US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/30/2023

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?

Existing

Does the system have Security Authorization (SA)?

Yes

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

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

The following minor applications were deployed on the Child Support Portal:
Data Access
Communication Center
Customer Inquiry Management (CIM)
iForms (International Forms)

Describe the purpose of the system.

The Child Support Portal (CSP) provides Office of Child Support Services (OCSS) internal and external stakeholders access to web-based tools and functions that support the Office of Child Support Services' (OCSS) mission. The CSP's web-based functions also support OCSS' commitment to enhance services via real-time access to pertinent information. The CSP provides authorized users with interactive access to select child support enforcement information.

The CSP provides many functions to the following stakeholders: employers, financial institutions, insurers, states, Tribes, and OCSS.

Employers use the CSP's web-based functions to provide OCSS with the employer's identifying and contact information, and employee status changes. Employers also use the CSP to provide lump sum payment information, and to provide a list of the states in which they operate and to 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 and Tribes use the CSP's web-based functions to access child support case information regarding obligor location, income and assets, and other inter-jurisdictional case information in the NDNH and Federal Case Registry (FCR) systems of records, as authorized by routine uses published for those systems of records. State and Tribal child support agencies also use the CSP to submit federally required reports, such as state plans and program self-assessment reports, including child support agency performance, agency contact information, and child support program information that does not include personal identifiers.

Representatives of OCSS use the CSP to submit, request and receive child support program reporting information that does not include personally identifiable information (PII), such as state plan and program self-assessment reports.

The NDNH interacts with other systems in the Federal Parent Locator Service (FPLS). Its primary purpose is to assist state child support agencies to locate noncustodial parents, putative fathers, and custodial parents to establish paternity and child support obligations, to enforce and modify orders for child support, and to address custody and visitation.

The Child Support Portal Registration Records system of records covers information provided by individuals who register to use the CSP's services to access information maintained in other OCSS systems of records. The CSP is a conduit (pass-through system) that provides authorized users with access to select, highly confidential child support case information maintained in the following systems of records:

- the OCSE National Directory of New Hires, HHS/ACF/OCSE, 09–80–0381;
- the OCSE Debtor File, HHS/ACF/OCSE, 09-80-0383; and
- the OCSE Federal Case Registry of Child Support Orders, HHS/ACF/OCSE, 09-80-0385.

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: user name or ID number, business function (e.g., enforcement), workload identifier (e.g., alpha work caseload), employer, county of employment, telephone number, telephone service provider, Tribal affiliation, Social Security number (SSN), date of birth, email address, the name, address and Federal Employer Identification Number (FEIN) of the individual's employer, selected security questions and responses, and individual passwords for access 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.

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

Communication Center will allow states, OCSE, and partners to share communications on the portal. Child support agencies, employers and OCSE staff can send documents to each other in support of child support enforcement.

The iForms application will allow users to create international child support Convention Forms. Convention Forms are needed to support cases that cross international boundaries. Once created, the forms can be translated and downloaded or printed to be sent to other countries.

The Office of Audit (OA) provides OA agency personnel with a means to upload child support case audit record files to SSA, to manage these files, and retrieve them

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 applications include functions such as Employer Services, locate, intergovernmental reference guide, and the electronic document exchange (EDE). Employer Services enables authorized users to enter terminations, lump sum payouts, and employer contact information that the CSP network will send to state child support agencies. It also provides a method for multistate employers to identify the states where they do business and where they have subsidiaries. Employer Services allows the organization to report new hire and quarterly wage information through one of the states in which they do business. Employer Services also allows insurers to query federal offset data

EDE allows states to exchange encrypted case-related documents. Documents sent via Communication Center are stored in ODC GSS temporarily.

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.

Demographic data, Employee Records, Training records, Insurance Information

User Credentials

Federal Employee Identification Number (FEIN)

Child Support Case Numbers; Residential address

Business contact information

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

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 U.S.C. § 654(26), State plan for child and spousal support
42 U.S.C. § 653(l) and (m), Federal Parent Locator Service
2007 Hague Child Support Convention, Articles 11(4), 12, 25, 55 and 57
Uniform Interstate Family Support Act of 2008, § 706(b)(1)

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.

“Child Support Portal Registration Records ,” No. 09-80-0387, 87 FR 3560 (January 24, 2022)

Identify the sources of PII in the system.

Identify the OMB information collection approval number and expiration date

Child Support Portal Registration, OMB NO: 0970-0370, expires February 28, 2025

Is the PII shared with other organizations?

Yes

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

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. MOUs are in place with HHS OpDivs and other federal agencies.

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. All user activity in CSP is captured in audit logs. CSP administrators may be required to view PII in order to assist users with registration or authentication issues.

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.

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. To request access to a record about you, submit a written request to the System Manager. The request should include your name, telephone number and/or email address, current address, and signature, and sufficient particulars (such as, date of birth or SSN) to enable the System Manager to distinguish between records on subject individuals with the same name.

In addition, the request must reasonably identify the record and specify the information contested, the corrective action sought, and the reasons for requesting the correction; and should include supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.

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 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.

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

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.

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.

New hire orientation, Computer Awareness and Record Management, and annual security awareness training is required for all. Training is provided by HHS, ACF, and by OCSE. Contractors with elevated privileges do additional role-based training based on job responsibilities.

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.

Upon approval of a disposition schedule by the National Archives and Records Administration (NARA), the user registration records will be deleted when OCSE determines that the records are no longer needed for administrative, audit, legal, or operational purposes, and in accordance with the NARA-approved schedule. Approved disposal methods for electronic records and media include overwriting, degaussing, erasing, disintegration, pulverization, burning, melting, incineration, shredding, or sanding. 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 system leverages cloud service providers that maintain an authority to operate in accordance with applicable laws, rules, and policies, including Federal Risk and Authorization Management Program (FedRAMP) requirements. Specific administrative, technical, and physical controls are in place to ensure that the records collected, maintained, and transmitted using the OCSE Data Center General Support System are secure from unauthorized access. Access to the records within the system is restricted to authorized personnel who are advised of the confidentiality of the records and the civil and criminal penalties for misuse, and who sign a nondisclosure oath to that effect. Agency personnel are provided privacy and security training before being granted access to the records and annually thereafter. Additional safeguards include protecting the facilities where records are stored or accessed with security guards, badges and cameras; limiting access to electronic databases to authorized users based on roles and either two-factor authentication or user ID and password (as appropriate); using a secured operating system protected by encryption, firewalls, and intrusion detection systems; reviewing security controls on a periodic basis; and using secure destruction methods prescribed in NIST SP 800-88 to dispose of eligible records. All safeguards conform to the HHS Information Security and Privacy Program, https://www.hhs.gov/ocio/securityprivacy/index.html. 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.

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

No

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

Yes

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

Yes