US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/16/2016

OPDIV:

ACF

Name:

Project Save Our Children

PIA Unique Identifier:

P-3374316-132963

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?

No

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 Secretary's 3 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. 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 receive financial, emotional, and medical support from both parents, even when they live in separate household. We promote effective child support enforcement tools couple with family-centered customer service.

In 1998 OCSE, in cooperation with the U.S. Department of Health and Human Services Office of the Inspector General (OIG) and the U.S. Department of Justice, created Project Save Our Children (PSOC) to coordinate efforts in support of activities resulting from the federal criminal non-support laws. The Child Support Recovery Act of 1992 made failure to pay child support a class B federal misdemeanor offense. The Deadbeat Parents Punishment Act of June 1998 created new categories of federal felonies for the most egregious child support violators. The Project Save Our Children System tracks enforcement requests received from a government official to get law enforcement involved in outstanding child support cases and supports the process for submitting appropriate cases for criminal prosecution.

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

The Project Save Our Children (PSOC) System collects, maintains (stores) and shares data within HHS; and with other Federal, State, and Local agencies tracking enforcement requests received from government officials to get law enforcement involved in outstanding child support cases and supports the process for submitting appropriate cases for criminal prosecution. The system collects the following data: the requester's first and last name (government official), requester's email address, the subject's first and last name, the subject's child support case ID, the subject's email address, the recipient's first and last name, recipient's email address, recipient's mailing address, the specific requests to law enforcement, system user phone number, and system user credentials (passwords). This data is directly entered into the system by the requester 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.

The user credentials collected are for system users and administrators that need access to the system and system information in order to complete their job duties. The email address of the user is used as their "username" and a system specific password is stored.

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

The Project Save Our Children (PSOC) System collects, maintains (stores) and shares data within HHS; and with other Federal, State, and Local agencies tracking enforcement requests received from a government official to get law enforcement involved in outstanding child support cases and supports the process for submitting appropriate cases for criminal prosecution. The system collects the following data: the requester's first and last name (government official), requester's email address, the subject's first and last name, the subject's child support case ID, the subject's email address, the recipient's first and last name, recipient's email address, recipient's mailing address, system user phone number, system user credentials (passwords), and the specific requests to law enforcement for the purpose of identifying individuals with outstanding child support cases requiring law enforcement.

All user credential and subsequent user PII is kept for only the length of employment. When an employee departs, their user account and all information is removed from the system. All case related data is currently kept on a permanent basis as the system is only 2 years old. The case data must be kept at minimum for the length of time the case is open. We are currently evaluating what type of retention process to adopt for closed case data.

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

Yes

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

Name

E-Mail Address

Mailing Address

Phone Numbers

Child Support Case ID

User Credentials

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

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The primary purpose of the PII collected, maintained, and stored in the PSOC system is to assist in identifying individuals with outstanding child support that requires law enforcement involvement and for the creation of system user accounts.

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

Not Applicable (N/A)

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

42 U.S.C. 652, 653, 664, and 666

https://www.federalregister.gov/articles/2015/04/02/2015-07440/privacy-act-of-1974-system-of-records-notice#h-18

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.

09-80-0383 OCSE Debtor File

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Other Federal Entities

Identify the OMB information collection approval number and expiration date

Not applicable.

Is the PII shared with other organizations?

Yes

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

Within HHS

To identify child support cases that require law enforcement

Other Federal Agencies

To identify child support cases that require law enforcement

State or Local Agencies

To identify child support cases that require law enforcement

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

The PSOC system shares information within HHS, and with other Federal, State, and Local agencies without any established formal agreements.

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.

No system user PII (i.e., name and email) will be disclosed outside of the system's direct purposes for controlled access.

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

After an employee requests access to the PSOC system, an email approval request is sent to the OCSE manager. After official written approval, the system administrator creates the user account then notifies the employee via email or phone to let them know that a system account has been created with their information.

There is no process in place to notify the requesters of the collection of their PII because the requests are submitted voluntarily.

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.

