US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/09/2018

OPDIV:

ACF

Name:

Child Support Portal

PIA Unique Identifier:

P-6339911-476655

The subject of this PIA is which of the following?

Major Application

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

Describe the purpose of the system.

The Child Support Portal (CSP) provides OCSEs internal and external stakeholders access to web-based tools and functions that support OCSEs mission. The CSPs web-based functions also support OCSEs commitment to enhance services via real-time access to pertinent information. The CSP provides authorized users with interactive access to selected child support enforcement information. The CSP was previously covered under the Federal Parent Locator Services (FPLS) Enterprise Services Portal (ESP) privacy impact assessment (PIA), which was re-aligned and is now titled the OCSE Data Center (OCSE DC). The CSP provides many functions to the following stakeholders: employers, financial institutions and insurers, states, and the OCSE.

Employers use CSP web-based functions to provide the OCSE with their demographic, contact information, and employee status changes. Employers also use the CSP functions to provide a list of the states in which they operate and designate a single reporting state to submit new hire information to the National Directory of New Hires (NDNH).

Financial institutions and insurers use CSP web-based functions as a secure means to provide information on financial assets and potential insurance payouts for delinquent obligors.

States use CSP web-based functions to request and receive: child support case participant employment data, employee benefits data, employer demographic data, data on federal case collection remedies on delinquent obligors, state compliance reporting performance statistics, and NDNH data for research purposes. States use CSP functions to provide obligor information updates, federally required reports on state child support performance, and state contact information, and state child support policy information. States use also CSP functions to exchange interstate child support case information.

The OCSE uses CSP web-based functions to support and administer OCSE business functions. They also request and receive state-provided child support performance reports for auditing purposes.

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

The system will collect, maintain, and store the following information relating to user registration for access to the platform and subsequent services: first and last name, last four digits of Social Security Number (SSN), date of birth (DOB), mailing address, federal employer identification number (FEIN), user ID, password, and answers for 5 out of 11 challenge questions. In addition some federal tax information is collected, however this excludes any financial account or identifying numbers. Employer users must also provide their employer's name and business contact information for registration which includes: business phone number, business fax number, business email address, and full business address including: street, city, state, zip code.

Employer Services collects, stores, and shares business operating states and employment reporting state.

Interstate Actions (InterAct) collects, stores, and shares chat history from its users. The InterAct CSP function was in its pilot phase, but is now planned for removal. Chat history sharing does not occur. Chat history might include sensitive information discussed between state users. This data will be disposed after the InterAct function is removed.

Electronic Document Exchange (EDE) collects and shares files from state users. These files contain child support case information on custodial parent(CP), non-custodial parent (NCP), child(ren), and DOB information.

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

The CSP web application's main purpose is to facilitate exchange of data, facilitate data collection functions, query information, and most importantly; facilitate resolution of some of the problems caused by the interstate movement of custodial parties (CP) and non-custodial parents (NCP). The CSP web application's include functions such as Employer Services, locate, intergovernmental reference guide, and the electronic document exchange (EDE). Employer Services allows businesses to voluntarily provide a list of the states in which they operate and designate a single reporting state to submit new hire information to the OCSE and NDNH. EDE allows states to exchange encrypted case-related documents.

Access to any of the applications or services is controlled by role-based access based on the function each user is assigned to perform. All CSP registration information is kept indefinitely until that user's account is closed, after which the registration data is kept for audit purposes temporarily according to audit record retention schedules.

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

Yes

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

Clinical Study Data

User Credentials

Federal Employee Identification Number (FEIN)

Child Support Case Numbers

Business contact information

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

Employees

Public Citizens

Business Partners/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 for PII is to register individuals for a system account.

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

There are no secondary uses for the PII.

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

42 USC § 654(26)
42 USC § 653(l) and (m)

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.

09-80-0387, Federal Parent Locator Service Child Support Services Portal, HHS/ACF/OCSE

Identify the sources of PII in the system.

Online

Government Sources

Within the OpDiv

Non-government Sources

Members of the Public
Private Sector

Identify the OMB information collection approval number and expiration date

OMB: 0970-0370 10/31/2015; Renewal In Progress

Is the PII shared with other organizations?

Yes

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

State or Local Agency/Agencies: The CSP facilitates intergovernmental exchange of authorized information between states in support of mandated child support case processes. States get child support information based on Child support cases being worked on, functions such as the electronic document exchange (EDE) enable states to share pertinent data needed towards case resolution.

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

OCSE has Security Agreements in place with all state child support agencies where data sharing occurs.

Describe the procedures for accounting for disclosures.

Disclosure of data in audit logs is due to an IRS 1075 publication requirement for Office of Child Support Enforcement (OCSE) to provide states with audit files. Disclosure to any other Portal users is established through agreements, and any PII information accessed is tracked by Portal audit records of user transactions. All authorized users who get access to this disclosed information, must adhere to OCSE Security Safeguards when they access such data. The OCSE Security Safeguards include FISMA, HHS, NIST, and IRS security requirements as well.

