaluate the user's concern, review the logs to determine if there is indeed an issue, and then work to resolve any concerns related to inappropriately used data or incorrect data. Once that is done, the user will be contacted and updated on the issue.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

The need and requirement for data integrity, availability, accuracy, and relevancy will be identified by system users and can be rectified by contacting the system program manager or system help desk with concerns about their user account. Also should the end user require an update to the PII data in the end user account (e.g. name, email address, location (mailing address) or phone number change) the end user can contact the system program manager or system administrators with concerns about their user account.

When a user leaves OCSE and no longer needs a user account, a written request to remove the user is sent out to the system administrator after approval from a manager. The administrator removes the user account and all related PII data.

There is a new process in place to review the list of users for Integrity, Availability, Accuracy and Relevancy. The user list is reviewed by the project manager or system owner to determine if any user data/access needs to be updated or removed. The manager then notifies the administrator of the updates needed to the Customer Inquiry Management user list. This process will take place on an annual basis.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

Needed to work on a case

Administrators:

Need access to resolve issues with the system

Contractors:

The administrators are direct contractors

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

End user accounts are requested through the program office system owner/program manager who reviews, authorizes and approves the creation of the end user account based upon the individual end user's roles and responsibilities associated with the OSCE Customer Inquiry Management system. End user roles and responsibilities will determine the type and content data and information necessary for job function (both PII and Non-PII). Role-based access will determine and control who will have access to PII. The authorized and approved account creation request is submitted to the OSCE Customer Inquiry Management, system administrator who creates the individual account and notifies the end user of the authorized, approved, and created account. The end user initially logs on, provides appropriate information to authenticate himself/herself enabling account access.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

End user accounts are requested through the program office system owner/program manager who reviews, authorizes and approves the creation of the end user account based upon the individual end user's roles and responsibilities associated with the OSCE Customer Inquiry Management system. End user roles and responsibilities will determine the type and content data and information necessary for job function (both PII and Non-PII). Role-based access will determine and control who will have access to PII. The authorized and approved account creation request is submitted to the OSCE Customer Inquiry Management, system administrator who creates the individual account and notifies the end user of the authorized, approved, and created account. The end user initially logs on, provides appropriate information to authenticate himself/herself enabling account access. Therefore access is role-based on only those will approved access are able to have access to the PII data is needed to work on a case.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

All Department users to include federal employees, direct contractors, and other system users must review and sign an acknowledge statement of the HHS Rule of Behavior (Rob). This acknowledgement must be completed annually thereafter, which may be done as part of annual HHS Information Systems Security Awareness Training. All users of Privileged User accounts for Department information technology resources must read these standards and sign the accompanying acknowledgement form in addition to the HHS RoB before accessing Department data/information, systems, and/or networks in a privileged role. End users are required to complete the following:

Annual HHS Information Systems Security Awareness Training;

Annual HHS Privacy Training; and Reading the Rules of Behavior for Use of HHS Information Resources and signing the accompanying acknowledgement.

Describe training system users receive (above and beyond general security and privacy awareness training).

Users receive documentation on the CIM System and learn from colleagues. This documentation includes user guides with step by step instructions on how to properly use the CIM System.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

OCSE is in communications with the ACF Records Manager to determine the specific National Archives and Records Administration (NARA) retention schedule. All records will be retained until a determination is made as to the final records disposition schedule. Once established the records will be disposition consistent with the records disposition schedule.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative controls, including but not limited to:
System security plan (SSP)
File backup/archive conducted by hosting agency (ServiceNow)
User manuals

Technical Controls:
User Identification and Authorization
Passwords
Firewalls at hosting site
Monitoring and Control scans provided by hosting agency
PIV cards (future plan)

Physical controls
The system servers are hosted in a secure data center and can be physically accessed by only the authorized infrastructure staff. Enforcement of established physical security capabilities (management walk-throughs and assessment of security locks, doors, desks, storage materials. Security Guards employing access controls to individuals requesting facility access. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. All physical access to data centers by employees is logged and audited routinely. Physical containment and isolation of Systems, Data bases, and Storage assets that collection, maintain, store, and share PII. Secured and limited access facilities: data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee. Compartmentalization and physical separation of system components (servers, cables, storage access, off-site backup facilities and storage). Employment of Locks, Fences, Geographic Isolation of physical system assets.

Identify the publicly-available URL:

https://ocse.service-now.com/wf/webform.do

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

No

Does the website use web measurement and customization technology?

No

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null