As a requirement, the system collects information on the subject and the subject's child support case ID. The PSOC system does not collect information directly from the individual and the individuals do not receive notification that their personal information is being collected. The subject does not have the option to opt-out of the use or collection of their PII because the information is entered into the system by a requester and is collected for tracking enforcement requests received from a government official to get law enforcement involved in outstanding child support cases and supports the process for submitting appropriate cases for criminal prosecution.

The requester's submit information voluntarily to the PSOC system. When a request is initiated, the requester then has the option to opt-out of providing PII.

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

As a requirement, the system collects information on the subject and the subject's child support case ID. The PSOC system does not collect information directly from the individual and the individuals do not receive notification that their personal information is being collected. The subject does not have the option to opt-out of the use or collection of their PII because the information is entered into the system by a requester and is collected for tracking enforcement requests received from a government official to get law enforcement involved in outstanding child support cases and supports the process for submitting appropriate cases for criminal prosecution.

Subject individuals are not notified and their consent is not required 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). As previously mentioned, notification and consent is not required for the subject's because the PII collected is required and is not provided directly from the subject.

PSOC collects system user first and last names and email addresses from the employees upon their consent and manager approval to create a system account. System users are notified by the system administrator and consent is obtained from these system users whose PII is in the PSOC 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.

As a requirement, the system collects information on the subject and the subject's child support case ID. The PSOC system does not collect information directly from the individual and the individuals do not receive notification that their personal information is being collected. The subject does not have the option to opt-out of the use or collection of their PII. The reason why the subject cannot opt-out is because the information is entered into the system by a requester and is collected on the subject for tracking enforcement requests for a government official to get law enforcement involved in outstanding child support cases and supports the process for submitting appropriate cases for criminal prosecution.

Subject individuals are not notified and no processes are 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.

PSOC collects system user first and last names and email addresses from the employees upon their consent and manager approval to create a system account. There are processes in place to resolve an user's concern when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. System users can contact the system administrator with concerns about their account information. Users can either contact via email by sending a message to an OCSE shared mailbox or by submitting a ticket on the OCSE SharePoint site. At that time, the system administrator and system program manager 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 via email or phone.

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 account. Also should the system user require an update to the PII data in the their account (e.g. name, email address, location (mailing address) or phone number change) the user can contact the system program manager or system administrators with their request.

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

There is a new process in place to review the list of system 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 PSOC system user list. This process takes 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.

System user accounts are requested through the program office system owner/program manager who then reviews, authorizes, and approves the creation of the account based upon the employees roles and responsibilities associated with the PSOC program. The authorized and approved account creation request is submitted to the PSOC system administrator who creates the account and notifies the employee of the authorized, approved, and created account. The employee initially logs on, provides appropriate information to authenticate himself/herself and therefore enables 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.

System user accounts are requested through the program office system owner/program manager who then reviews, authorizes, and approves the creation of the account based upon the employees roles and responsibilities associated with the PSOC program. The authorized and approved account creation request is submitted to the PSOC system administrator who creates the account and notifies the employee of the authorized, approved, and created account. The employee initially logs on, provides appropriate information to authenticate himself/herself and therefore enables account access.

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 the HHS Rules of Behavior (RoB) acknowledgment statement. This acknowledgment must be completed annually thereafter, which may be done as part of the annual HHS Information Systems Security Awareness Training. All system users with Privileged User accounts must read the Use of HHS Information Resources standards and sign the accompanying acknowledgment in addition to the HHS RoB before accessing Department data/information, systems, and/or networks in a privileged role. ECMRS 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 acknowledgment.

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

Cursory system user training is provided by the PSOC system administrator when a user account is first created and system access is granted. No specific or periodic, annual or refresher training is provided. There is no system-specific training for PII.

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 disposed of 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.

PII is secured using the following:

Administrative controls, including but not limited to:
System security plan (SSP)
File backup/archive

Technical Controls:
User Identification and Authorization
Passwords
Firewalls at hosting site
Monitoring and Control scans

Physical controls

The system servers are hosted in a secure data center and can be physically accessed by only the authorized infrastructure staff from ACF/HHS can access.
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.

All physical access to data centers by employees is logged and audited routinely.
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.