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 notification for system users occurs at the time of collection of their PII which is during user account set-up. The CSP presents the user with a web form that requires them to enter their PII in order to proceed. The user must enter their registration information, then hit submit. The information is then displayed back to the user, with the exception of the password, so they can confirm their details are correct. Throughout the process, the Privacy Policy is available to the user via a link at the bottom of the page. There is no process in place for individuals' PII that is collected as part of their involvement in child support cases as the collection of their information is mandated by federal statute.

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.

There is no opt-out method for the collection or use of an individual's PII. If a system user wants to opt-out of the collection or use, then they will not be granted a system account; this may or may not be allowed based on job duty.

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

Consent is not required from individuals involved in child support cases because the information collected is mandated by federal statute. System users are notified of major system changes in advance using Broadcast Messages on the CSP Welcome Page. When necessary, email notifications are also sent to registered users to notify them of the impact of the changes being made. If the system user does not reach out after seeing the Broadcast Message or email, this is interpreted as consenting to the change.

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.

Individuals seeking to amend a record about themselves or inquire about the way their PII was obtained, is used, or has been disclosed should address the request for amendment to the System Manager.

Individuals can determine the best way to contact the System Manager by visiting the 'Contact Us' page within the CSP which includes a phone number and email address for the CSP Help Desk. The request should 1) include the name, telephone number and/or email address, last four digits of the Social Security number (SSN), and address of the individual, and should be signed;

2) identify the record being addressed is from the CSP; 3) identify the information that the individual believes in not accurate, relevant, timely or complete; 4) indicate what corrective action is sought; and 5) include supporting justification or documentation for the requested amendment.

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

An annual review of all authorized users and their data is conducted. An automated program performs an annual review of all authorized users and their PII is matched against the National Directory of New Hires (NDNH) database to verify the data integrity, availability, and relevancy. If this software fails to match the current user data against the NDNH, it sends a notification to the system administrator, who then manually verifies the data and resolves any issue. Users may also access their own profile data at any time on a user profile page. If they find that their contact information is inaccurate, they may change it on their own. If they find that their PII data is inaccurate, as used to verify them against the NDNH, they may contact the help desk to resolve any issues (as described in the above answer).

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

Users:

Users have access to their own PII only.

Administrators:

In the production environment, system administrators manage registration tasks and have access to all user PII.

Contractors:

Direct contractors serve as both administrators and users.

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

Each user has access to their own personal PII and no other personal information. Only administrators may access the PII of all user accounts. There are two user roles within the User-Based Access Control scheme that provide administrator level access to an account. Only an existing system administrator or back-end system administrator may grant one of these roles after approval from the Contracting Officer Representative (COR) via email. These roles are only granted to OCSE federal staff or direct contractor staff with a specific business need.

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.

User roles have sufficient granularity to restrict users to the minimum amount of PII necessary to perform their job. User roles are designed and assigned according to the principle of least privilege, giving a user account access to only the amount of information which is essential to the user's work. Users that hold the role of system administrator or back-end system administrator have the highest level of access to PII in the form of user profiles and can grant access to other user accounts. System administrators need access to full user profiles to support user identity verification during registration and for restoring access when users forget their credentials. During the user registration process, the system requires only the minimum amount of PII necessary for identity verification and account creation. This method prevents additional and/or optional PII from being submitted by the user and stored in the system for others to access. In addition, the SSN reduction effort has minimized administrator access to SSNs by truncating existing records to only keep the last 4 digits and restricting new accounts to only collect the last 4 digits.

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.

Annual security awareness training is required for all personnel that work on/with CSP and is provided by Health and Human Services (HHS)/Administration for Children and Families (ACF).

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

Annual training includes Internal Revenue Service (IRS) regulations, Federal statutes, and HHS and ACF regulations. OCSE provides additional annual training based on employee role and job function within the operating division (OpDiv).

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.

In tandem with the ACF Records Officer, OCSE is proposing the following data retention timelines to the National Archives and Records Administration (NARA): The minimum data retention period for the CSP is 5 years after cutoff unless a data set contains federal tax information in which case it must be retained for a minimum of 7 years as defined by IRS compliance requirements (IRS Publication 1075). Cutoff for CSP user accounts is defined as the date in which the account is deactivated.

At this time, system data goes through a defined destruction process on or after the 7 year mark, while user account information is kept indefinitely while a logical destruction approach is planned.

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

The information is secured in accordance with a system classified as "moderate" according to FIPS 199. Security controls include, but are not limited to:

Administrative Controls:
Security Assessments by independent assessors
System Interconnection Agreements
Signed Rules of Behavior
Annual Security Awareness Training
Risk Assessments
Separation of Duties

Technical Controls:
Firewalls
Boundary Protection - Deny By Default / Allow By Exception
User Identification and Authorization for organizational and non-organizational users
Multifactor Authentication
Audit and Accountability
Vulnerability scanning
Intrusion Detection monitoring
Use of Cryptography

Physical Controls:
The CSP MA is hosted within the OCSE Data Center (ODC) General Support System (GSS) and thus inherits the physical controls from the ODC GSS. These controls are outlined in the ODC GSS PIA.

Identify the publicly-available URL:

https://ocsp.acf.hhs.gov/

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that do not collect PII

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